Strategy and organisational cybersecurity: a knowledge-problem perspective

Mark Paul Sallos and Alexeis Garcia-Perez
Centre for Business in Society, Coventry University, Coventry, UK
Denise Bedford
Georgetown University, Washington, District of Columbia, USA, and
Beatrice Orlando
Department of Management, Sapienza University of Rome, Roma, Italy

Received 2 March 2019
Revised 16 March 2019
Accepted 4 July 2019

Abstract

Purpose – The purpose of this paper is to frame organisational cybersecurity through a strategic lens, as a function of an interplay of pragmatism, inference, holism and adaptation. The authors address the hostile epistemic climate for intellectual capital management presented by the dynamics of cybersecurity as a phenomenon. The drivers of this hostility are identified and their implications for research and practice are discussed.

Design/methodology/approach – The philosophical foundations of cybersecurity in its relation with strategy, knowledge and intellectual capital are explored through a review of the literature as a mechanism to contribute to the emerging theoretical underpinnings of the cybersecurity domain.

Findings – This conceptual paper argues that a knowledge-based perspective can serve as the necessary platform for a phenomenon-based view of organisational cybersecurity, given its multi-disciplinary nature.

Research limitations/implications – By recognising the knowledge-related vectors, mechanisms and tendencies at play, a novel perspective on the topic can be developed: cybersecurity as a "knowledge problem". In order to facilitate such a perspective, the paper proposes an emergent epistemology, rooted in systems thinking and pragmatism.

Practical implications – In practice, the knowledge-problem narrative can underpin the development of new organisational support constructs and systems. These can address the distinctiveness of the strategic challenges that cybersecurity poses for the growing operational reliance on intellectual capital.

Originality/value – The research narrative presents a novel knowledge-based analysis of organisational cybersecurity, with significant implications for both interdisciplinary research in the field, and practice.

Keywords Strategy, Complexity, Epistemology, Intellectual capital, Systems theory, Knowledge-problem, Cybersecurity theory

Paper type Conceptual paper

1. Introduction

1.1 Information technology and the cybersecurity problem

Since its popularisation, information and communication technology has redefined economic value creation by enabling businesses to decrease their dependence on tangible assets and capital, in favour of intellectual capital. This, in turn, has made most markets rely on what Kuehl (2009) describes as the first man-made domain. A benefit of exploiting the cyber domain is the newfound ability of businesses to leverage its relative absence of temporal and geographical constraints as an enabler of novel business models. However, an increasingly meaningful side effect of this reliance lies in the scope of the vulnerability it entails. Cyber threats can disrupt the security, stability and sustainability of organisations by affecting the confidentiality, integrity and availability of informational/structural capital. Examples of this potential for disruption and the externalities it imposes range from organisational collapse (i.e. Ashley Madison – Baraniuk, 2015), to the incapacitation of the infrastructures of nation-states (Kaiser, 2015; Zetter, 2016). Even when discussing the societal effects of cybersecurity, organisations still present themselves as the core vectors of action, given their dual role of technology developers and facilitators of its use. Paradoxically, cybersecurity remains a

Journal of Intellectual Capital
Vol. 20 No. 4, 2019
pp. 581-597

1469-1930
DOI 10.1108/JIC-03-2019-0041

secondary task within most business models, as it provides limited opportunities for monetisation and value creation – the organisational raison d'être. Given its adversarial dynamics, cybersecurity strategy is rooted in a metaphorical self-perpetual "war" scenario, which, unlike its individual "battles", cannot be definitively won. In other words, cybersecurity is not a problem that can be "solved". Furthermore, much like most strategic endeavours, cybersecurity management exhibits an epistemic core.

1.2 Cybersecurity, knowledge and intellectual capital

"Knowledge" as a construct permeates the cybersecurity and the wider organisational risk narratives in a number of ways. The link between risk and knowledge has been highlighted by Neef (2005), who argues that an organisation's ability to effectively manage risk is rooted in its ability to manage relevant knowledge. In relation to cybersecurity, Tisdale (2015) outlines the need for multi-dimensional approaches which expand the "typical" technical outlook, in favour of a systems/complexity orientation and a knowledge management foundation. Within an Information Security (IS) context, Shedden *et al.* (2011, p. 152) illustrate the importance of accounting for the risks towards "the cultivation and deployment of organisational knowledge". Julisch (2013) describes a relationship between knowledge limitations and the ineffectiveness of a cybersecurity strategy as evidenced by an over-reliance on intuition, absent security foundations, inadequate governance, or a dependence on static/generic "knowledge" of the context. In a broader context, Kianto *et al.* (2014) argue that organisational value generation based on intellectual capital is inherently moderated by knowledge management practices. Given that organisational cybersecurity management aims to protect both intellectual assets and their operationalisation, it fulfils a moderating function for the value generation process, converging with the domain of knowledge management.

Besides their relatively consistent, complementary message, these papers exhibit significant epistemological variability as they reflect the dominant themes of their individual disciplinary settings. This hinders the clarity of this shared narrative, though not necessarily of the individual papers. The absence of a common interpretation of knowledge limits the homogeneity of insight and prescriptive utility that can be achieved through a phenomenon-driven, rather than a discipline driven approach. The former enables studying organisational cybersecurity as an interplay of technology, people and processes, with a focus on competitive performance, intellectual capital and sustaining value creation.

Although Intellectual Capital is a well-established and flourishing research topic, it is still perceived as one that continuously evolves (Guthrie *et al.*, 2012) in response to changes in the social, economic and technological environment. Defined as "the sum of everything everybody in a company knows that gives it a competitive edge. Intellectual capital is intellectual material, knowledge, experience, intellectual property, information that can be put to use to create value" (Dumay, 2016, p. 169), most scholars acknowledge the role of intellectual capital in value creation. That means a shift in intellectual capital research from the organisation to its wider ecosystem, where knowledge and value are created (Dumay, 2013; Dumay and Garanina, 2013, p. 21). Paradoxically, cybersecurity risks emerge as a result of – among other factors, the systemic interaction of those elements that form the organisational ecosystems and which they, in turn, contribute to shaping, such as the organisation's internal processes and its modes of competition and value capture. Subsequently, a solely technical outlook on cybersecurity as a function is myopic, failing to account for emergent socio-technical organisational mechanisms and processes involving the organisation's human, relational and structural capital, which underpin value generation. This leads us to argue that a knowledge-based view of cybersecurity and its management would have a direct effect on intellectual capital management by affecting the dynamics of human, relational, structural, as well as renewal and trust capital (Kianto *et al.*, 2014).

We also argue that a core pillar for meta-disciplinary inquiry into a strategic perspective of cybersecurity is the notion of knowledge. Knowledge, in this context, must be anchored within the characteristics of its application setting in order to avoid ambiguity, tautological definitions and conceptual inconsistencies. More specifically, this paper aims to help both the cybersecurity research and practice communities engage with the distinct strategic challenges that organisations face in the pursuit of a localised, and at the same time evolving approach to cybersecurity. These challenges, which are described at length in the following sections, highlight the essential role of knowledge – not just as an asset, but also as the dynamic output of continuous processes, for both the effectiveness and the efficiency of defensive strides.

Furthermore, we argue that an explicit, context specific epistemological foundation is essential for the reconciliation of the variety of perspectives and dimensions of cybersecurity management and strategy. Such an epistemology should enable cybersecurity strategists to guide their efforts based on contextually appropriate answers to fundamental questions such as: "What can be known about cyber security vulnerabilities and threats?", "What is cyber security knowledge?", "Where to look for it?", and, "How can it be used?". In addition, we aim to provide a relational understanding of core epistemic constructs such as knowledge, uncertainty, beliefs and truth in the context of organisational cybersecurity.

To achieve its aims, the remainder of this paper has been organised as follows: a critical overview of knowledge in its role within organisational literature is provided in Section 2; Section 2 also explores the epistemic substrata of cybersecurity strategy and is used to propose an explicit epistemological position. Finally, Section 3 explores the regularities of cybersecurity epistemic challenges which must be accounted for in the development of a phenomenon-oriented approach to organisational defence.

2. Knowledge, strategy and cybersecurity – a theoretical precursor

Throughout the last three decades, interpretations of knowledge as a construct have underpinned several core strands of strategic management and organisational theory. Examples include the knowledge-based view of the organisation (Curado and Bontis, 2006), Dynamic capabilities (Eisenhardt and Martin, 2000; Zahra and George, 2002; Arend and Bromiley, 2009), and knowledge management (Nonaka and Peltokorpi, 2006; Ragab and Arisha, 2013). However, the utility of such attempts has been put into question for reasons which include an unclear or contended interpretation of knowledge (Wilson, 2002), varied degrees of perceived empirical utility (Edvardsson, 2009; Ibrahim and Reid, 2010), overly divided themes which dilute the original vision of progress (Davenport, 2015) and, eventually an inability to circumvent Occam's razor (Wilson, 2002).

This tradition of employing "knowledge" as an explanatory or a prescriptive construct presents regularities which are noteworthy when applied to an epistemic view of organisational cybersecurity strategy. Identifying what distinguishes an "effective", or at least enduring epistemic foundation of concepts in organisational theory remains a speculative endeavour. However, the significant body of literature on the topic provides a blueprint of key aspects that position individual conceptualisations in a wider context. These are generally interdependent, and include the epistemological stance which informs the locus of knowledge (i.e. the knower), its manifestation/form (the known), as well as the role, the nature and the attainability of truth. We also hold the relational positioning of uncertainty as contextually relevant.

All of these points will be addressed through an evolutionary lens of organisations as function-selected hierarchical systems. This perspective serves as a heuristic for representing the role of market competitive mechanisms and dynamics as adaptive pressures and change triggers. Furthermore, as we explore strategic knowledge as an enabler of inference and effective decision making, we recognise the influence of

assumptions about cognition and environmental dynamics in these processes. This allows us to anchor the discussion beyond its philosophical roots to accommodate the progress made in studies of cognition, and systems theory for organisational cybersecurity in the following chapter. By doing so, we aim to support the establishment of a phenomenon-oriented approach to strategic enquiry on the topic, based on an adequate epistemic diagnosis of the predicament that organisations face. This, we hold, enables the conceptual framing of organisational cybersecurity in a discipline agnostic manner, which presents novel avenues for investigation, and a range of potential investigative tools.

In order for this to be achieved, organisational cybersecurity knowledge will be explicitly explored in line with the previously outlined "blueprint". We will therefore start by considering the applicability of individual and collective views of knowledge in the current setting of analysis.

2.1 Locus of knowledge: systemic view

Given its turbulent role as a construct in organisational theory, the notion of knowledge is difficult to address in the absence of context-specificity. As a central topic in the evolution of philosophy, a continuum of positions can be identified, that are distinguishable in their views on both the object and the subject of knowledge. The relationship between the "knower" and the "known" is thus a key area of contention of the philosophical divide. Proponents of an individualist position view knowledge and the knower to be indivisible for most purposes. Subsequently, they hold that attempts to "manage" the epistemic contents of an organisation are generally concerned with information mistaken as knowledge (Wilson, 2002). In an attempt to distinguish the concept from information, Nonaka and Peltokorpi (2006) argue that "[…] knowledge is about beliefs, commitment, perspectives, intention and action". This perspective supplements the Platonic notion of the belief as the unit of knowledge (Boisot, 2011), which is generally accepted beyond disciplinary confines, by associating it with intention and action.

However, we view this perspective as limited within our context, as it induces a systemic myopia due to a sole focus on individual beliefs and actions. Such a mechanistic representation can underemphasise the role of coordinated knowledge networks which exhibit non-summative attributes. They also enable collective, complementary patterns of action and behaviour reflecting emergent social and epistemic dynamics. Within the context of organisations, these are also moderated through structural power dynamics. As a result, we do not deny the role of the agent as the basic locus of knowledge, but instead propose that this position is limited when explaining phenomena which span across levels/systemic hierarchies, i.e. the behaviour of an organisational function. Thus, the locus of knowledge must account for the role of the cognisant agent within his/her social context of action (Brown and Duguid, 2001; Guzman and Wilson, 2005) and on externalised, "objective knowledge" which underpins explicit critical inquiry (Popper, 1978).

An increasingly widespread perspective in evolutionary psychology and cognitive studies explores knowledge and rationality through the lens of their teleologic function. This view suggests that, given the hyper-social evolutionary niche inhabited/constructed by humans (Laland *et al.*, 2000; Sperber and Mercier, 2012), the primary functional evolutionary pressures imposed on reasoning and, thus, conceptual knowledge processes, have been of a social nature. Implicitly, the general problem-solving attributes of reasoning are exaptive (Gould and Vrba, 1982), i.e. a side-effect of a different teleological function.

This perspective supports the view that knowledge has an essential social form, beyond its individual relativist (Proctor, 1998; Wilson, 2002) and abstract "objective" dimensions (Popper, 1978). Such an interpretation favours a pragmatic, systems-oriented view of knowledge in organisations. If knowledge is a lever for shaping intent into action, the activity of an organisation is conditioned by a coordinated network (with potentially

multiple sub-systems) of knowers. As individual action in such settings relies on the structure and the requirements of the system, its pragmatic utility is reflected in the performance of overall system.

Furthermore, new knowledge can be made "useful" (i.e. actionable towards achievement of an objective of the organisation as a system) through an interplay of dissemination and coordination strategies where the influence of individual knowers can be leveraged into action through structural mechanisms including not only the human capital of the organisation but also its relational and structural capital. Similarly, evolving environmental pressures can render previously effective representational models and knowledge objects locally maladaptive – a core premise of "organisational unlearning/relearning" processes (Zhao *et al.*, 2013). Thus, a collective perspective also influences what constitutes the unit of knowledge, bridging the gap between actor belief and systemic action. The "claim" in this case seems to be more compatible with both the formal evaluation process needed to pursue the justification component of the Platonic "justified true belief", and with the notion and degree of truth (Popper, 2005).

The utility of the claim as a unit of knowledge relies on a recognition of the fact that the relationship between claims and beliefs is not absolute. While claim validation/evaluation procedures may not be sufficient to change individuals' beliefs and behaviour, identifying discrepancies between the two is possible by recognising indicators of anomalous action. This ability to identify relevant patterns of inconsistencies between claims and beliefs as drivers of action is analogous to a meta-cognitive process – seeking knowledge about knowledge and its limitations. Tracking and adapting inferential representations and procedures requires an externalised unit of knowledge, especially in a collective setting. Thus, a relational dynamic base of knowledge claims enables a collective meta-cognition analogue, and the pursuit of adaptive epistemic measures. Such an ability is undoubtedly valuable within the context of strategy formulation as a precursor to rational adaptation and heuristic selection (Peters *et al.*, 2010).

2.2 Epistemic pragmatism

> Truths in strategy are neither certain nor final, and our wishing cannot make them so. Whatever philosophical foundations strategy may build upon – pragmatist or otherwise – they must surely incorporate this difficult truth (Powell, 2002, p. 879).

The emerging narrative places our interpretation of knowledge at the intersection of pragmatism and critical realism. We present this stance as "bottom-up" pragmatism due to the central evolutionary/competitive focus, the epistemological centrality of action and utility, as well as the locus and unit of knowledge. Unlike other epistemic processes, such as scientific enquiry, organisational knowledge is adaptive to the extent that it is useful in better enabling/sustaining value creation. This is particularly relevant for cybersecurity as a function which cannot be monetised within most business models, yet preserves Intellectual Capital and its operationalisation process. The resulting position shapes notions such as certainty, belief and truth. It also holds knowledge as emergent from the interaction between the subject and the object of inquiry. In doing so, the conceptual emphasis on an abstract, traditional interpretation of truth is avoided in favour of a more dynamic, evolutionary focus (Proctor, 1998).

In practical terms, our approach to the study of cybersecurity knowledge entails a focus on three key aspects: fitness-inducing belief-claim systems; adaptivity – that is, an adaptive approach to the formation of beliefs to facilitate coevolution between the system (i.e. the organisation or community of practice) and its environment; and an understanding of knowledge as context-bound. Clarke (1989) presents a "theory of rational acceptance" as a pragmatic alternative to the emphasis on truth. Acceptance is presented as the balance

between the costs associated with adopting a mistaken proposition and the costs of gathering additional evidence to inform a decision. As knowledge development in organisations is in itself pragmatic (purpose bound) and contextual (utility constrained), and addresses a diverse mix of dynamic ontological phenomena which are deemed relevant to organisational activity and performance, the truth value of individual beliefs is local, temporary, and secondary to their ability to trigger favourable action.

From a strategic perspective, the core utility of knowledge is inferential (Mercier and Sperber, 2011). By its very nature, strategy formulation addresses future occurrences. However, its role in decision-making entails the use of perception and observations (representational or procedural) for the identification and exploitation of ontological regularities which connect behaviour patterns with specific outcomes. So, for example, vulnerability management entails identifying conjunctures between the attributes of systems and possible patterns of behaviour (malicious or otherwise) which can lead to inferable, undesirable consequences. Within this context, knowledge about other conjunctures which do not fit this pattern lacks direct strategic utility, as it does not enable inferences related to the area of concern, while the absence of ontological regularity, generally through complexity, limits possible inferences to a meta-representational position – knowledge about (lack of) possible knowledge, and its limitations. (Allen *et al.*, 2007)

2.3 Knowledge and uncertainty

The limitations of knowledge, both current and potential, are generally addressed through the notion of uncertainty. Haimes (2011, p. 1178) defines uncertainty, from a systems-based outlook, as "the inability to determine the true state of a system". Such inability can be rooted in the presence of "incomplete knowledge" (i.e. "epistemic uncertainty") and/or in "stochastic variability" (i.e. "aleatory uncertainty"). Unlike epistemic uncertainty, stochastic variability does not, by definition, address representational regularities which could be illuminated through additional knowledge.

Within the context of risk and decision-making, Cox (2012) classifies uncertainty based on its attributes rather than its cause. Subsequently, if a system cannot be accurately modelled, or if its future states cannot be reasonably foreseen, it can be argued that the system exhibits "deep uncertainty". Allen and Boulton (2011) on the other hand equate deep uncertainty to complexity (i.e. non-linear dynamics). On this basis they propose that, given the limitations of inference/planning under deep uncertainty and the inherent inability to suppress the stochastic variability through enquiry, assumptions ground the projection of a system's state and enable a representation of conditional/probabilistic "certainty". Thus, the use of assumptions as epistemic crutches in areas of deep uncertainty, such as cybersecurity strategy, is unavoidable.

Outside of the systems-based perspective, Mousavi and Gigerenzer (2014) argue that such assumptions, in the form of heuristics, are central to human cognition given its perceptual and inferential limitations and high environmental complexity. In a more rigid approach to the subject, Mousavi and Gigerenzer (2014) describe uncertainty as characterising any situation outside of complete, or probabilistic certainty. That is, a situation where causal relationships or outcomes are not knowable, or where risk cannot be inferred probabilistically. Risk assessment in this case relies either on the characteristics of the situation/system (i.e. a-priori), or on statistical analysis in conditions of highly homogenous occurrences.

Based on the interpretation above, "technologies of rationality" (March, 2006) such as risk management, adaptive management or resilience management have a heuristic function within the context of organisational cybersecurity management. Such approaches generate an output of contingent certainty through a series of processes underpinned by meta-representational assumptions concerning what is known and what can be known.

In doing so, the core uncertainty faced by decision-makers in the context of cybersecurity is only addressed by traditional business strategy tools to a limited extent. This leads us to argue that the accuracy of the output of a management strategy is determined by how applicable the specific process it uses is to its application setting, rather than by the "goodness"/"quality" of the heuristic in itself – a context-construct fit. Gigerenzer and Brighton (2009) describe this fit through the concept of "ecological rationality" and position it as an essential consideration for decision-making under uncertainty.

From a pragmatic perspective, achieving a satisfactory degree of ecological rationality and, implicitly, inferential accuracy, does not necessarily entail a suppression of uncertainty concerning the properties of the system. Instead, it entails an ability to accurately evaluate the local fitness of a heuristic in relation to a set of expectations. This can take the form of feedback-based adaptation, which can include experiential learning, learning from others and variation/selection processes (March, 2006). Through such approaches, a contextually sensitive, meta-systemic type of knowledge can be generated concerning conjunctures of system states, environment states, and applicable strategies. At the same time, given the established belief-claim dependence of knowledge, and the structure-persuasion requirements for individual knowledge to trigger action in organisations, the occurrence of learning driven by ecological rationality is not generalisable for it to cover contexts such as cybersecurity.

As a result, we argue that, in relation to cybersecurity strategy, knowledge should not be treated as an asset, but as the contextually sensitive foundation of inference manifested in beliefs and claims (which underpin representational models and procedures), and, thus, as the dynamic determinant of the context-construct fit in cybersecurity decision-making. At an organisational level, the individual nature of the belief is often circumvented by using attributes related to local structure and information/knowledge dissemination. As a result, organisations can exercise rational order (McKelvey, 2001) in spite of the potentially heterogenous individual beliefs of members. Furthermore, the efficacy of actions which target the dynamic characteristics of a problem is likely to be increased by an awareness of the inferential potential of the various approaches to decision making and heuristics inherent to a given environment. Based on our proposed interpretation of knowledge, the essential mechanism of calibration of the organisation strategy relies on assimilation of feedback and strategies for selection of adaptive pathways. An ability to distinguish adaptive beliefs becomes the precursor of knowledge building. The following section explores why organisational cybersecurity strategy is conditioned by a fundamental knowledge problem with local manifestations, and societal consequences.

3. The cybersecurity strategy knowledge problem

Throughout the previous section we have proposed that the strategic utility of knowledge is inferential, as it guides system behaviour towards desired future states which, by definition, cannot be directly observed. Management strategies must infer the value of the procedures/processes employed in relation to an objective based on available evidence. The effectiveness of local measures of uncertainty mitigation must be evaluated. This applies even to adaptive strategies which rely on a suppression of inference due to a distrust in the accuracy or the utility of the process. As a result, the notion of a "knowledge problem" in relation to cybersecurity strategy can be perceived as a descriptor of a hostile context for effective inference. This can entail the absence of observable ontological regularities, or limitations in the ability to acquire and use relevant information concerning the vulnerability base, relevant threat behaviour and the potential effects of cybersecurity incidents on business or society.

3.1 Ontological nonlinearity of the cybersecurity problem

In line with systems-thinking, the degree of complexity which characterises a problem area determines the utility gained through predictive/inferential approaches by constraining

what can be known (Boisot, 2011). Complexity, in this sense, entails nonlinearity within a system's interacting elements. Complex systems should also be distinguished from complicated systems which, in spite of high dynamism and convoluted behaviour, exhibit linearity and causal consistency (Phister, 2010; Merali and Allen, 2011). Thus, the term complexity is used to describe a vast spectrum of system behaviour. Benbya and McKelvey (2006a, p. 17) suggest that systems can exhibit three possible states: stable, chaotic and an intermediate state of "critical complexity", "emergent complexity" or "melting zone". Stable system behaviour entails causal linearity and proportionality. Any uncertainty in such systems is epistemic and can be mitigated against through the assimilation of sufficient and adequate information. On the opposite pole, systems in chaotic states offer no inferable regularities, and are characterised by predominantly stochastic uncertainty. As the consistent lack of regularity can be considered a regularity in itself, knowledge collected about such systems is meta-representational, that is, knowledge about knowledge.

IS has been explored through a chaos-theory perspective by Sharma and Dhillon (2009). We hold IS chaotic behaviour as a scale-dependent phenomenon, given aggregate incident consistency which indicates patterns of emergence. For example, while longitudinal studies such as Romanosky's (2016) generally show patterns of regularity in their representations of cybercrime incidents at a macro-level, it is unlikely that the volume and type of incidents faced by the individual actors included shows any degree of consistency. This phenomenon is compatible with what Manson (2001) classifies as aggregate complexity – a distinct branch of complexity studies which focusses on interactions between linked system components. Such interactions can show emergent regularities that cannot be decomposed or inferred through a mechanistic perspective (Gershenson, 2013). These regularities may result from a range of possible interactions between the different components of a complex system and with those in its environment (Rickles *et al.*, 2007). In practical terms, within the context of cybersecurity breaches, a specific effect such as loss of Intellectual Property can be generated by malicious actors in a number of ways (i.e. threat vectors), depending on the properties of the system within a specific setting of space and time.

In addition to the dynamics of relationships, emergence and locality as defined by the interaction between system components and the environment, Manson (2001, p. 410) also outlines the key role of "learning and memory within systems", embodied in their structural adaptation which is often enabled by the variety of its components. As the state of a system is to a large extent the result of its exposure to evolutionary pressures, the attributes that define such a state are likely to be have been used to make past decisions on the fitness of the system. When faced with novel conditions and relationships, such systems therefore rely on those same internal structures and sub-systems for their adaptivity. Thus, if no adequate adaptive change pathways are available, a system lacks resilience to perturbations, which may lead to a structural collapse (Holling, 2001). In this sense, social systems such as organisations are distinct. Their ability to make inferences is anchored in structural and cognitive mechanisms that expand the scope of their base of representations and procedures beyond those inherent to the system and its structure. For example, an organisation can adapt to the destructive potential of a cybersecurity breach in an anticipatory manner as long as the occurrence and consequences of such breach have been adequately inferred in advanced.

All of these indicators of non-linearity are likely to influence an organisation's ability for effective inference in relation to its cybersecurity efforts. For example, vulnerabilities emerge from the structure and patterns if interaction of a system's actors and its technological infrastructure, rather than from an additive logic between the two. The assessment of a system's vulnerability entail the inference of potential threats which could exploit a system component/attribute. It also relies on the conceptualisation of a relevant, homogenous, hierarchical and temporal sample of reference and the consideration for adaptive pathways which are grounded in the properties and "capital"/potential which have

been historically accumulated by the system (Holling, 2001). Finally, an awareness of potential disproportionality in the causal relationships between threads and vulnerabilities is also required. While this may seem a convoluted way of describing a vulnerability within the context of cybersecurity, it illustrates the embedded complexity of the concept which can be masked through implicit assumptions. This view also highlights the need for an emphasis on holism as a way to interpret discrete phenomena within the context of systemic strategy, as argued by Haimes (2012).

However, the emphasis on holism can raise analytical difficulties in systems which cannot be outlined in objective, consistent ways. The presence of an organisation in the cyberspace or "digital world" is generally shaped by the interaction between software vendors and developers, system architects and engineers, technologically active employees, managerial initiatives, organisational partners and end-users. Thus, delimiting the "cyber perimeter" of an organisation can be difficult, as vulnerabilities can emerge from sources that are, by their very nature, outside of the organisation. This network of interdependencies and the subsequent sensitivity to non-local phenomena (i.e. externalities) highlight the coevolutionary nature of organisational systems whereby "all 'evolution' is really coevolution […]" (Benbya and McKelvey, 2006b, p. 287). Thus, from a pragmatic perspective, given the secondary role of cybersecurity in organisational value creation, cybersecurity performance relies on the local manifestation of threats, on the organisation's adaptive capacity, namely "system learning" and positioning, as well as on its ability to develop, sustain and adapt adequate inferential procedures, and to act on resulting insights.

From a different perspective, the high degree of abstraction that complexity theory entails in relation to a micro-setting (e.g. that of an organisation) limits its practicality. The process of employing its principles for prescriptive use in the form of concrete actions and strategy is subject to interpretation. However, this ontological framing carries significant, more direct implications for the notion of knowledge, as it anchors the concept of knowledge in the principles of feedback and adaptation. In addition, a complex systems view provides a series of general, abstract assumptions which relate to the regularities that underpin any rational interpretation of cybersecurity. These include a limited accuracy in the quantification of dynamic, non-linear phenomena; the scale-dependent emergence of system attributes and patterns; a local manifestation of non-linearity and stochastic uncertainty; and finally, an emphasis on adaptive mechanisms and co-evolution. Additionally, within the context of the "knowledge problem" narrative, the systems perspective introduces a meta-cognitive dimension to the core logic of inference, strategy and action. In the absence of a cognitive anchoring, beliefs are replaced by path-dependent, context-defined tendencies as drivers of behaviour. Historically accumulated structures, sub-systems and relations define the foundation for adaptation when faced with perturbations. Even when accounting for cognition, this ontological substratum confines available system pathways and the ability to respond, and relies on the "belief" – arguably knowledge, as a trigger of action.

3.2 Epistemic limitations

The second dimension of the knowledge problem narrative lies in the exploration of the epistemic barriers faced, which are primarily information-oriented. This section addresses those phenomena that must be accounted for when formulating a cybersecurity strategy, which impede the ability to exploit regularities through inferential procedures.

3.2.1 Adversarial adaptation and asymmetry. One possible starting point in the exploration of epistemic uncertainty in relation to cybersecurity strategy is the informational asymmetry between the attacker and the defender. Although the adversarial macro-dynamics of this relationship are core to all competitive strategy, the contextual role of information is distinct, as breaches generally rely on an informational imbalance. Attackers aim to acquire

advantageous information concerning potential vulnerabilities and target appeal, while defence generally entails an anticipation of possible, or at least likely threats. This asymmetry is amplified by the ability of malicious actors to empirically validate assumptions and dedicate their full focus to finding a contextually adequate attack vector. In contrast, organisations as targets are primarily concerned with (market) value creation and maximisation, and therefore must centre their defence on the proportionality of their effort in relation to the perceived/assumed scale of the threats. Also, from the perspective of threat actors the costs of unsuccessful attacks are generally low, whereas unsuccessful defence can significantly affect operational sustainability of the attacked entity. There is an additional asymmetry in the objectives of each side: a successful defender must protect against all significant breach attempts, while a successful attacker must only achieve a single breach. A noteworthy trend relating to this asymmetry is the increasing complexity of cybercriminal operating models, which increasingly leverage specialisation and risk-spreading to form what Kraemer-Mbula *et al.* (2013) refer to as "cybercrime ecosystems", and Thomas *et al.* (2015) call "the underground economy".

3.2.2 Information sharing limitations and information asymmetries: sector-specific variation and reliance on third parties. Information sharing is widely seen as a beneficial mechanism for the mitigation of the attacker-defender asymmetry previously described (Gal-Or and Ghose, 2005). As a principle, it is central in a wide range of national cybersecurity strategy and policy initiatives (e.g. UK Cyber Security Strategy – UK Government 2009, 2011; the Cybersecurity Strategy for the European Union – European Commission, 2013; EO 13691 – White House, 2015). However, in spite of these efforts from policy-makers, effective information-sharing is, subject to sector-specific exceptions, impeded at least partly by the tension between the potential utility and the sensitivity of the shared content. This phenomenon is not novel. Ziv (1993) highlighted that without an ability to enforce "truth telling", participants in information sharing within oligopolistic circumstances are incentivised to prioritise the (mis)representation of their position and strength. The resulting market dynamics positions third party vendors as key owners of aggregate information. However, this also increases a misalignment in incentives to share information, as the "state of affairs" can be misrepresented in favour of a strategically convenient narrative (Greenberg, 2012). Furthermore, given the contextual dependencies which shape the nature of cyber incidents beyond the technological layer, and difficulties associated with the establishment of complex causal narratives (e.g. Detection proficiency, Osbourne, 2015; Attack attribution, Rid and Buchanan, 2014), the knowledge value of external incidents can vary significantly.

3.2.3 Misaligned incentives: strategic ignorance, biases and assumed rationality. Incentive misalignments occur at multiple levels within the context of cybersecurity, and can damage trust and result in deviations from expected behaviour and outcomes. As a result of misaligned incentives, gaps can occur between the representations that feed strategy development and the actual behaviour of agents. More specifically, Moore (2010) proposes a link between information systems failures and the misattribution of liability away from the actors that are responsible for defence. Misaligned incentives are likely to occur in dichotomous aspects of cybersecurity, such as the trade-off between accessibility/efficiency and security. Behavioural studies indicate that individuals are likely to favour approaches that are optimised for their operational priorities, often in the detriment of security (Kraemer *et al.*, 2009; Pfleeger and Caputo, 2012). As a result, the effectiveness of security policy relies on the identification and the discouragement of process deviations which fall outside of the scope of the chosen security stance. Without an awareness of actual beliefs and practices driving such deviations, subsequent strategy formulation is likely to employ a distorted interpretation of problem.

This brings to light a well explored limitation of risk models and technologies of rationality in general, namely the behavioural variability from rule-based representations of rational behaviour and reasoning (March, 2006; Pfleeger and Caputo, 2012). Inference into the behaviour of systems and agents must rely on a representation of likely actions and outcomes. However, the discrepancy between expected rationality models and actual behavioural tendencies has, over time, produced a significant stream of literature and distinct disciplines such as behavioural economics, with the aim of understanding and exploiting regularities in "irrationality" (Tversky and Kahneman, 1974; Kahneman and Frederick, 2002; Slovic *et al.*, 2005). While the association of widespread cognitive tendencies and inferential mechanisms with the notion of "irrationality" based on norms derived from traditional logic has been questioned (Gigerenzer, 1996), their role in problematic decision-making settings, such as cybersecurity, is uncontroversial (Pfleeger and Caputo, 2012). As a result, a knowledge centred approach to cybersecurity strategy must incorporate means of calibrating local assumptions about the projected and the actual behaviour of relevant actors. Game-theoretic approaches have been proposed for this purpose as essential tools in understanding threat behaviour (Bier *et al.*, 2008). However, their heuristic nature raises the issue of ecological rationality as a precondition for their utility.

3.2.4 Limited capabilities and situational awareness. Finally, a key barrier to the development of knowledge in the context of cybersecurity strategy formulation lies in the confines of the local capabilities and situational awareness exhibited by individual organisations. Discussing this factor at a high level of abstraction is difficult, as generalisations can only provide limited insight in relation to specific settings. However, capabilities and cyber situational awareness, as defined by Franke and Brynielsson (2014), are an overarching theme which underpins an organisation's strategic positioning, cyber resilience and responsiveness to environmental dynamics. Both the cognitive and the technical dimensions of an organisations' cyber situational awareness are underpinned by specific skillsets. Proxy indicators for the aggregate availability of such skillsets, such as the dynamics of the employment market for roles related to IS or Cybersecurity, indicate a justifiable, rapid growth in the corporate interest within the field. However, in spite of centralised efforts being made to proportionally increase the supply of expertise, there are a number of barriers which affect progress in this area. These include the absence of a centralised, common body of knowledge of the cybersecurity domain; the evolving, context-dependent requirements of the role; and the emphasis on "experience and social factors" over "learned technical skills and graduate entry" (Reece and Stahl, 2015, p. 193).

4. Conclusions

Cybersecurity management is a challenging dimension of the modern organisational landscape, and requires consideration within strategies, values, structures and practices. Its importance is exacerbated within organisational models which leverage intangible assets and intellectual capital as the primary platform for value generation. We argue that cybersecurity strategy is a multifaceted construct which benefits from a knowledge-centric narrative. From this new perspective, a cybersecurity strategy built upon effective knowledge management practices has the potential to channel the organisation's intellectual assets and their operationalisation towards value creation. This paper has set out the basis for such a narrative and highlighted the need for a pragmatic view of knowledge which entails emphasis on "belief-(claim)-action-result" rather than "information-truth-belief-action" when preparing for, dealing with, and recovering from cybersecurity incidents. By anchoring it to action, we have presented strategic knowledge as a local construct bound in its scale, scope and time value.

We have also addressed the concept of uncertainty in the context of cybersecurity and its management. We suggest that uncertainty is a nested concept which is subject to a

meta-representational form of knowledge, that is, knowledge about lack of cybersecurity knowledge within the boundaries of the organisation. We argue that although assumptions are essential in navigating uncertainty, they require a continuous calibration to reflect the interaction between non-linear environmental dynamics and the organisational momentum. Erroneous assumptions can be both highly costly and not evident to the management board, especially when supporting a plausible/expected narrative. That is why an adaptive epistemic approach to cybersecurity management is essential.

We also propose that, like cyber vulnerabilities, organisational knowledge is emergent. Cybersecurity-relevant organisational knowledge cannot be described as a sum of knowledge and beliefs of all internal organisational actors, and instead is a function of the structure-mediated interactions between actors, their beliefs and the environment, which serve as a source of adaptation/calibration for further behaviour.

Finally, we argue that a cybersecurity management strategy requires an ability in rigorous formulation and for its continuous adjustment so that it yields a contextually satisfactory result. The central argument put forward in this paper is that to achieve such a result, organisations require an ability to overcome the spectrum of ontological opaqueness and epistemic limitations derived from non-linearity, cognition/agency, social structures and organisational behaviour and technological attributes. The relative manifestation of these limitations is likely to be local, organisation-specific and closely related to the organisation's intellectual capital base, despite their seemingly general nature. However, as cyberspace is an increasingly embedded part of core societal structures, there is a noticeable evolutionary imperative for (organisational cybersecurity) phenomenon-driven approaches to better understand and engage the disruptive behaviour and potential of threats. We argue that a shared interpretation of knowledge is central to the multidisciplinary cohesion needed to support organisational cybersecurity efforts.

Our contribution goes beyond highlighting the potentially tautological claim that knowledge, and therefore intellectual capital, is important for strategy, to propose a context-specific conceptual interpretation which includes the aspects that substantiate the distinct "knowledge problem" imposed by cybersecurity. This presents numerous opportunities for further empirical and conceptual studies, exploring the practical implications of the knowledge-problem lens. Given the emphasis on context-locality, the perspective put forward would benefit from both explorative and comparative case-studies. In addition, the three core components of the knowledge-problem argument should be critically examined in practice. Finally, the prescriptive implications and potential should be explored from the perspective of the dominant constructs/approaches, including cyber risk and resilience management.

While approached as an organisational issue, cybersecurity presents significant externalities for individuals and society at large. In order to support organisations in their efforts, a realistic and comprehensive picture of the adaptive constraints they face is needed. Underpinning expectations of reasonable organisational security investments and efficacy lies a localised ability of making adequate inferences within the strategic context. The local scope of "unknown unknowns" and erroneous representational models underpinning inference serves as a barrier for pursuing contextually adequate defensive measures, to the detriment of both the organisations and their stakeholders. Thus, beyond incentives and penalties, there is a societal imperative of supporting and fostering the organisational means of tackling the knowledge problem.

4.1 Future work

By focussing on the multi-disciplinary nature of cybersecurity, this research has highlighted the importance of a knowledge-based approach to the study of the concept, which represents a novel perspective on the subject. The view of organisational cybersecurity as a "knowledge problem" opens new areas for the study of the concept beyond its technological dimension.

Interdisciplinary research is encouraged based on a systemic, pragmatic interpretation of knowledge as a meaningful dimension of effective cybersecurity management in organisations. In particular, we propose that further research take this perspective as a starting point to study the link between cybersecurity and value creation, mediated by knowledge and intellectual capital. Examples of such research could include: in-depth case studies exploring the conceptualisation and epistemic substrate of organisational cybersecurity management practice; the development of practice-oriented/operational frameworks aimed to assist organisations; and critical analyses of the implications of a knowledge-based interpretation of cybersecurity management. Such contributions would serve to consolidate the theoretical, empirical and methodological foundations of cybersecurity as an enabler of business strategy, addressing the distinctiveness of the challenges that it poses for the growing operational reliance of organisations on intellectual capital.

References

Allen, P. and Boulton, J. (2011), "Complexity and limits to knowledge: the importance of uncertainty", in Allen, P., Maguire, S. and McKelvey, B. (Eds), *The Sage Handbook of Complexity and Management*, Sage Publications, London, pp. 164-181.

Allen, P.M., Strathern, M. and Baldwin, J.S. (2007), "Complexity and the limits to learning", *Journal of Evolutionary Economics*, Vol. 17 No. 4, pp. 401-431.

Arend, R.J. and Bromiley, P. (2009), "Assessing the dynamic capabilities view: spare change, everyone?", *Strategic Organization*, Vol. 7 No. 1, pp. 75-90.

Baraniuk, C. (2015), "Ashley Madison: 'Suicides' over website hack [online]", available at: www.bbc.co.uk/news/technology-34044506 (accessed 24 May 2018).

Benbya, H. and McKelvey, B. (2006a), "Toward a complexity theory of information systems development", *Information Technology & People*, Vol. 19 No. 1, pp. 12-34.

Benbya, H. and McKelvey, B. (2006b), "Using coevolutionary and complexity theories to improve is alignment: a multi-level approach", *Journal of Information Technology*, Vol. 21 No. 4, pp. 284-298.

Bier, V.M., Cox, L.A. and Azaiez, M.N. (2008), "Why both game theory and reliability theory are important in defending infrastructure against intelligent attacks", in Bier, V.M. and Azaiez, M.N. (Eds), *Game Theoretic Risk Analysis of Security Threats. International Series in Operations Research & Management Science*, Vol. 128, Springer US, Boston, MA, pp. 1-11.

Boisot, M. (2011), "Knowledge management and complexity", in Allen, P., Maguire, S. and McKelvey, B. (Eds), *The Sage Handbook of Complexity and Management*, Sage Publications, London, pp. 436-453.

Brown, J.S. and Duguid, P. (2001), "Knowledge and organization: a social-practice perspective", *Organization Science*, Vol. 12 No. 2, pp. 198-213.

Clarke, D.S. Jr (1989), *Rational Acceptance and Purpose: An Outline of a Prgamatist Epistemology*, Rowman & Littlefield, Totowa, NJ.

Cox, L.A.T. Jr (2012), "Confronting deep uncertainties in risk analysis", *Risk Analysis*, Vol. 32 No. 10, pp. 1607-1629.

Curado, C. and Bontis, N. (2006), "The knowledge-based view of the firm and its theoretical precursor", *International Journal of Learning and Intellectual Capital*, Vol. 3 No. 4, pp. 367-381.

Davenport, T.H. (2015), "Whatever happened to knowledge management" (online), available at: https://blogs.wsj.com/cio/2015/06/24/whatever-happened-to-knowledge-management/ (accessed 24 May 2018).

Dumay, J. (2013), "The third stage of IC: towards a new IC future and beyond", *Journal of Intellectual Capital*, Vol. 14 No. 1, pp. 5-9.

Dumay, J. (2016), "A critical reflection on the future of intellectual capital: from reporting to disclosure", *Journal of Intellectual Capital*, Vol. 17 No. 1, pp. 168-184.

Dumay, J. and Garanina, T. (2013), "Intellectual capital research: a critical examination of the third stage", *Journal of Intellectual Capital*, Vol. 14 No. 1, pp. 10-25.

Edvardsson, I.R. (2009), "Is knowledge management losing Ground&Quest; developments among icelandic SMEs", *Knowledge Management Research & Practice*, Vol. 7 No. 1, pp. 91-99.

Eisenhardt, K.M. and Martin, J.A. (2000), "Dynamic capabilities: what are they?", *Strategic Management Journal*, Vol. 21 Nos 10-11, pp. 1105-1121.

European Commission (2013), "EU Cybersecurity plan to protect open internet and online freedom and opportunity – cyber security strategy and proposal for a directive" (online), available at: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security (accessed 24 May 2018).

Franke, U. and Brynielsson, J. (2014), "Cyber situational awareness – a systematic review of the literature", *Computers & Security*, Vol. 46 No. C, pp. 18-31.

Gal-Or, E. and Ghose, A. (2005), "The economic incentives for sharing security information", *Information Systems Research*, Vol. 16 No. 2, pp. 186-208.

Gershenson, C. (2013), "The implications of interactions for science and philosophy", *Foundations of Science*, Vol. 18 No. 4, pp. 781-790.

Gigerenzer, G. (1996), "On narrow norms and vague heuristics: a reply to Kahneman and Tversky", *Psychological Review*, Vol. 103 No. 3, pp. 592-596.

Gigerenzer, G. and Brighton, H. (2009), "Homo heuristicus: why biased minds make better inferences", *Topics in Cognitive Science*, Vol. 1 No. 1, pp. 107-143.

Gould, S.J. and Vrba, E.S. (1982), "Exaptation – a missing term in the science of form", *Paleobiology*, Vol. 8 No. 1, pp. 4-15.

Greenberg, A. (2012), "Cybersecurity Bill's Backers cite antivirus firms' bogus cybercrime stats" (online), available at: www.forbes.com/sites/andygreenberg/2012/08/02/cybersecurity-bills-backers-cite-antivirus-firms-bogus-cybercrime-stats/ (accessed 24 May 2018).

Guthrie, J., Ricceri, F. and Dumay, J. (2012), "Reflections and projections: a decade of intellectual capital accounting research", *The British Accounting Review*, Vol. 44 No. 2, pp. 68-82.

Guzman, G.A.C. and Wilson, J. (2005), "The 'Soft' dimension of organizational knowledge transfer", *Journal of Knowledge Management*, Vol. 9 No. 2, pp. 59-74.

Haimes, Y.Y. (2011), "On the complex quantification of risk: systems-based perspective on terrorism", *Risk Analysis*, Vol. 31 No. 8, pp. 1175-1186.

Haimes, Y.Y. (2012), "Systems-based guiding principles for risk modeling, planning, assessment, management, and communication", *Risk Analysis*, Vol. 32 No. 9, pp. 1451-1467.

Holling, C.S. (2001), "Understanding the complexity of economic, ecological, and social systems", *Ecosystems*, Vol. 4 No. 5, pp. 390-405.

Ibrahim, F. and Reid, V. (2010), "Unpacking knowledge management: management fad or real business practice?", *Enterprise Risk Management*, Vol. 2 No. 1, pp. 24-38.

Julisch, K. (2013), "Understanding and overcoming cyber security anti-patterns", *Computer Networks*, Vol. 57 No. 10, pp. 2206-2211.

Kahneman, D. and Frederick, S. (2002), "Representativeness revisited: attribute substitution in intuitive judgment", in Gilovich, T., Griffin, D. and Kahneman, D. (Eds), *Heuristics and Biases*, Cambridge University Press, Cambridge, pp. 49-81.

Kaiser, R. (2015), "The birth of cyberwar", *Political Geography*, Vol. 46 No. C, pp. 11-20.

Kianto, A., Ritala, P., Spender, J.-C. and Vanhala, M. (2014), "The interaction of intellectual capital assets and knowledge management practices in organizational value creation", *Journal of Intellectual Capital*, Vol. 15 No. 3, pp. 362-375.

Kraemer, S., Carayon, P. and Clem, J. (2009), "Human and organizational factors in computer and information security: pathways to vulnerabilities", *Computers & Security*, Vol. 28 No. 7, pp. 509-520.

Kraemer-Mbula, E., Tang, P. and Rush, H. (2013), "The cybercrime ecosystem: online innovation in the shadows?", *Future-Oriented Technology Analysis*, Vol. 80 No. 3, pp. 541-555.

Kuehl, D.T. (2009), "From cyberspace to cyberpower: defining the problem", in Kramer, F.D., Starr, S.H. and Wentz, L. (Eds), *Cyberpower and National Security*, 1st ed., Potomac Books, Inc, Dulles, VA, pp. 24-42.

Laland, K.N., Odling-Smee, J. and Feldman, M.W. (2000), "Niche construction, biological evolution, and cultural change", *Behavioral and Brain Sciences*, Vol. 23 No. 1, pp. 131-146.

McKelvey, B. (2001), "What is complexity science?", *Emergence*, Vol. 3 No. 1, pp. 137-157.

Manson, S.M. (2001), "Simplifying complexity: a review of complexity theory", *Geoforum*, Vol. 32 No. 3, pp. 405-414.

March, J.G. (2006), "Rationality, foolishness, and adaptive intelligence", *Strategic Management Journal*, Vol. 27 No. 3, pp. 201-214.

Mercier, H. and Sperber, D. (2011), "Why do humans reason? Arguments for an argumentative theory", *Behavioral and Brain Sciences*, Vol. 34 No. 2, pp. 57-74.

Mousavi, S. and Gigerenzer, G. (2014), "Risk, uncertainty, and heuristics", *Journal of Business Research*, Vol. 67 No. 8, pp. 1671-1678.

Neef, D. (2005), "Managing corporate risk through better knowledge management", *The Learning Organization*, Vol. 12 No. 2, pp. 112-124.

Nonaka, I. and Peltokorpi, V. (2006), "Objectivity and subjectivity in knowledge management: a review of 20 top articles", *Knowledge and Process Management*, Vol. 13 No. 2, pp. 73-82.

Osbourne, C. (2015), "Most companies take over six months to detect data breaches" (online), available at: www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/ (accessed 24 May 2018).

Peters, K., Maruster, L. and Jorna, R.J. (2010), "Knowledge claim evaluation: a fundamental issue for knowledge management", *Journal of Knowledge Management*, Vol. 14 No. 2, pp. 243-257.

Pfleeger, S.L. and Caputo, D.D. (2012), "Leveraging behavioral science to mitigate cyber security risk", *Computers & Security*, Vol. 31 No. 4, pp. 597-611.

Phister, P.W. (2010), "Cyberspace: the ultimate complex adaptive system", *The International C2 Journal*, Vol. 4, pp. 1-30.

Popper, K. (1978), "Three worlds", *The Tanner Lecture on Human Values*, The University of Michigan, Ann Arbor, MI, pp. 143-167.

Popper, K. (2005), *The Logic of Scientific Discovery*, Routledge, London.

Powell, T.C. (2002), "The philosophy of strategy", *Strategic Management Journal*, Vol. 23 No. 9, pp. 873-880.

Proctor, J.D. (1998), "The social construction of nature: relativist accusations, pragmatist and critical realist responses", *Annals of the Association of American Geographers*, Vol. 88 No. 3, pp. 352-376.

Ragab, A.F.M. and Arisha, A. (2013), "Knowledge management and measurement: a critical review", *Journal of Knowledge Management*, Vol. 17 No. 6, pp. 873-901.

Reece, R.P. and Stahl, B.C. (2015), "The professionalisation of information security: perspectives of UK practitioners", *Computers & Security*, Vol. 48 No. C, pp. 182-195.

Rickles, D., Hawe, P. and Shiell, A. (2007), "A simple guide to chaos and complexity", *Journal of Epidemiology & Community Health*, Vol. 61 No. 11, pp. 933-937.

Rid, T. and Buchanan, B. (2014), "Attributing cyber attacks", *Journal of Strategic Studies*, Vol. 38 Nos 1-2, pp. 4-37.

Romanosky, S. (2016), "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, Vol. 2 No. 2, pp. 1-15.

Sharma, S. and Dhillon, G. (2009), "IS risk analysis: a chaos theoretic perspective", *Issues in Information Systems*, Vol. 10 No. 2, pp. 552-560.

Shedden, P., Scheepers, R., Smith, W. and Ahmad, A. (2011), "Incorporating a knowledge perspective into security risk assessments", *VINE*, Vol. 41 No. 2, pp. 152-166.

Slovic, P., Peters, E., Finucane, M.L. and MacGregor, D.G. (2005), "Affect, risk, and decision making", *Health Psychology*, Vol. 24 No. 4, pp. S35-S40.

Sperber, D. and Mercier, H. (2012), "Reasoning as a social competence", in Landemore, H. and Elster, J. (Eds), *Principles and Mechanisms*, Cambridge University Press, Cambridge, pp. 368-392.

Thomas, K., Yuxing, D., David, H., Elie, W. and Grier, B.C. (2015), "Framing dependencies introduced by underground commoditization", *Proceedings of the Fourteenth Workshop on the Economics of Information Security (WEIS)*, *Delft*, *June*.

Tisdale, S.M. (2015), "Cybersecurity: challenges from a systems complexity knowledge management and business intelligence perspective", *Issues in Information Systems*, Vol. 16 No. 3, pp. 191-198.

Tversky, A. and Kahneman, D. (1974), "Judgment under uncertainty: heuristics and biases", *Science*, Vol. 185 No. 4157, pp. 1124-1131.

UK Government (2009), "Cyber security strategy of the United Kingdom" (online), available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf (accessed 24 May 2018).

UK Government (2011), "The UK Cyber security strategy: protecting and promoting the UK in a digital world" (online), available at: www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (accessed 24 May 2018).

White House (2015), "Executive order – promoting private sector cybersecurity information sharing" (online), available at: https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari (accessed 24 May 2018).

Wilson, T.D. (2002), "The nonsense of 'Knowledge Management' ", *Information Research*, Vol. 8 No. 1.

Zahra, S.A. and George, G. (2002), "Absorptive capacity: a review, reconceptualization, and extension", *The Academy of Management Review*, Vol. 27 No. 2, pp. 185-203.

Zetter, K. (2016), "Inside the cunning, unprecedented hack of Ukraine's power grid" (online), available at: www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (accessed 24 May 2018).

Zhao, Y., Lu, Y. and Wang, X. (2013), "Organizational unlearning and organizational relearning: a dynamic process of knowledge management", *Journal of Knowledge Management*, Vol. 17 No. 6, pp. 902-912.

Ziv, A. (1993), "Information sharing in oligopoly: the truth-telling problem", *The RAND Journal of Economics*, Vol. 24 No. 3, pp. 455-465.

Further reading

La Torre, M., Dumay, J. and Rea, M.A. (2018), "Breaching intellectual capital: critical reflections on Big Data security", *Meditari Accountancy Research*, Vol. 26 No. 3, pp. 463-482.

Merali, Y., Papadopoulos, T. and Nadkarni, T. (2012), "Information systems strategy: past, present, future?", *Journal of Strategic Information Systems*, Vol. 21 No. 2, pp. 125-153.

About the authors

Mark Paul Sallos completed his PhD Degree on the subject of Cybersecurity Management at Coventry University. Mark's work focusses on exploring the knowledge dimension of cybersecurity and its management in organisations and society. He has experience on the application of qualitative and quantitative research methods in this field.

Alexeis Garcia-Perez is Reader in Cyber Security Management at the Research Centre for Business in Society of Coventry University (UK) and Visiting Research Scholar at Georgetown University (USA). His socio-technical understanding of information systems has allowed Alexeis's research to focus on the wider challenges of data, information and knowledge management in organisations and society, leading research and teaching on these subjects in the UK and other countries. Alexeis Garcia-Perez can be contacted at: ab1258@coventry.ac.uk

Denise Bedford is Adjunct Professor at Georgetown University's Communication Culture and Technology program, Adjunct Faculty at the Schulich School of Business, York University, Visiting Scholar at Coventry University, and Distinguished Practitioner and Virtual Fellow with the US Department of State. Her current research interests include knowledge architectures and knowledge engineering, knowledge economies and knowledge cities, intellectual capital management and knowledge sharing behaviours.

Beatrice Orlando is Adjunct Professor of Strategies for Business Growth at Sapienza University and of Business Management at UNINT, Rome. Her current research focus is entrepreneurship and innovation, with research interests that range from innovation adoption and open innovation, to behavioural strategy of the firm, diversification, organisational slack and firms' decision making.