Original Article

Breaking bad? In search of a (softer) systems view of security ergonomics

Denis Fischbacher-Smith
Adam Smith Business School, University of Glasgow, Glasgow, E12 8QQ, UK.

Abstract A series of terrorist attacks in late 2014 and early 2015 prompted the head of the UK's Security Service to comment on the need to improve the information flows available to the service in order to deal with the emerging task demands that it faces. The comments highlighted the tensions that have been created in the post-Snowden revelations around domestic surveillance and intelligence gathering and these concerns span both public and private sector organisations. The intervention by the head of MI5 raises a series of questions about the design of security organisations and their function, and does so within a wider systems context, where changes in the environment require corresponding changes in the core processes and functions of the organisation. This is a central domain of security ergonomics and the manner in which an organisation can frame its response to an ever more complex threat matrix is the main purpose of this article. The question becomes one of how one might 'design' such a high performing organisation and especially one that can satisfy the zero-failure mandate that is often required of the security function. The argument presented here is that those organisations that see security as a 'bolt-on' function to existing organisational activities will invariably fail to capture the wider strategic dynamics of threat-response interactions and, more significantly, the role that other organisational activities can play in shaping that process. This article approaches the question from the perspective of two related bodies of research – Soft Systems Methodology and Ergonomics/Human Factors.

Security Journal (2016) **29,** 5–22. doi:10.1057/sj.2015.41

Keywords: security ergonomics; soft systems methodology; organisational design; human factors; socio-technical systems

The online version of this article is available Open Access

Introduction

> My sharpest concern as Director General of MI5 is the growing gap between the increasingly challenging threat and the decreasing availability of capabilities to address it (Parker, 2015)

The quote from Parker, the Director General of MI5, highlights the core challenge facing the provision of a security function in modern organisations (and especially state-based security institutions), namely to ensure that the capabilities of the organisation match the ever-changing task demands that are imposed upon it. These threats currently include: the shift to mass casualty suicide terrorism (especially where no warnings are given of the attack) (Bowen, 2004; Fischbacher-Smith *et al*, 2010); the increasing threats from cyberattacks carried out by organised criminal gangs and state-actors (Choo and Smith, 2008; Farwell and Rohozinski, 2011; Collins and McCombie, 2012); the increased use of social media to recruit and train hostile actors; and the threats posed to those critical infrastructures upon which modern societies depend (Boin and Smith, 2006). These threats have all increased the task complexity associated with intelligence gathering and the protection of both organisations and nation-states. If these security processes fail, then it is highly likely that the system will 'fail to danger' and in a way that will have severe consequences. This process – essentially one of 'breaking bad[1], in which relatively small failures have potentially disproportionality catastrophic consequences – represents a core problem facing the provision of a security function. Essentially, the security function seeks to prevent malicious attacks at the same time that the hostile attackers seek to by-pass security controls. Against this background, a key question is how one might 'design' an adaptive, high performing organisation that can satisfy the zero-failure mandate that is often required of the security function. The aim in this article is to consider the implications of such a systems-based approach for security, with a particular focus on the generation of strategic errors in the design phase of developing security processes.

This article takes a strategic perspective to the design of the security workspace and incorporates a systems ergonomics approach into that discussion. It seeks to develop a series of frameworks that can be used to consider the task demands facing security organisations and highlights some of the challenges that are inherent in framing security within an organisational management paradigm. In particular, Cherns' (1987) principles for the analysis of systems design are presented as a means of highlighting the potential areas of conflict that can exist in developing a high-performing security function. The arguments presented here consider the provision of security from a more holistic perspective and highlight the nature of task complexity and the challenges that it generates.

The main argument presented here is that organisations that see security as a 'bolt-on' function to existing organisational activities will invariably fail to capture the strategic dynamics of threat-response interactions and, more significantly, the role that other organisational activities can play in that process. This article approaches the question from the perspective of two related bodies of research – Soft Systems Methodology (SSM) and Ergonomics/Human Factors (E/HF). In particular, it seeks to frame the problem space that is generated by a zero-failure mandate by using a SSM approach to structure the problem (Checkland, 1985a, b, 1989; Checkland and Scholes, 1990). It develops this by considering Cherns' framework for the design of socio-technical systems and contextualising this discussion in the wider E/HF literature. E/HF also has considerable potential to help frame the security problems from a more holistic perspective and also to avoid the organisational and agency stovepiping that can lead to fractures in controls, such as those present during the September 11th attacks. As the security function has HF as a core, determining element of its activities, then clearly E/HF has the ability to speak to the relationships between design, the potential for error and the generation of vulnerabilities.

Designing a Security System From a Systems Perspective

> If the intelligence community is interested in real improvement, it should begin with a focus on process, not structure and function (Clark, 2013, p. xvi)

Designing an effective security system from first principles requires an organisation to ensure that its overall strategic and security goals are aligned in order to prevent any incompatibility between them. Security, along with risk management, is essentially a strategic process rather than simply an operational one. It is also an activity where the design of its core processes needs to be undertaken from a holistic (systems) perspective.

A systems approach is based on the view that the whole is greater than the sum of the parts (Reason, 1995; Jackson, 2000). As such, it seeks to frame the nature of the problems in a way that recognises how changes in one part of the system can have wider implications for organisational performance by destabilising control and performance measures elsewhere (Smith, 2005). Defining the nature of the problem, and the processes needed to address the associated task demands, is seen as the most important step in ensuring the effective performance of the system. This holistic perspective contrasts with the reductionist approach that often prevails within the analysis of complex phenomena. Recent research has argued that: 'it is the whole that determines the behavior of the parts' (Capra and Luisi, 2014, p. 73) and this highlights the importance of adopting a systems approach. In essence, a systems-based approach highlights the importance of both the wider characteristics of the organisational processes and the nature of the environment in which the system is contextualised. This provides a means of shaping performance and effectiveness at different levels of granularity. As a first step in this process, it is important to define what is meant by the nature of the system, especially within an organisational setting, and in doing so also to identify some of the main parameters of the system being considered.

For our present purposes, we will adopt the following definition of a system:

> a system is a set of interrelated elements which function together as an entity embedded in an environment. The last condition above assumes that the system is open to some external environment. In effect, the distinction of where the system proper ends and the environment begins is arbitrary. A natural delimitation occurs only if a system is completely closed within itself (Scheidegger, 1992, pp. 213–214).

This highlights one of the core challenges facing organisational security, namely the permeable nature of the system-environment boundary. Many of the present security challenges facing organisations arise out of the nature of those boundary conditions and the difficulties that managers have in controlling that interface. The very nature of modern organisations (that is, open, accessible and connected) creates potential vulnerabilities through the interactions between people, technologies, politics and the economic structures that serve to determine organisational effectiveness (Turner, 1994; Tsoukas, 1999; Hodge and Coronado, 2007). Thus, any system has elements that interact together and this has the effect of creating emergent properties that were not initially considered in the design of the organisation's defences and operating protocols. The result is the generation of potential vulnerabilities in the systems defences that can serve to erode the capabilities of any contingency planning process (Smith, 2005).

Within this broad context there are several aspects of a systems approach that have relevance to this discussion and which need to be highlighted. Jackson (2000), for example, argues that a systems approach has three key attributes:

- That a systems approach is holistic rather than reductionist and that this holistic perspective allows for the greater consideration of emergent properties in any analysis

(Jackson, 2000). There is also some acknowledgement that changing one part of the system will have consequences elsewhere (Rockart and Scott-Morton, 1984; Galbraith, 2002; Lichtenstein and Plowman, 2009).
- That an advantage of a systems approach can be found in its interdisciplinary and inclusive nature (Jackson, 2000) and that it invariably has a focus on real-world problems that are set in what Wilson (2014) terms 'ergonomics in the wild' (p. 7).
- These systems are invariably structured according to the cognitive frameworks and associated knowledge structures of humans (Jackson, 2000) and therefore the strategies and decisions that we take are shaped by these worldviews (Checkland, 1989).

For many of these conceptualisations of the system, a common feature is that the core beliefs, values and assumptions of key actors within the organisation lie at the heart of decision making and strategy development (Checkland, 1989; Mitroff *et al*, 1989; Checkland and Scholes, 1990; Pauchant and Mitroff, 1992; Johnson, 1992) and are often seen as part of the organisation's wider cultural web in which the mental models of managers are important in shaping their decision-making behaviours (Johnson, 1992; Hodgkinson and Johnson, 1994). For example, Hollnagel (2001) has highlighted the importance of worldviews in conceptualising a cognitive approach to ergonomics stating that:

> … the defining characteristic of a cognitive system – and, therefore, also of a joint cognitive system – is its ability to maintain control of what it does. Control is, furthermore, not an isolated property of any identifiable part or component of a joint cognitive system, but rather an emergent property of the system as such (Hollnagel, 2001, p. 312).

Hollnagel (2001, p. 314) also argues that as control is dynamic, 'it requires a way to think of and represent the dynamics and the forces of cognition, both how it can work and how it can fail'. Given the importance of control processes to the performance of a security organisation then it is clear that the core beliefs, values, and assumptions of key decision-makers need to be articulated and incorporated into the design and maintenance of the systems core processes.

From an early conceptualisation of systems ergonomics, a system can also be seen as a set of interacting components where the interactions that take place involve the transfer of information and energy (Singleton, 1967a). The centrality of humans in this process led Singleton (1972) to argue that the application of human factors from a systems perspective is an essential element in seeking to deal with the consequence of errors in an evermore complex setting. Singleton (1967b) also highlighted three elements of a systems' approach that are relevant to a discussion of security ergonomics:

- the role of functional characteristics and their interactions in shaping systems performance
- the role and importance of human actors as an integral part of the system
- the ways in which decisions are taken around process and organisational design are categorised and ordered as a means of ensuring that the goals of the system are consistently borne in mind during any changes made to other systems elements (Singleton, 1967a, b).

Each of these factors has relevance to debates around the design of security functions within organisations. Put another way, security needs to address a number of core questions:

- What is the focus and purpose of the system and does this purpose vary in the perceptions of the key actors involved?
- What is the potential for human error to arise within a system that is ever more complex and how significant are the consequences of such errors?
- How do systems operators ensure that any moves away from the system's 'designed-for' state are recognised and the potential for emergent conditions to erode controls is acknowledged and managed?

There are a number of other important aspects of systems thinking including the shift in focus from objects within the system to the relationships between those objects and the processes that take place within these connecting elements (Capra, 1985; Capra and Luisi, 2014). Thus, the mapping of relationships and interconnections within the system can also be deemed to be important, especially because it also gives rise to emergent conditions that arise out these relationships. A logical extension of this argument is that where the implemented processes and structures do not reflect the underlying task demands then there will be considerable potential for the generation of negative emergent conditions that could prove damaging (Capra and Luisi, 2014).

A systems approach also concerns the manner in which knowledge is constructed, transferred and operationised within connected networks (Capra, 1985; Clark, 2013). In particular, there is a shift away from the notion of a universally shared objective form of knowledge and a move towards a more epistemic way of thinking in which the questions asked of the system are important in framing the nature of understanding (Capra and Luisi, 2014). Once again, this places the assumptions and beliefs that the observers have about the world – their worldviews and sensemaking processes (Checkland, 1989; Checkland and Scholes, 1990; Weick, 1995; Weick, 2001) – as central elements for constructing and managing the system. This also raises the potential for a dislocation in the ways that emergent conditions are recognised and acted upon. What then are the opportunities that exist for framing the processes around security and how can we recognise the central role that human actors play in the process? The remainder of this paper considers an adapted version of Cherns' framework for socio-technical systems as a means of contextualising the importance of a systems' approach to security ergonomics.

Framing a System for Security

Humans invariably play a significant role in the provision of security where they can be considered as occupying a number of roles – attackers, defenders and victims – as well as acting as the designers and managers of the wider system. We can add to this the categorisation developed by Checkland's Soft Systems Methodology, where the human elements of the system are seen in terms of those who make the system work, those who own the system, and those who are the chief beneficiaries of the outputs of the system (Checkland, 1985a; Checkland, 1989; Checkland and Scholes, 1990). Each of these groups – actors, owners and customers – have a particular set of worldviews (weltanshung) that serve to shape the ways in which they make sense of the world around them (Checkland, 1989; Checkland and Scholes, 1990). These worldviews reflect their core beliefs, values and assumptions about the nature of the system and the various transformations that take place within it (Checkland, 1989; Weick, 1995; Weick, 2001). These groups of actors will require the competence to undertake their core tasks (as attacker or defender), display the commitment to make the function work (or, in the case of attackers, make it fail by by-passing systems defences), and will also require a level of awareness around the performance (transformations) of the system. These three issues (competence, commitment and awareness) were identified by Reason (1993a) as core source types within the formation of an organisational culture and which are seen to shape decision-making processes. While Reason developed these source types in relation to issues around safety, it is our contention here that they also apply to the provision of security. In making this link, we should note that security is required to embrace even more uncertainty than many other risk and safety issues because of the role that intentional actions play in the generation of harm. As such, it can be argued that these source types assume a greater importance within a security context because of the need to encompass this additional uncertainty.

We can place these source types at the core of our initial framework for a systems' approach to security so that they interact with the core beliefs, values and assumptions held by key actors, owners and customers within the organisation. This is shown in Figure 1. Consensus around these issues will also be important in achieving the strategic goals set for security and minimising conflict (or lack of consensus) across these three source types in order to prevent fractures within control systems. Any deficiencies in security competence, commitment and awareness may serve to amplify dislocations that exist between the assumptions made about how the function operates in theory and how it works in practice. Criticisms made in the aftermath of the September 11th attacks highlighted the important roles played by differences in perceptions around systems defences, information sharing and the significance of evidence in the performance of security provision across organisational boundaries (Goodman, 2003; Posner, 2003; Kean, 2011; Loftus, 2011). Many of these issues are often seen as intangible prior to a systems failure and as a consequence they often lead to processes associated with the incubation of risk (Turner, 1978; Reason, 1993b; Reason, 1995; Turner, 1994).

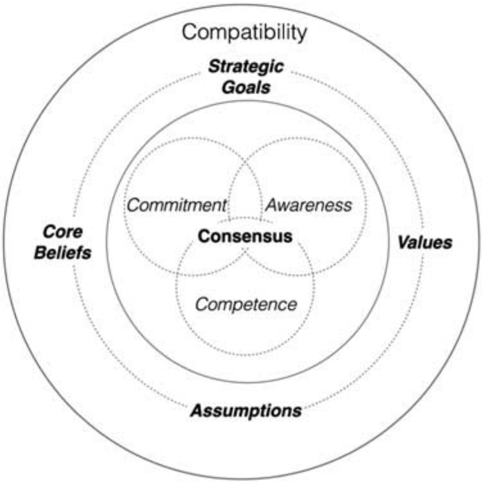

Figure 1: Epsitemic elements of developing a system.

A key factor here concerns the compatibility of these elements within the context of the wider strategic goals set out for the security function and the associated transformation processes that take place elsewhere in the system.

The main elements of Figure 1 provide a means of asking key questions about the ways in which it is possible to frame and evaluate the various elements of the security function within a wider organisational system. A lack of competence, commitment, and awareness around security-related tasks will be reflected in, and influenced by, the core beliefs, values and assumptions held by key actors within the organisation as well as key stakeholders. These processes will then shape the approaches taken to the development and implementation of strategic goals and will also influence the willingness of individuals to engage in processes around change management. The compatibility of these 'hidden' elements with the organisation's strategy represents a first, but crucial stage in the development of its capabilities.

The notion of compatibility also sits at the core of Cherns' (1976, 1987) framework as the first of ten principles for the design of socio-technical systems and it is within this context that the goals are set for the system. It is around the tensions that can exist in relation to compatibility that any potential conflicts between the cultural core of the organisation and the views of its principal stakeholders (that is, actors, customers and owners) needs to be addressed:

> we must recognize that design is an arena for conflict. It has to satisfy an array of objectives, each represented by some organizational element: the way in which this conflict is managed and used to yield positive results sets the pattern for the handling of subsequent conflicts (Cherns, 1987, p. 154).

The potential for conflict can be seen, therefore, to sit at the core of the organisational design process and can mitigate against the creation of a culture that supports a zero-failure mandate. If there is no agreement or core compatibility around Reason's three source types, then it is likely that the potential for conflict will be high. Similarly, if the core beliefs, values and assumptions of the key decision makers and other actors in the organisation are not compatible, but these tensions remain hidden, then there is the potential for the incubation of crisis to occur as a result (Reason, 1995; Turner, 1976; Reason, 1997). For these reasons, the elements outlined in Figure 1 form the basis of our framing of Cherns' (1987) wider principles and this revised framework is shown in Figure 2. Figure 2 allows us to consider how the notion of compatibility, where we have situated Reason's source types, can impact on the rest of Cherns' principles for the design of socio-technical systems. We can now consider the remaining principles in turn.

Minimum critical specification

Building on the core issue of compatibility, a significant issue within any systems design process concerns the notion of a minimum critical specification for performance. Cherns (1987) argues that organisations typically set this specification in terms of either a negative position (that is, restricting the performance criteria to those issues that are absolutely essential) or a positive one (that is, where the various task requirements associated with

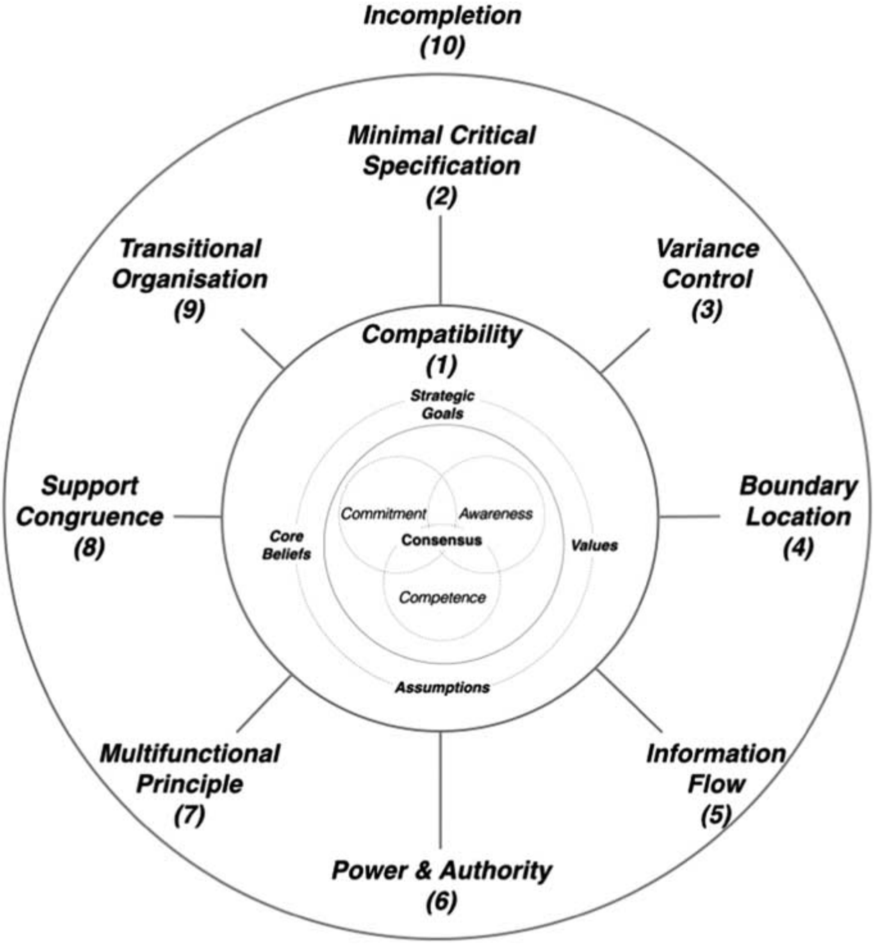

Figure 2: Cherns' principles of the design of sociotechnical systems.
Source: based on information in Cherns (1987).

managing the system are identified completely). From a security perspective, this raises some interesting challenges.

The provision of security is a complex process because of the multiple interactions that take place at both the level of the threat and the organisational defences that are in place to deal with the task demands that those threats generate. Security is also complicated because of the need to generate intelligence around the range of multi-layered threats that an organisation faces, and then to convert that intelligence into actionable knowledge that allows for risks to be identified and managed. Taken together, this complex and complicated nature of security generates variety within the threats that need to be 'managed'. The variety within the threats will require corresponding levels of variety within the control measures put in place to deal with those threats (Ashby, 1958). Reductionist approaches to dealing with the threats will invariably increase the potential for emergent conditions by failing to consider how localised changes will move the security process away from its 'designed-for' state without taking account of these changes on the performance of the system as a whole. This creates challenges for security management, especially where the organisation has a 'zero-failure mission' (Hagin *et al*, 2014).

Another reason why zero-failures may be problematic is that the performance challenges for security occur in what has been termed a hyper-competitive environment (D'Aveni, 1995, 1998). Here, processes around globalisation generate challenges for controlling security in organisations because of the extent of the organisation's networks and their significance. The extent of an organisation's supply chains and its dependence on key sources of raw materials may make it vulnerable to international conflicts. Closer to home, a dependence on critical infrastructures can also generate vulnerabilities that lie outside of the organisation's control. Given the role of human actors in generating many of these threats, the process can be likened to 'predator-prey' relationships in which the relative fitness of both parties to deal with each other's capabilities will be a determining factor in their ability to achieve their goals. These conflicts occur at different scales and in different locations, thereby requiring the security function to operate optimally at various points in space and time. The result of such competition has generated what has been termed a 'hyper-conflict' environment in which the processes around globalisation have created a threatening context in which organisations operate (Mittelman, 2010, 2011). In turn, this has created a series of security challenges around information management and sharing, the protection of extended supply chains, and a set of problems around personnel checking and insider threats that emerge out of this wider globalisation process. While a global pool of expertise and human resource talent brings obvious benefits to recruiting organisations, it also increases the task requirements around background checking in order to prevent risks from insider threats (Day, 2007; Hershkowitz, 2007; Harber, 2009).

Figure 3 provides a generic illustration of the nature of such a hypercompetitive environment and highlights a range of issues that have implications for security across economic, political, technological and organisational dimensions. The interactions between these elements has the potential to generate the potential for hyper-conflict along with new and emergent threats that the organisation has yet to consider.

Variance control

It is not inconceivable that an organisation charged with providing security will have to deal with a sizable proportion of the issues highlighted in Figure 3. The security function will have to control the variance that exists across its threat environment and ensure that it has the processes in place to deal with the challenges that these threats generate. Variance control is an important factor in ensuring that the defences in place across the organisation are universally robust and that local adaptations have not been allowed to erode their capability. Variance control is also a key element of dealing with the potential for latent conditions (Reason, 1990, 1997) that can allow errors or violations to by-pass organisational controls. The actions of externally generated threats also creates a range of other challenges around information flows, boundary spanning processes and the power to obtain information. These issues form the next three principles outlined by Cherns, namely: boundary location, information flows and power and authority.

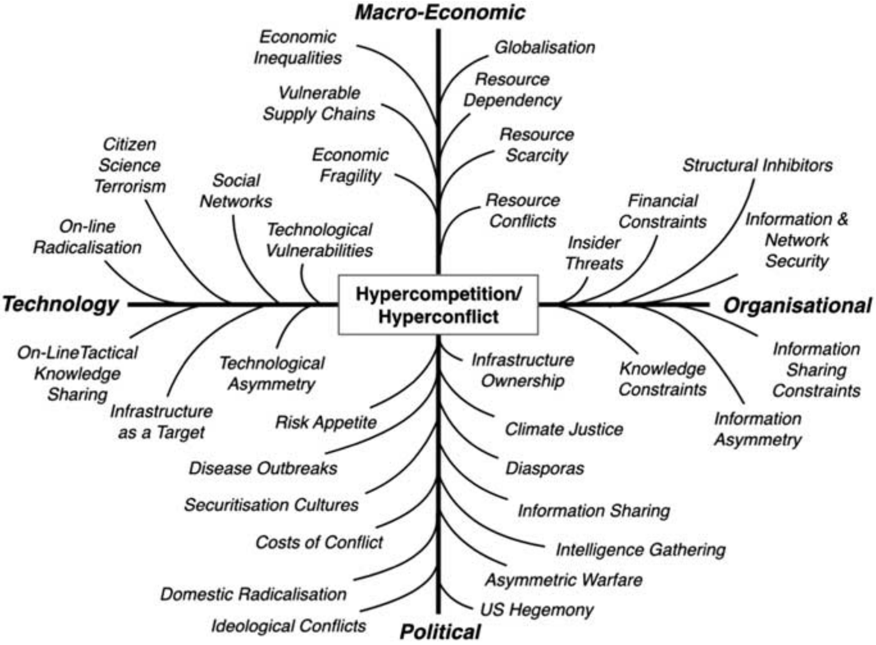

Figure 3: Hyper-competition and hyper-conflict.

Boundary location

Security challenges invariably transcend organisational boundaries and especially within a global, hyper-competitive environment. Boundary location is, therefore, an important element of performance and it can be seen to operate at a range of spatial and functional levels. Operating across geographical boundaries opens up the potential for threats within an organisation's supply chain. This, in turn, transcends multiple legal jurisdictions and requires the organisation to develop effective working relationships with the relevant legal systems involved. The recent hacking of Sony's networks illustrated how the boundaries between the state and organisational provision of security have become increasingly intertwined (see: Michal, 1994). The scale and complexity of these interactions also generates the potential for emergence as well as a requirement to improve information flows and intelligence gathering capabilities. Increasingly, this needs to be done across public–private sector boundaries, although this generates problems around information sharing. In a globalised environment, the spatial dynamics for the provision of security is problematic, especially where the threats are generated by non-state actors and because of the increasing interdependence of the state on trans-national corporations (Mittelman, 2010). As a consequence, security theory is no longer as dominated by the focus on international relations as it has been in the past and this also generates challenges around the conceptualisation of security. One effect of this broadening of the boundaries of security theory has been to increase the demands around information processing. It is increasingly apparent that both public and private sector information sources are important in dealing with the task demands associated with the provision of security, especially around the protection of the privatised utilities (Boin and Smith, 2006).

Information flows

Information flows and the processes by which information is converted into actionable intelligence and knowledge are a major challenge for organisations but this is especially important where the provision of security is a primary task (Waltz, 2003). While many seem content to share a great deal of personal information through social media, they are unhappy at attempts by the state to collect metadata in pursuit of a security policy agenda that became public knowledge as a result of the Snowden revelations (Etzioni, 2015; Friedersdorf, 2014; Greenwald, 2014). Similarly, revelations around 'enhanced interrogations' after the September 11th attacks have also been heavily criticised, despite the horrific nature of the attacks themselves, especially as the actionable intelligence that was derived remains contentious (Halpern *et al*, 2008; Schiemann, 2012; US Senate Select Committee on Intelligence, 2012). Supporters of enhanced interrogation and increased surveillance invariably argue that we are dealing with a set of threat actors that do not conform to accepted social norms and therefore extraordinary measures are needed by the state to deal with the task demands of that threat: in essence, a process that could be seen as akin to an application of the Law of Requisite Variety. Opponents argue that such measures erode the principles of a free, democratic society and that such oppressive measures simply bring us down to the same level as those who would threaten us (Bellamy, 2006; Guiora and Page, 2006).

This political impasse encapsulates the challenge facing security operators dealing with the threats from violent extremists and organised crime. Echoes of this can also be found in debates around intrusive monitoring of employees through social media and email traffic (Hoffman *et al*, 2003; Slovensky and Ross, 2012) and reflects a wider set of concerns around the power of companies and the state.

Power and authority

The ability to use power and authority to shape policy and practice within organisations is often a significant challenge for the security function. Within many organisations, the security function often does not hold a position that allows it to shape, align and influence the overall corporate strategies and goals that are required to deal with the threats. Moving towards the provision of a zero-failure performance standard would require the security function to extend its influence across the various operating divisions of the organisation. This would necessitate the creation of effective processes around communication and information sharing as well as the implementation of an extensive programme of cultural change in some cases. Thus, security would have to move beyond its normal remits – with a focus on detection and prevention of threats – to encompass a cultural change agenda and risk communication mandate. This is likely to prove challenging, especially when working with an extended network of partner organisations. The security function would need to embrace the multi-functional principle that forms the next element in Cherns framework.

Multifunctional principle and support congruence

The multifunctional principle reflects a significant challenge for an organisation as it seeks to adapt to its threats, especially within a diminishing resource base. This invariably leads organisations to increase the utilisation of existing resources, thereby increasing the task demands on staff who assume multi-functional roles as a consequence. This also relates to the issue of support congruence, where security functions within the organisation need to be supported along with the processes by which the performance of those functions is measured and rewarded. This also relates to the importance of expertise within those processes that support the security function. Within a globalised environment, these challenges extend over extended spatial scales and across multiple cultures. As a result, the risk of information loss is considerably heightened unless the supporting elements of the system are adequately resourced.

Transnational organisation and the incompletion principle

The last two elements in Chern's framework relate to the processes of managing change and dealing with the task demands associated with emergent conditions. The first of these is the notion of the transitional organisation. Here, the organisation is in a process of continuous change (or adaptation) and these processes can have an impact on the performance of organisational defences as the system is moved away from its 'designed-for' state. Changes around the configuration of the system will invariably lead to the creation of emergent conditions and these, in turn, can lead to fractures in controls (Perrow, 1984; Tsoukas, 1999; Smith, 2005; Hodge and Coronado, 2007). Finally, the on-going demand for providing security underpins the incompletion principle. Here the emergent conditions and evolution of the threat matrix facing an organisation will ensure that those threats will always challenge the capabilities of the organisation to contain, identify and neutralise them. The provision of security will always be an incomplete task as threat actors seek to identify and exploit on-going systemic weaknesses.

Against this background, the provision of security needs to take account of the dynamics of the process from a more holistic perspective if it is to be effective. It also needs to account for the motivations of those individuals and groups who threaten the organisation. Given that most, if not all, security threats are generated by intelligent actors (who actively seek to cause harm), then the provision of sufficient controls to deal with the variety in the threats remains a considerable challenge. It requires the organisation to improve its knowledge management processes and to ensure that decision makers recognise the impact that their actions can have on shaping the threats that the organisation faces. Similarly, organisational performance can be seen as a function of task complexity which is generated by the environment in which it operates. Organisational effectiveness, and by implication security performance, is an essentially fragile process and it is a function of the reluctance of many managers to see the double-edge nature of the effectiveness construct and its relationship with failure (Fischbacher-Smith, 2014a, b). Thus, the worldviews that are held by those who 'own' the system are important in determining the design parameters in which the system works (Checkland, 1989; Checkland and Scholes, 1990).

Discussion

Thus far, we have argued a case for a systems-based approach to dealing with organisational security and have set out the framework developed by Cherns as a means of conceptualising the main steps that are needed within such an approach. The framework, developed in

Figure 2 above, also raises some questions about organisational effectiveness and we can now explore those issues in more detail.

One of the core elements of developing an effective security provision concerns the creation of an organisational culture (expressed in terms of Reason's source types) that recognises the limitations that can be embedded within that culture because of a failure to consider the level of consensus around the commitment, competence and awareness of key decision makers. It could also be argued that there will also be a need to surface the core beliefs, values and assumptions that underpin the development of the organisation's strategic goals as this will ensure that key decision makers are fully aware of the basis for the decision. A failure to deliver this core aim will result in the embedding of weaknesses into the design of security processes and structures that is akin to Turner's (1976, 1978, 1994) notion of incubation. As the organisation evolves, it will be necessary to revisit this cultural core to ensure that there is still an effective mapping of these elements against the strategic goals of the organisation.

Building upon this cultural core, the essence of Cherns' framework is based upon a series of interconnected elements that begin with the development of a critical specification for the main processes used to develop security capabilities. It is here that any zero-failure standard would need to be specified and the organisation would also need to ensure that this standard was compatible with the other strategic goals that were in place. Once the standards are established and agreed across the organisation (and its network partners if appropriate) then the organisation needs to be certain that it has established and tested mechanisms for the control of variance within the system. This will be important in developing the parameters of the control systems that are in place and establishing the boundaries of the system over which such controls need to function. Framing the boundaries of the system is an essential element in ensuring that gaps within the control parameters are addressed and this is especially important for organisations that operate across multiple locations. Finally, ensuring effective information flows is also an essential component of an effective security system. This is often problematic for organisations where the information required to achieve a high level of security performance is sensitive and, therefore, not easily shared with others in the organisation's network. In addition, all organisations invariably suffer from constrained information flows (Fischbacher-Smith, 2014a, b), and this is especially problematic when dealing with the identification of early warnings and weak signals that are an essential component of intelligence gathering. Any failures around variance control, boundary location, and information sharing will severely impair the organisation's attempts at developing a zero-failure performance standard. The ability to achieve and maintain effectiveness in this regard is often a function of the power and authority given to security managers to override lapses in performance in other parts of the organisation. Again, this is an organisational characteristic that can change over time, resulting in the erosion of organisational capability.

Figure 4 seeks to contextualise Cherns' elements as part of a wider process around the creation and erosion of organisational effectiveness. The key elements around effectiveness have, at their core, the essential requirement around the compatibility of security goals with the main strategic objectives of the organisation. It is here that the organisation needs to ensure that it achieves consensus around the source types of commitment, awareness and competence. It is only by surfacing the core assumptions, beliefs and values that key actors hold, that assurances can given around the compatibility of security with the wider strategic goals. At the same time, it is important to try and understand the core beliefs, values and

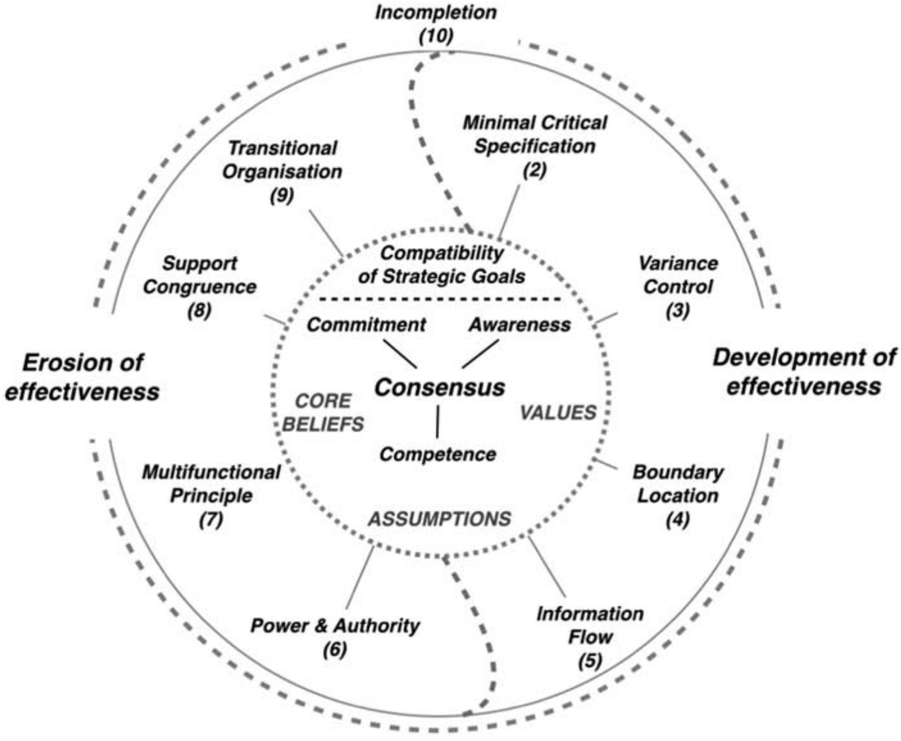

Figure 4: Incorporating effectiveness into the Cherns framework.

assumptions of those hostile actors who are likely to pose a threat to the organisation. The gaps that exist between these two sets of variables will provide the basis for an initial assessment of vulnerabilities within the system. This then allows managers to pay attention to the key elements of the framework (Stages 2–5) that are essential in achieving organisational effectiveness. Each of these elements builds on the platform provided by the previous element. Stages 2 to 5 are, therefore, the essential and non-substitutable elements in the design of effective security processes. A failure in any one of these elements will lead to the potential erosion of the controls that are put in place to deal with threats. These opening stages will, however, only provide a baseline for the development of security capability.

If the security function does not have the power and authority to challenge any incompatibilities within the organisation's strategic goals, or to help change the relative priorities that the organisation has around security, then it will begin to incubate the potential for failure. Similarly, if the security function does not develop the multifunctional capabilities required to deal with a diverse and evolving threat matrix, as well as to ensure that it has the skills and capabilities to promote the security agenda across the organisation, then it will struggle to effect a cultural change process. The multifunctional principle will also require an extensive training programme for staff to develop the capabilities needed to operate within a multi-threat environment. This multifunctional capability is seen as being an essential component for organisations working within a complex environment where the need to adapt to changing task demands is high (Cherns, 1987). Similarly, the need to provide support for the goals of security is also an important element in ensuring that the organisation does not become ineffective. This will invariably require changes to the reward system within the organisation while ensuring that other organisational goals do not undermine the support for a security agenda. A failure to deal with strategic drift within the organisation will ultimately lead to a transitional process that moves the organisation into an ineffective state and which will lead to a failure (as incompletion) of the strategy, thereby requiring the redevelopment of the process from first principles.

The Cherns' framework provides a systematic way of considering the development of an organisation's security strategy and it highlights the importance of a systems approach to dealing with the problems that can arise from security threats. Unless organisations take a holistic and adaptive approach to dealing with the demands of the threat matrix that they face then they will risk creating a set of security processes that fail to deal with those task demands. It is also necessary for the principles set out by Cherns to be constantly reassessed to ensure that the capabilities to deal with evolving threats are in place. While these principles will not guarantee a zero-failure level of performance, it will provide a more systematic way of developing capabilities that provide an organisation with the potential to move ever closer to that goal.

Conclusions

There is little doubt that the provision of security, both within and across organisational networks as well as throughout a range of societal settings, is a complex and complicated task. The complexity of the security task arises from the scale of the threats involved, the manner in which those threats emerge, and the problems that exist in the responses that the organisation makes to contain those threats. The security task is made even more complex because of the nature of the threats that arise from the direct actions of hostile human actors. Unlike most other forms of risk, the majority of security threats are not accidental but are intentional, where the perpetrators of the act seek to by-pass existing control measures to cause a range of harms.

This article has sought to argue the case for a systems ergonomics approach to dealing with the task demands associated with the provision of security and has outlined a process by which it is possible to identify some of the main points of fracture that can be generated by taking a narrow reductionist approach to developing the security function. The article has, at the same time, also outlined some areas where additional research is needed to develop both the theoretical and the practical aspects of security ergonomics in order to deal with the ever-evolving set of threats that organisations face. Perhaps more than any other function within an organisation, security is subject to the transitional and incomplete nature of change that was outlined by Cherns. The constantly evolving threat matrix and the increasingly adaptive nature of hostile actors ensures that a systems approach to this problem is a requirement that organisations ignore at their cost. This creates some highly demanding issues for those involved in the design of security organisations for, as Carayon notes:

> Increasing work system complexity poses unique challenges to the people involved in the design, implementation and maintenance of sociotechnical systems (Carayon, 2006, p. 525).

A systems approach to dealing with security ergonomics can be seen as an effective way of approaching this task complexity because, as Cherns reminds us, taking a piecemeal approach to such issues will invariably lead to problems around those incomplete elements that arise from more reductionist approaches.

Acknowledgements

The work reported in this article was supported by a grant from the EPSRC (EP/G004307/1) on Cargo Screening. The author would like to thank Professor Moira Fischbacher-Smith and Dr Alex Stedmon for comments on an earlier draft of this paper. Thanks are also due to two anonymous reviewers whose comments have also made this a much better article. Invariably, all errors of commission and omission remain those of the author.

Note

[1] The term is a colloquialism used in the South West of the United States, although its origins have been traced back to commentaries on Wall Street activities in 1919. The term was popularised in the United States by the TV series relating to the production of crystal meth.

References

Ashby, W.R. (1958) Requisite variety and its implications for the control of complex systems. *Cybernetica* 1(2): 83–99.

Bellamy, A.J. (2006) No pain, no gain? Torture and ethics in the war on terror. *International Affairs* 82(1): 121–148.

Boin, A. and Smith, D. (2006) Terrorism and critical infrastructures: Implications for public-private crisis management. *Public Money and Management* 26(5): 295–304.

Bowen, W.Q. (2004) Deterrence and asymmetry: Non-state actors and mass casualty terrorism. *Contemporary Security Policy* 25(1): 54–70.

Capra, F. (1985) Criteria of systems thinking. *Futures* 17(5): 475–478.

Capra, F. and Luisi, P.L. (2014) *The Systems View of Life: A Unifying Vision*. Cambridge, UK: Cambridge University Press.

Carayon, P. (2006) Human factors of complex sociotechnical systems. *Applied Ergonomics* 37(4): 525–535.

Checkland, P. (1985a) Achieving 'desirable and feasible' change: An application of soft systems methodology. *The Journal of the Operational Research Society* 36(9): 821–831.

Checkland, P. (1985b) From optimizing to learning: A development of systems thinking for the 1990s. *The Journal of the Operational Research Society* 36(9): 757–767.

Checkland, P. (1989) Soft systems methodology. *Human Systems Management* 8(4): 273–289.

Checkland, P.B. and Scholes, J. (1990) *Soft Systems Methodology in Action*. Chichester, UK: Wiley.

Cherns, A. (1976) The principles of sociotechnical design. *Human Relations* 29(8): 783–792.

Cherns, A. (1987) Principles of sociotechnical design revisited. *Human Relations* 40(3): 153–161.

Choo, K.K. and Smith, R. (2008) Criminal exploitation of online systems by organised crime groups. *Asian Journal of Criminology* 3(1): 37–59.

Clark, R.M. (2013) *Intelligence Analysis. A Target-Centric Approach*. 4th edn. Los Angeles, CA: SAGE/CQ Press.

Collins, S. and McCombie, S. (2012) Stuxnet: The emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism* 7(1): 80–91.

D'Aveni, R.A. (1995) Coping with hypercompetition: Utilizing the new 7S's framework. *The Academy of Management Executive* 9(3): 45–57.

D'Aveni, R.A. (1998) Waking up to the new era of hypercompetition. *The Washington Quarterly* 21(1): 183–195.

Day, M. (2007) Doctors held for bombing attempts, but NHS defends vetting procedures. *British Medical Journal* 335(7609): 9.

Etzioni, A. (2015) NSA: National security vs. individual rights. *Intelligence and National Security* 30(1): 1–37.

Farwell, J.P. and Rohozinski, R. (2011) Stuxnet and the future of cyber war. *Survival* 53(1): 23–40.

Fischbacher-Smith, D. (2014a) The dark side of effectiveness: Risk and crisis as the 'destroyer of worlds'. *Journal of Organizational Effectiveness: People and Performance* 1(4): 338–348.

Fischbacher-Smith, D. (2014b) Organisational ineffectiveness: Environmental shifts and the transition to crisis. *Journal of Organizational Effectiveness: People and Performance* 1(4): 423–446.

Fischbacher-Smith, D., Fischbacher-Smith, M. and BaMaung, D. (2010) Where do we go from here? The evacuation of city centres and the communication of public health risks from extreme events. In: P. Bennett, K. Calman, S. Curtis and D. Fischbacher-Smith (eds.) *Risk Communication and Public Health*. Oxford: Oxford University Press, pp. 97–114.

Friedersdorf, C. (2014) The latest Snowden leak is devastating to NSA defenders. *The Atlantic* 7 July, http://www.theatlantic.com/politics/archive/2014/07/a-devastating-leak-for-edward-snowdens-critics/373991/.

Galbraith, J.R. (2002) Organizing to deliver solutions. *Organizational Dynamics* 31(2): 194–207.

Goodman, M.A. (2003) 9/11: The failure of strategic intelligence. *Intelligence and National Security* 18(4): 59–71.

Greenwald, G. (2014) *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. London: Hamish Hamilton.

Guiora, A.N. and Page, E.M. (2006) Unholy trinity: Intelligence, interrogation and torture. *Case Western Reserve Journal of International Law* 37(2): 427–447.

Hagin, J., Perrelli, T., Gray, D. and Filip, M. (2014) Report from the United States Secret Service Protective Mission Panel to the Secretary of Homeland Security. Washington DC: United States Secret Service Protective Mission Panel.

Halpern, A., Halpern, J. and Doherty, S. (2008) 'Enhanced' interrogation of detainees: Do psychologists and psychiatrists participate? *Philosophy, Ethics, and Humanities in Medicine* 3(1): 1–11.

Harber, J.R. (2009) Unconventional spies: The counterintelligence threat from non-State actors. *International Journal of Intelligence and CounterIntelligence* 22(2): 221–236.

Hershkowitz, M. (2007) The 'insider' threat. *Journal of Police Crisis Negotiations* 7(1): 103–111.

Hodge, B. and Coronado, G. (2007) Understanding change in organizations in a far-from-equilibrium world. *Emergence: Complexity and Organizations* 9(3): 3–15.

Hodgkinson, G.P. and Johnson, G. (1994) Exploring the mental models of competitive strategists: The case for a processual approach. *Journal of Management Studies* 31(4): 525–552.

Hoffman, W.M., Hartman, L.P. and Rowe, M. (2003) You've got mail ... and the boss knows: A survey by the center for business ethics of companies' email and internet monitoring. *Business and Society Review* 108(3): 285–307.

Hollnagel, E. (2001) Extended cognition and the future of ergonomics. *Theoretical Issues in Ergonomics Science* 2(3): 309–315.

Jackson, M.C. (2000) *Systems Approaches to Management*. New York: Kluwer Academic/Plenum Publishers.

Johnson, G. (1992) Managing strategic change: Strategy, culture and action. *Long Range Planning* 25(1): 28–36.

Kean, T. (2011) The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States Washington DC: Government Printing Office.

Lichtenstein, B.B. and Plowman, D.A. (2009) The leadership of emergence: A complex systems leadership theory of emergence at successive organizational levels. *The Leadership Quarterly* 20(4): 617–630.

Loftus, E.F. (2011) Intelligence gathering post-9/11. *American Psychologist* 66(6): 532–541.

Michal, K. (1994) Business counterintelligence and the role of the US intelligence community. *International Journal of Intelligence and Counter Intelligence* 7(4): 413–427.

Mitroff, I.I., Pauchant, T.C., Finney, M. and Pearson, C. (1989) Do (some) organizations cause their own crises? Culture profiles of crisis prone versus crisis prepared organizations. *Industrial Crisis Quarterly* 3(4): 269–283.

Mittelman, J.H. (2010) *Hyper-Conflict. Globalization and Insecurity*. Stanford, CA: Stanford University Press.

Mittelman, J.H. (2011) What drives global security and insecurity? *Global Change, Peace and Security* 23(2): 113–116.

Parker, A. (2015) Terrorism, Technology and Accountability. Address by the Director General of the Security Service, Andrew Parker, to the Royal United Services Institute (RUSI) at Thames House, London, 8 January.

Pauchant, T.C. and Mitroff, I.I. (1992) *Transforming the Crisis-Prone Organization: Preventing Individual Organizational and Environmental Tragedies*. San Fransisco, CA: Jossey-Bass Publishers.

Perrow, C. (1984) *Normal Accidents*. New York: Basic Books.

Posner, G. (2003) *Why America Slept: The Failure to Prevent 9/11*. New York: Random House.

Reason, J.T. (1990) *Human Error*. Oxford: Oxford University Press.

Reason, J.T. (1993a) Managing the management of risk: New approaches to organisational safety. In: B. Wilpert and T. Qvale (eds.) *Reliability and Safety in Hazardous Work Systems: Approaches to Analysis and Design*. Hove, UK: Lawrence Erlbaum Associates Ltd., pp. 7–22.

Reason, J.T. (1993b) The identification of latent organizational failures in complex systems. In: J.A. Wise, V.D. Hopkin and P. Stager (eds.) *Verification and Validation of Complex Systems: Human Factors Issues*. NATO ASI Series, Heidelberg, Germany: Springer, pp. 223–237.

Reason, J.T. (1995) A systems approach to organizational error. *Ergonomics* 38(8): 1708–1721.

Reason, J.T. (1997) *Managing the Risks of Organizational Accidents*. Aldershot, UK: Ashgate.

Rockart, J.F. and Scott-Morton, M.S. (1984) Implications of changes in information technology for corporate strategy. *Interfaces* 14(1): 84–95.

Scheidegger, A.E. (1992) Limitations of the system approach in geomorphology. *Geomorphology* 5(3–5): 213–217.

Schiemann, J.W. (2012) Interrogational torture: Or how good guys get bad information with ugly methods. *Political Research Quarterly* 65(1): 3–19.

US Senate Select Committee on Intelligence. (2012) Committee Study of the Central Intelligence Agency's Detention and Interrogation Program, Washington DC: US Senate Select Committee on Intelligence (S.Rpt. 113–288).

Singleton, W.T. (1967a) Ergonomics in systems design. *Ergonomics* 10(5): 541–548.

Singleton, W.T. (1967b) The systems prototype and his design problems. *Ergonomics* 10(2): 120–124.

Singleton, W.T. (1972) Techniques for determining the causes of error. *Applied Ergonomics* 3(3): 126–131.

Slovensky, R. and Ross, W.H. (2012) Should human resource managers use social media to screen job applicants? Managerial and legal issues in the USA. *The Journal of Policy, Regulation and Strategy for Telecommunications* 14(1): 55–69.

Smith, D. (2005) Dancing with the mysterious forces of chaos: Issues around complexity, knowledge and the management of uncertainty. *Clinician in Management* 13(3/4): 115–123.

Tsoukas, H. (1999) David and Goliath in the risk society: Making sense of the conflict between Shell and Greenpeace in the North Sea. *Organization* 6(3): 499–528.

Turner, B.A. (1976) The organizational and interorganizational development of disasters. *Administrative Science Quarterly* 21(3): 378–397.

Turner, B.A. (1978) *Man-Made Disasters*. London: Wykeham.

Turner, B.A. (1994) The causes of disaster: Sloppy management. *British Journal of Management* 5(3): 215–219.

Waltz, E. (2003) *Knowledge Management in the Intelligence Enterprise*. Norwood, MA: Artech House.

Weick, K.E. (1995) *Sensemaking in Organizations*. Thousand Oaks, CA: SAGE.

Weick, K.E. (2001) *Making Sense of the Organization*. Oxford: Blackwell.

Wilson, J.R. (2014) Fundamentals of systems ergonomics/human factors. *Applied Ergonomics* 45(1): 5–13.