In: Laura R. Cleary, Roger Darby (Eds.) Managing Security: Concepts and Challenges,
London, Routledge, November 2021, p. 140-159
DOI: 10.4324/9781003137061

10 Cyber Security & Knowledge Management

Roger Darby, Lorraine Dodd & Jeremy Hilton

Roger Darby ORCID:

Lorraine Dodd ORCID: 0000-0002-0282-1633

Jeremy Hilton ORCID: 0000-0003-1462-2399

Introduction

In recent years, digital transformation and internet connectivity have provided unprecedented opportunities for both public and private organisations. The resulting price paid for such transformation by defence and security organisations is vulnerability to a growing number of cyber risks and threats. The adoption of reactive approaches to combatting the burgeoning range of potential assaults is proving ineffective. Physical attacks, like 9/11, and natural disasters, involving tsunamis and pandemics, have prompted governments to adopt new strategies for dealing with risk and threats; however, similar intrusions and shocks in the digital sphere (e.g. digital theft, disruption, sabotage and political warfare), have not been met with a commensurate strategic, organisational response. This is exacerbated by increasing cyber-attacks, which have undermined state security; including for example, in 2009 the malware attack against the Iranian nuclear industry, Russia's attacks against Estonia in 2007 and Georgia in 2008, interference in the 2016 USA and 2017 French presidential elections, and the Norwegian parliament in 2020. It is contended here that states are not only experiencing information warfare, but also cognitive warfare where hostile forces seek to undermine what nation states understand to be true and false. The public and private sectors are equally vulnerable to attack from state, non-state actors and terrorist proxies. It is argued in this chapter that effective cyber defence and security require not just a whole-of-government, but a whole-of-society approach.

It is also contended in this chapter that the fundamental concepts of cyber security need to be better understood by organisations if cyber-resilience and security are to be achieved. The ability to understand and anticipate your organisation's part in an increasingly complex operating environment is key to its survival. Defence and security organisations need to cultivate a culture of cyber-resilience and develop an appropriate security framework. One key

asset highlighted in this chapter is the utility of knowledge in fostering vital shared understanding. It is axiomatic that knowledge sharing has many comparable benefits for organisations and individuals. So, the management of this key resource is critical to an organisation's success or failure regarding cyber security, defence and resilience.

It is argued that systemic risk and cyber threats challenge existing paradigms for managing data, information and knowledge, and that a more radical approach to creating, capturing and sharing knowledge is required if security institutions are to remain agile and responsive. Further, if the security sector acknowledges data, information and knowledge as strategic assets, it needs to be more aware of systemic risk methods and the advantages in Knowledge Management (KM), placing these at the centre of a strategic management approach that can then be enhanced, rather than impeded, by powerful IT systems.

Technical Terminology

First, it is necessary to define the concepts central to cyber security and defence, starting by drawing a distinction between the terms 'security system', and 'defence system'. The term 'system' in the context of this chapter has a particular meaning:

> … the concept of 'system' is used not to refer to things in the world but to a particular way of organising our thoughts about the world… We consider the notion of 'system' as an organising concept … (Flood and Jackson, 2004: p16).

Thus a 'security system': is organised to prevent, or block-out, latent (or potential) threats to self.

This definition stands in contrast to that of defence system, which assumes that there is a threat actor, or perpetrator, with whom the defending system has a relationship (usually assumed to be adversarial). In this context, a defence system effects capability in response to a patent threat to self. This distinction is important because the way in which any capability (i.e. as a security system or a defence system) is then developed and exploited, needs to take the different purposes into account; in particular, when determining what constitutes important and relevant knowledge that needs to be managed and shared for the varied purposes of cyber security and cyber defence. *Cyber security*, which often also encompasses information security, refers to

the establishment of systems to ensure the integrity, confidentiality, and availability of information (Caravelli et al, 2019). These cyber security systems comprise an evolving set of tools and technologies, risk assessment approaches, specialised skills training, and best practices in organisational knowledge management designed to protect networks, devices, programs, and data from unauthorized access. On the other hand, *Cyber defence* (Darko et al, 2017) focuses on preventing, detecting and providing timely responses to attacks or patent threats.

There are three inter-related verbs that relate to cyber security and defence: *secure*, *defend* and *protect*. While often used interchangeably, they actually involve different activities for varied purposes, as Exercise 10.1 illustrates.

Exercise 10.1:

It may be helpful to think about the ways in which an organisation would *secure* its physical premises and compare those with the ways in which it would *defend* its premises. These ways would necessarily be different. They would also be different from the ways in which an organisation would need to *protect* its premises.

Write down the activities you would envisage taking place against each of the three purposes of *securing*, *defending* and *protecting* your organisation's premises. This may necessarily involve assumptions about the different natures (e.g., accidental or deliberate) of risk, threat, attack and hazard.

As highlighted in Chapter 2, the terms threat, risk, impact and vulnerability are crucial concepts in the lexicon of defence and security. For example, *Threat* connotes an intimidation and menacing potential cause of an unwanted incident, which is intended to result in harm to a system or organisation and tends to have a more deliberate intent**.** Whilst *Risk* generally, is calculated according to probability and impact. *Impact*, can be seen as a realised outcome or consequence, that can be negative or positive, direct (e.g., financial) or non-direct (e.g., reputational). *Vulnerability*, is a systemic weakness due to an asset or control that can be exploited by one or more threats (ISO: 27001, 2017; The National Cyber Security Centre (NCSC), 2020).

To aid in the understanding of these important concepts, Figure 10.1 illustrates the inter-relationship of concepts. This Concept Map can be used to highlight where key areas might need to be strengthened; for example, in terms of where knowledge management and information security need to be focused in specific organisations concerned with different aspects of business or security contexts.

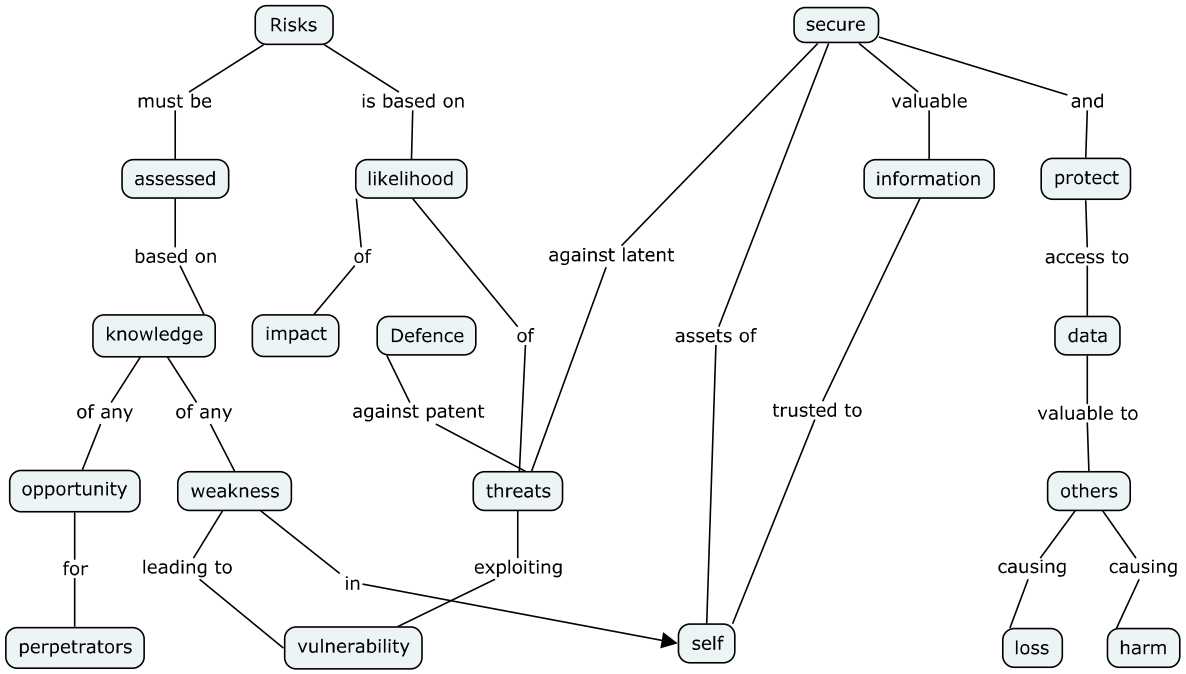

Figure 10.1: Concept Map showing the concepts relating to cyber defence and security (Source: L. Dodd)

Exercise 10.2:

Extend the concept map in Figure 10.1 to develop the concepts relating to cyber risk assessment and the importance of sharing knowledge, where knowledge can often be based on unchecked assumptions.

Concept maps were developed at the Institute for Human-Machine Cognition (Novak & Canas, 2008) to empower users to construct, navigate, share and criticize knowledge models. Their strength lies in the connections between named concepts; for example, in Figure 10.1, in

relation to risks and being secure, the concept of 'weakness' is specifically mapped in terms of any weakness that leads to vulnerability, which could be exploited via patent threats. This also points to the importance of risk assessment being dependent on knowledge.

As discussed in Chapters 1 and 2, managing risk is a critical part of the Defence and Security business. In this chapter, we are specifically concerned with assessing cyber risk. The ability to understand and anticipate your organisation's part in an increasingly complex operating environment plays a key role in its continued survival. As discussed in Chapter 2, we endeavour to objectively analyse the external and internal risk environments, conscious of the fact that risks may emerge from hidden (possibly incorrect) assumptions. This internal extension into perspectives on risk is what is meant by systemic risk. It is then natural to ask: Where might the major contribution to systemic risk come from?

Exercise 10.3:

Can you elaborate on the aspects of risk that begin to embrace systemic risk, for example:

- Your own and your organisation's hidden and or unspoken assumptions and beliefs about what might be facing you in the future.
- Your tacit acceptance of constraints and restraints being placed on parts or all your organisation's degrees of freedom of manoeuvre or choice; importantly where managerial control structures may be impeding vital functional structures.

Anymore?

Much of the systemic risk resides within one's own assumptions (Dreyer et al., 2018); also, within systems of governance (e.g., points of agency, lines of authority, responsibility and accountability). Therefore, another contributor to systemic risk is the nature of the inter-relationships and the intricacy of organisational inter-dependencies. These two key factors lie at the heart of systemic risk. Examples of major systemic failures tend to stem from behaviours that are bounded by an organisation's focus of interest (e.g., focus on the 'bottom-line' at the expense of lost potential value and damage to reputation), unspoken beliefs (e.g., hidden assumptions) and unacknowledged preferences (e.g., preferred ways of working).

Viable System Model for diagnosing organisational cyber resilience

To think through these systemic challenges, it is important to diagnose the organisation for its cyber vulnerabilities using, for example, the Viable System Model (VSM) (Espejo and Gill, 1997). The VSM is frequently used as a diagnostic tool to improve the cyber resilience and continued viability of organisations. It is, however, quite a challenging methodology to grasp as it does not consider organisations in the usual, organogram way, but from a functional management perspective, viewed in a recursive hierarchical manner. The value of VSM is that it considers not only the different focus of each layer of management, but also how the organisation joins up across the layers and what coheres the organisation. It is ideally suited to explore the functional aspects of cyber risk, cyber vulnerability and risk management.

VSM is derived from a neuro-cybernetic analogy based on the human system. Quite simply, our organisations have a brain and a coherent, collaborative set of functional organs, and they operate in and interact with an environment. This leads to the three main elements of the VSM as shown below in Figure 10.2: the management and operational elements, with the environment sitting to one side.

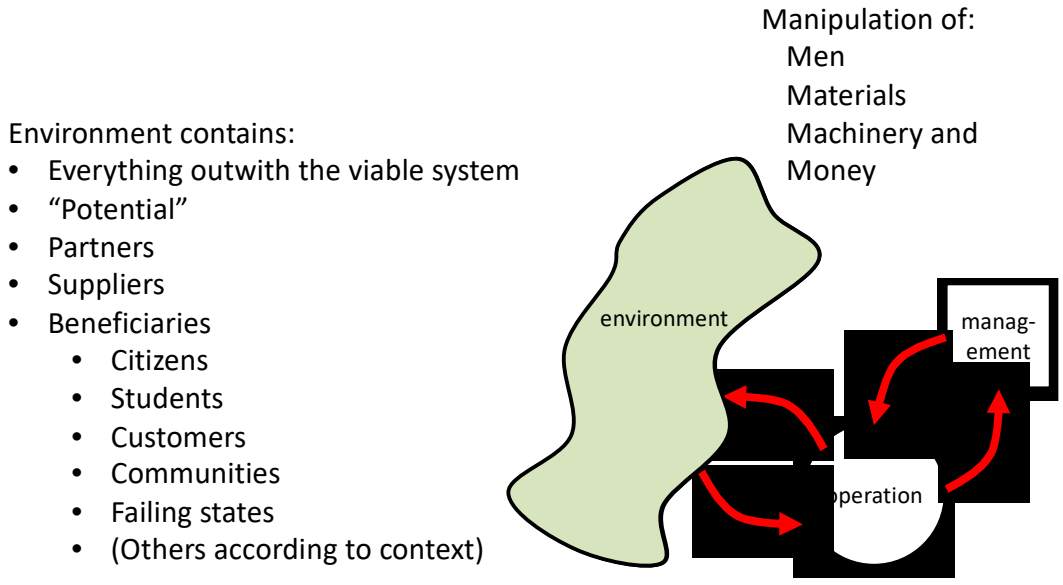

Figure 10.2 - Basic Elements of VSM (Source: J. Hilton derived from (Beer, 1985))

The management element comprises strategic direction and value-setting; an externally focused 'horizon-scanning' element; and day-to-day internally focused management. The

operations element comprises the parts of the organization that add value. From an institutional perspective, these would be the front-line service providers: defence forces, police, etc.

The VSM is nested, which is necessarily complex (Conant and Ashby, 1970), and can be applied at any level in society. For example, from a cyber perspective, one can consider the government-level (National Cyber Security Centre) development of cyber policies and best practice, down through an organisation's board-level consideration of cyber risk, to a senior leadership team's development of policy and auditing compliance, to operational units' implementation and management of controls. Each layer can be considered separately, but importantly, the VSM encourages consideration of the links and channels between the layers. It enables one to ask questions and to diagnose issues and challenges resulting in a more resilient and cyber-secure organization.

The VSM (see Figure 10.3) looks quite complicated. System 5 includes the leadership and strategic management; System 4 is the future-looking and research aspect; and, System 3 is the day-to-day management (including System 3* which includes periodic reviews of the operating elements that bypass the local operational-level management). An ongoing dialogue between System 4 and System 3 is important as it is this relationship that ensures the organisation continues to be viable, adapting to ongoing changes in the environment in a timely, effective way. System 2, a key aspect of day-to-day management, includes the essential coordination and conflict resolution across the operations arms of the business or service.

The operating units in System 1 are the parts of the organisation that add value. System 1 needs to be able to operate in its environment as freely as possible. The remaining systems are there to support and direct System 1. Consequently, each operating unit will have its own internal policy, development, operational control, coordination and monitoring, hence the recursive nature of the model. System 1 needs to be viable, but as sub-units within the organisation, they are subject to organisational policies and direction. Within the context of Cyber Security, the System 4 function should be monitoring the cyber risks, national policy and other business guidance and discussing with the System 3 what policies and controls should be put in place. These should then be issued across the organisation via the System 2 function, and periodic audits of compliance would be undertaken by the system 3* function.

Exercise 10.4

Within your organisation, identify who undertakes the function of researching outside the organisation to determine risks, cyber security best practice and relevant guidelines. The next step is to identify who undertakes an appropriate risk assessment and develops appropriate controls issued through organisational policies and procedures. Finally, who in your organisation will decide the appropriate controls and, if necessary, cyber security-focused IT solutions. Then try to construct a VSM.

Although Figure10.3 is a complicated diagram, it is a useful framework for asking questions about who in your organisation is taking responsibility for cyber security and vulnerability and how. The links between the functions are important here as you must consider these links in terms of information and knowledge flows, processes and/or specific technology. Furthermore, it is essential to identify and clarify who operates the various functions and links, especially as some of these may be by parties contracted by the organisation. In these circumstances, it is important to realise that Defence and Security organisations will always retain the liability for any cyber risks even if services and operations are outsourced.

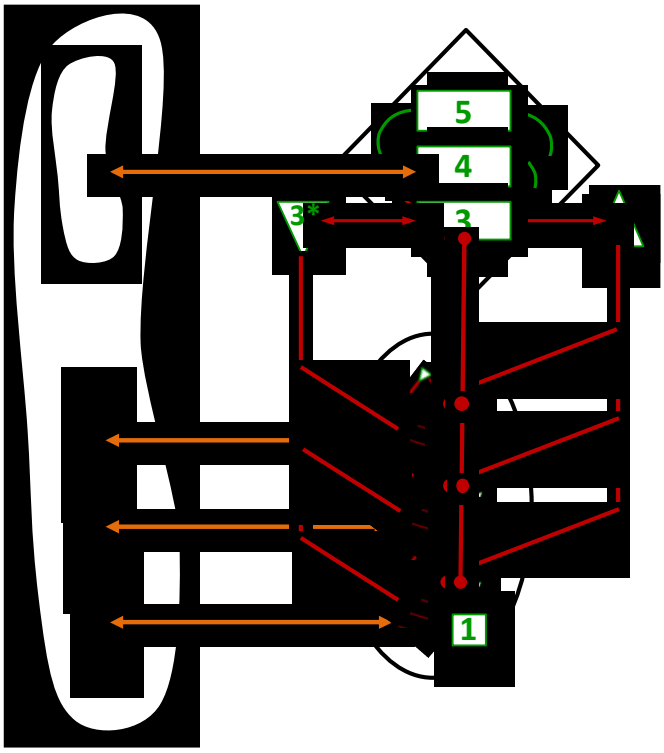

Figure 10.3: The Systems of the VSM (Source: J. Hilton derived from (Walker, 1991)

Example 10.1: The Importance of IT Governance

In September 2018, British Airways (BA) notified the Information Commissioners Office (ICO) that it had suffered a breach of customer data from its website and mobile app. The compromised data included customers' full names, email addresses and financial details (such as credit/debit card numbers, their expiry dates and CVV numbers). The breach was said to have involved user-to-BA transactions being diverted to a fraudulent site. This would appear to involve the perpetrators having gained access to BA's website and modifying the underlying code to run a 'data-skimming function' such that any customer information typed into an affected webpage could be sent directly to a server operated by the perpetrators, before it could be collected and stored by BA, whose customers would see no obvious signs that their data was being collected by anyone other than BA. The perpetrators must have gained access to the necessary code on the servers, which suggests a more systemic issue of IT governance, rather than an isolated vulnerability.

The functional organisation is represented as a VSM at Figure 4. The System 5 function is represented by the Service Sponsor in the top box of the diagram. The Service Sponsor is responsible for ensuring the service remains up to date, operates securely and meets the business and service needs. They are responsible for ensuring the System 3 and 4 functions are in constant communication to ensure the service remains fit for purpose.

The System 4 is represented by the Development box. It will ensure cyber security breach notifications are received and acted on, as well as ensuring code updates; also, that software patches are acquired and applied through a controlled software update process within the organisation.

System 3 day-to-day management of the service will include the System administrators, system operators and service operations teams. They will be informing the development team of the current state and performance of the system and will receive relevant tested code updates for the operational systems. These code updates will be passed to the relevant Systems 1.

Systems 1 identified below are for illustration purposes and do not represent a complete system. They include the key elements of the service such as the web application itself, the analytics algorithm incorporated in it, the code and data storage component and the software

development function. There is a dependency between some of them, shown by the zigzag lines, and the information or data that passes along the links is identified.

The System 2 ensures the coordination and conflict resolution between the operational systems. This includes workflow in code, business processes, security procedures and the rules-based model for the AI element. This is aimed at enabling as much autonomy at the System 1 level as is desired.

Within System 1, the software development function has developed the web application and this is operating in the web application system. The customer is sitting in the environment and has a form presented to them by the web application providing data from storage. They will enter data regarding the flight or service they wish. This is transferred to the AI system which pulls in additional data from the environment according to the algorithm needs. The AI algorithm will then return a response to the web application which will contain a decision and, depending on the service, a price tailored to the specific individual. The web application will also pull customer data from storage, incorporate the AI-generated response, and present this to the enquirer in the form of a quote, and so on. The enquirer may accept and pay. The simple flows are shown in blue.

The red lines indicate a malicious attack. If the web service and other code in use is not kept up to date regarding security updates and code patches vulnerabilities may be present in the code. By exploiting vulnerabilities in the web code, an attacker may be able to alter the code to insert additional code to intercept the data flows and collect customer data. This could be personal information, including financial data witch the attacker sits back and collects for future exploitation.

The VSM organisational diagnosis indicates the presence of vulnerabilities in the website software configuration and the web application developed by (or on behalf of) BA, the lack of effective defence against a threat exploiting the vulnerability. One might argue that the valuable information was not effectively secured against a latent vulnerability, but the data storage server most likely was protected. The BA website would have been given the necessary data

access privileges and so was a trusted application. Insufficient development, testing and management of the web server software enabled a breach. Therefore, there may have been issues in the development of the web site software, or in the configuration and maintenance of the web site server and application in its operational state.

Here, there may have been an insufficient risk assessment undertaken, or insufficient controls put in place. There may not have been an appropriate software development standard, or no monitoring of current breaches leading to software security patches being applied. From the VSM, several departments and individuals must all play their part. All of these need to be considered systemically and be monitored and audited as a coherent system to ensure there are no 'cracks' in the system that can be exploited.

The BA ICO principles make clear that *every conceivable aspect* of data and information processing must be covered by the organisation's security procedures. This means that every area of the BA business must be paying attention and be open to seeking out, managing and sharing knowledge relating to all aspects of physical, logical, device and website security.

If the problem 'system' is seen simply, and technically, as 'one compromised script' it could be treated as a technicality with blame placed at technical levels; however, the technical vulnerability in the third-party script used by BA was known about more generally and yet this *knowledge had not been managed or shared*. Therefore, there had been no responsibility or regard taken to do the costly, time-consuming updates, suggesting a more systemic problem at the level of knowledge sharing for risk assessment, pointing to IT governance at BA.

The VSM diagram at Figure 10.4 provides a whole system view that can be used to ask if cyber security management and operation is integrated.

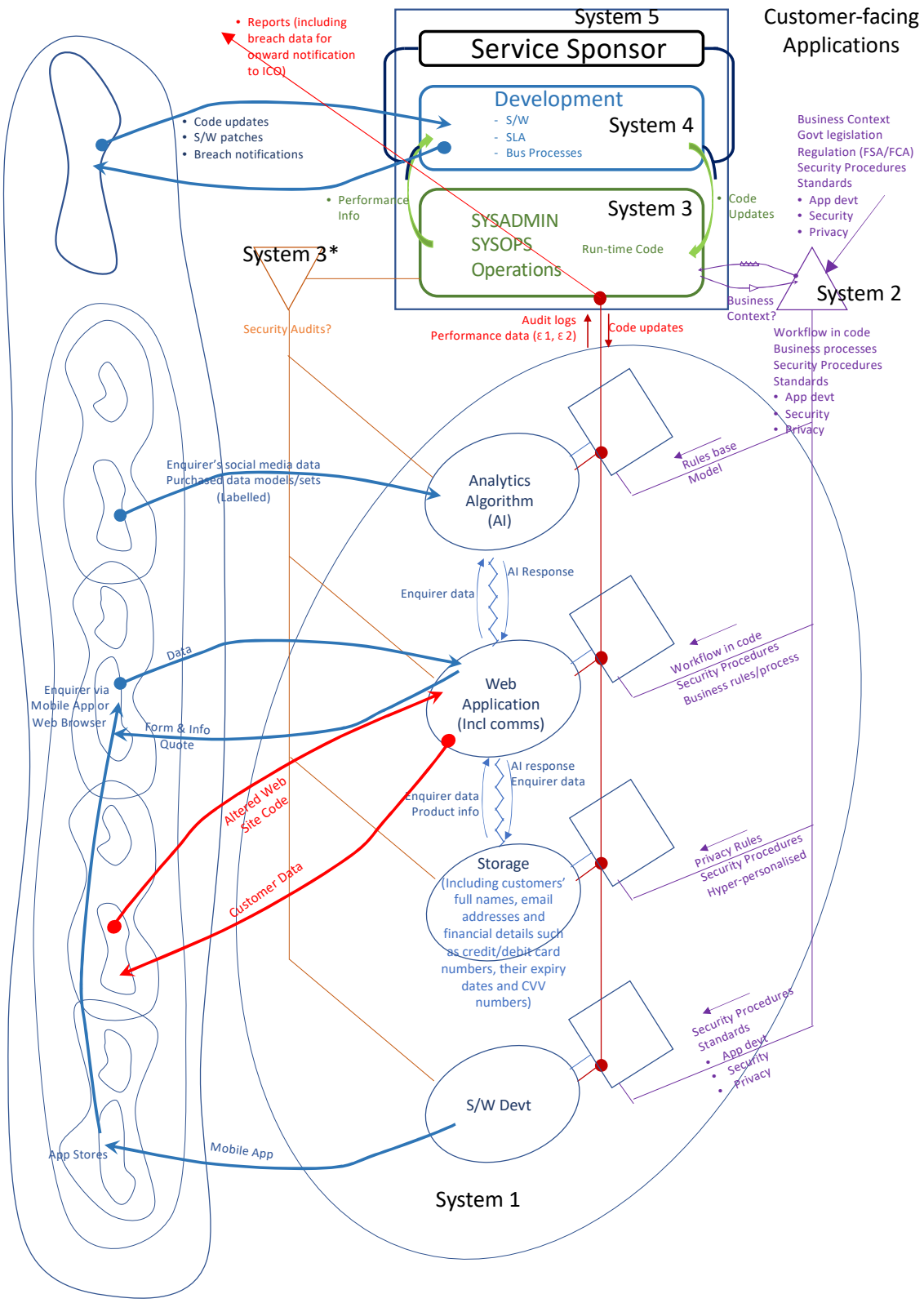

Figure 10.4 - VSM of BA Case Study (Source: J Hilton)

That there is a function that keeps up to date with cyber security issues, and that applies relevant security patches, is important; however, none of this is effective unless there is also a corporate

cyber security policy that is enforced appropriately and is periodically audited. Software development processes must incorporate cyber security aspects. Regulatory and legislative requirements must be known and complied with, particularly regarding payment protection and data protection. Vulnerabilities here, if exploited, can have a significant impact on the future viability of the organisation, as regulatory non-compliance can lead to significant fines and, in extremis, cessation of trading.

The significant amount of knowledge in people across the organisation must be kept up to date and made available to relevant parts of the organisation. Also, the requisite set of cyber-related information must be kept current and coherent; and, any changes in policy, or new vulnerabilities or potential attack methods must be made available to relevant parts of the organisation in order to update policy and implement technology. Consequently, knowledge management is essential in maintaining a cyber-secure viable organisation.

Knowledge Management

In the introduction to this chapter, we emphasised the utility of knowledge in understanding and anticipating increasingly complex operating environments. Knowledge sharing, and the management of that exchange, can provide comparable benefits for organisations. In this section, the relevance of Knowledge Management (KM) for meeting emerging challenges and opportunities linked to Cyber Security. That examination is framed with reference to the question:

> *In what ways might knowledge be acquired, shared and managed to meet 21st century security challenges?*

It is acknowledged that there is a paradox here, for, as knowledge boundaries become wider the need grows for more secure boundaries.

Exercise 10.5

Answer the following questions:

1. What is knowledge?
2. Why is knowledge important in the Defence and Security sector?
3. What is Knowledge Management?
    - What is the process?

Characteristics of KM Best Practice

It is useful to characterise knowledge according to the different perspectives on managing it. Building on Exercise 10.5 above, the aspects of knowledge referred to across academic literature are characterised as:

- A resource (i.e., as any other type of asset or resource that needs to be managed);
- A support to (and content thereof) managerial processes (i.e., seen as what needs to flow and be shared to support a KM process);
- A fundamental requirement for decision superiority and effective operational impact. (i.e., necessary to carry out an activity, course of action or a decision);
- A contribution (i.e., auditable element contributing to the achievement of objectives);
- A service (i.e., knowledge provided as a service to be acquired e.g., search engines);
- A capability dependent on competencies (i.e., adding to the organisation's capability);
- A 'weapon' to be used to good or bad effect.

These characteristics are inextricably linked to Knowledge Superiority in defence operations which require dominant defence space awareness and visualization. For example, as the defence space changes and the speed of conflict increases, the pace of information creation and decision-making also multiplies. Modern defence relies on information from many sources that must be assessed and compiled for immediate use. The timelines are shorter, and the individuals more significant in their roles. This type of conflict requires superiority at all levels of command and control. It demands situational awareness tools that are superior to those of opponents for anticipating their reactions, for sense-making, for problem solving and for superior decision-making.

Data, Information and Knowledge Management

This chapter also highlights a key conundrum faced across corporate and public sectors, including defence, regarding the distinction between data, information management (IM) and knowledge management (KM). Some researchers have argued that the difference between data, information and knowledge must be made as many people believe that they are

synonymous (Girard, 2004; Davis et al., 2006). Figure 10.5 below provides an illustration of the differences.

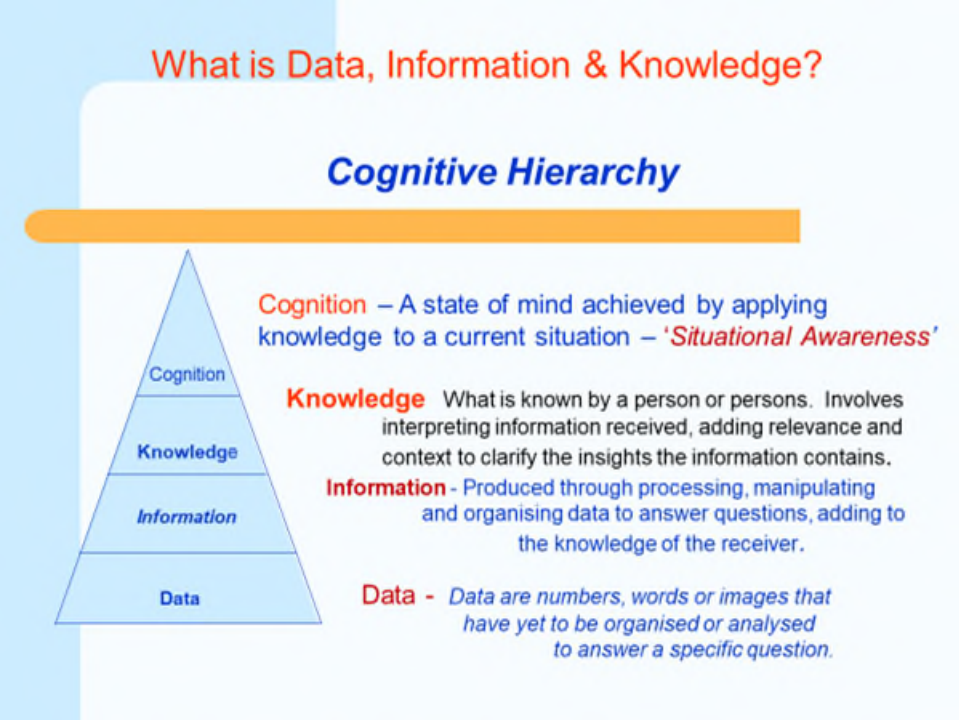

Figure 10.5: Cognitive Hierarchy (Source: R. Darby)

If knowledge is about the gathering and interpreting of information, then knowledge management is about the process through which that is done. Rumizen (2002) for example, defines KM as: 'The systematic processes by which knowledge needed for an organization to succeed are created, captured, shared and leveraged.' Collison and Parcell (2004) in turn suggest that KM:'…is about capturing, creating, distilling, sharing and using know-how.' Frappaolo (2006) draws a distinction between information and knowledge management, arguing that:

> ...the primary repository for knowledge is people's heads (at least until we agree that machines have intelligence). Electronic and paper-based knowledge repositories, then are merely intermediate storage points for information en route between people's heads (p.).

This difference highlights the important distinction respectively between 'explicit and implicit (tacit)' knowledge (Polanyi, 1962). Harnessing both explicit and implicit (tacit) knowledge is an increasing and necessarily important challenge to support organisational knowledge

creation. One of the fundamental aims of utilising KM is to understand the importance of tacit knowledge and have the skills and tools to convert tacit knowledge into explicit knowledge (Allee, 2002). For it is suggested that when explicit and tacit knowledge interact innovation occurs (Prusak, 1996; Nonaka et al., 2008).

It could be argued, however, that neither data, information nor knowledge is a bounded and discrete entity to be managed. Rather they form a dynamic symbiotic relationship and are seen in the data and information, as raw materials that enter an organisation by any means (for instance, physical, electronic or social) and knowledge, which is the organisationally constructed meaning of that data and information that is stored as a resource (physically, organisationally or personally) (Choo, 2006). Furthermore, in the untidiness of the lived experience in any organisation the boundaries between knowledge, information and data are not always clearly distinguished in organisational practice. KM is rooted in practice, action and social relationships with an important interplay between the individual and collective levels in an organisation (Stroh and Caligiuri, 1998; Davenport and Prusak, 1998).

Knowledge Sharing

Exercise 10.5:

How does your organisation:

- Create knowledge?
- Capture knowledge?
- Transfer Knowledge?
- How could your organisation improve the whole KM Dynamic?

It is self-evident that knowledge sharing has many comparable benefits for organisations and individuals; playing a major role in the process of knowledge management and as a key contributor to organisational success (Bouthillier and Shearer, 2002; Marr et al., 2003; Debowski, 2006). However, knowledge sharing can be perceived as difficult mainly due to the complex interactions between organisations and individuals which are affected by human factors as well as technical imperatives (Dalkir and Wiseman, 2004). Previous studies have highlighted the KM problems and technology adoption difficulties drawn from experts'

practices embedded in the work context (Hsiao et al., 2006, 2012) and is associated with what Darby (2012: p. 12) identifies as the 'dynamic of KM' involving knowledge creation, capture and transfer in organisations.

Further research has highlighted relevant issues regarding the dissemination of knowledge, locating knowledge holders and exploiting existing knowledge (Hubert et al., 2001; Sambamurthy and Subramani, 2005). Two pertinent issues arise from these studies. First, little consideration is given to knowledge attributes when analysing KM problems (Alavi and Leidner, 2001). Second, and more pertinently for this chapter, although previous studies have mainly examined how knowledge barriers can be mitigated to achieve better technology acceptance, they are generally insensitive to exploring how work contexts may affect KM problems (Purvis et al., 2001; Hubert et al., 2001). This highlights a challenge to previous research which appears to treat knowledge barriers as universal and acknowledges that different expert groups (including those in defence) may adopt different types of knowledge within different contexts (Gherardi, 2000; Orlikowski, 2002; Bogenrieder and Nooteboom, 2004). Knowledge in such contexts may reside in physical processes, social communities and service or industrial settings (Hsiao et al., 2012; Tyre and von Hippel, 1997; Lam, 1997).

Knowledge Management in the Defence Sector

It is argued in this chapter that KM in defence does not differ in theory from corporate versions, but in terms of *context, content and pace*. Corporate KM tools can depend on a more sedentary infrastructure, whilst operational settings in defence often require mobile solutions with corresponding questions of security, bandwidth, robustness and reliability; with varying content, and often more targeted to the particular operation. Most corporate situations do not need the comparable, quick reaction time required in conflict situations. Consequently, KM in the military context requires: knowledge processes that are robust and reliable within operational contexts; content and intellectual assets that are focused, precise, reliable, with suitable recall levels; and knowledge creation and conversion processes that match the pace of operations.

Concomitantly, modern-day 'information overload' is one of the greatest technical challenges facing national security communities. The ongoing, exponential increase in digital data

necessitates the use of more sophisticated analytical tools to effectively manage risk and proactively respond to emerging security threats. Constantly contending with the certainty of uncertainty at the strategic and operational levels, the provision and leveraging of knowledge resources, much like intelligence, can be a key enabler to deriving better outcomes in defence processes as well as with current and planned future outputs (see Chapter 2). However, defence organisations usually tend to be part of extremely large institutional structures designed along rigid hierarchies and reinforced by a top-down 'chain of command' culture. Security is a constant theme across defence operations and processes, taking many forms – operations security, communications security, information security and cyber security, for example – which strongly instil a 'need to know' basis and a conservative attitude towards disclosure or sharing of data, informational and even knowledge resources. Therefore, the management of data, information and knowledge in the defence sector stands at an interesting juncture. Key dilemmas facing the defence sector are on the one hand, identifying and effectively using the increasing potential of technical interoperability; on the other hand, the need for new management practices juxtaposed with the escalating global challenge to security to counteract the rise of emerging threats (Darby, 2012). Consequently, governments are increasingly identifying their digital infrastructure as a strategic national asset that also needs to be better protected.

It is argued in this chapter, that such threats to the defence sector challenge existing paradigms for managing data, information and knowledge and suggest a more radical approach to gaining knowledge superiority is a requirement to remain agile in the fast-moving, technologically advanced wider defence and security sector. Further, if the defence sector acknowledges data, information and knowledge as strategic assets it needs to be more aware of the advantages of KM and place it at the centre of the strategic management approach (Sveiby, 2001; Dalkir, 2005).

But what of the human component? The necessary body of people who must understand and operate these more sophisticated systems? As changes multiply, the need to manage change more effectively becomes even more important. It is self-evident that sense-making, problem solving, and decision making are more complex and more vital in military situations than ever before. New technologies have resulted in increasingly dynamic, unpredictable and complex

operations that require people to filter and analyse information from multiple sources. Concomitantly, know-how, expertise and interoperability are equally important key factors in a defence sector organisation's ability to create knowledge superiority (Gold and Arvind Malhotra, 2001; Malhotra, 2004). Command and control are taking on new dimensions and the role of military personnel is evolving; some would suggest they are becoming knowledge workers (Adler, 2007; Starbuck, 1992). It can be further argued that as organisations gain access to even more advanced technology the impetus behind successful global organisations (including those in the defence sector) to maintain competitive advantage is dependent upon the development of knowledgeable employees (and multi-level and multi-cultural relationships).

Exercise 10.6:

In a defence acquisition management context, project teams could be creating new knowledge about clients, costing, suppliers, legal and statutory issues, procedures or technical matters, which will not be effectively captured, transferred or related to future projects once the project team disbands. While KM in permanent organisations can focus on knowledge silos that exist within departmental or divisional constructs, organisational routines or organisational memory are unlikely to emerge at all in project-based teams or organisations. How can Defence manage the 'organisational memory' in these temporary working constellations more effectively to meet changing defence needs in the next 5 years?

Example 10.2: The Huawei Case

The British Government's original contentious decision to use the Chinese firm Huawei to provide a significant part of the UK's 5G telecommunications system caused alarm and heated debate related to the security implications. Huawei has risen from a small importer of foreign telecoms equipment to one of the world's largest makers of 5G mobile networks. A number of countries including the USA, Australia and Japan raised concerns that the kit may come with 'back doors' – deliberate security holes that can act as conduits for Chinese spies or cyber-saboteurs. On the other hand, many believed Huawei should be allowed to compete in new markets. Its products are high-quality and cheap. Excluding it would be costly and risks delaying 5G.

It is suggested the risks are real although countries can adopt 3 broad strategies to mitigate them:

1. *Technical* – Encouraging encryption would ease spying concerns, since intercepting data would produce only gibberish. Networks need to be defended in depth. Britain intended to exclude Huawei from sensitive parts of the network, though geography may limit that approach elsewhere. Because accidental bugs can be as dangerous as deliberate back doors, having several suppliers and spare capacity is a good idea. Redundancy and resilience are the watchwords.

2. *Encouraging Existing Industry Trends Towards Openness* – Present telecom networks are built with proprietary products. In future they will become just another piece of software running on off-the-shelf computers. That should allay worries about compromised hardware and make it easier for new entrants to compete. Open-source is in fashion and an alliance of tech companies is keen on open-source versions of antennae and masts that make up a mobile network's outer edge. Having code and devices open for inspection makes it easier to find security holes, and harder to hide back-doors.

3. *International Co-operation* - Britain had already stripped down and inspected all Huawei kit. Sharing the results and experience more widely would make more scrutiny possible to keep Huawei honest. In the longer term, an international inspection body, modelled for example, on the International Atomic Energy Agency, could be a good idea.

Computer security, like all security is about trade-offs, not absolutes. Back-doors are a concern, but most hackers make do with the accidental flaws. Russia, for example, has no domestic electronics industry to speak of, and therefore no ability to insert back-doors. Designing robust networks, building them with checkable equipment and sharing knowledge and expertise should make it harder for hackers from all countries, not just China.

Exercise 10.7

1. Analyse the debate about the British Government's initial intention to use Huawei in the installation of a 5G network. Was the UK governments final decision not to use Huawei right or wrong? Give your reasons.
2. What security concerns are raised by the Huawei case when a government is planning for the latest SDSR which may involve a decision about installing a 5G network provided by a foreign supplier?
3. Discuss the three strategies in the case to mitigate possible risks to national security. Are they resilient enough?
4. What strategies could be added to them to support the further mitigation of security risks?

Conclusion

This chapter has highlighted a pivotal issue in the contemporary security and defence milieu; namely, the ubiquitous role that cyber security and defence play in all societies across the world. Digital transformation and web-connectivity now provide unprecedented opportunities for individuals and organisations. This technological transformation has created vulnerability to an unparalleled, burgeoning range and scope of cyber risks and attacks on individuals and organisations alike. Governments, no matter how big or powerful, are not protected or immune from such cyber risks and attacks. Indeed, security and defence forces face a bewildering array of state-based and non-state actors, and terrorist proxies, which add to the complexity that state agencies are forced to manage with increasing difficulty. It is argued in this chapter that as the scale of cyber threat and risks is exponentially increasing, there is a real need to think and work systemically. Consequently, governments increasingly need to identify their digital infrastructure as a strategic national asset that needs to be better protected. This includes being systematic about what we take cyber concepts to mean; also, being systematic about cyber resilience by using cybernetic organisational diagnosis to check for cyber vulnerability. Furthermore, effective cyber defence and ultimate security require not just a whole-of-government, but a whole-of-society approach.

Not all governments are successful in managing rapid complex change, especially where there are tensions between what must remain commercial and what needs to be regarded as sovereign stewardship or guardianship (Jacobs, 1992). There are additional challenges for those

governments engaged in post-conflict recovery and development, as they often do not have commensurate strategic organisational responses to common digital disruption, theft, sabotage and political warfare occurring in the area of cyber security. This chapter has emphasised the need for a deeper understanding of cyber resilience and security within an organisationally focussed security framework.

Several emerging themes have been raised in this chapter in relation to KM and Cyber Security in complex environments. One theme highlighted is the basis on which knowledge is shared as well as managed. For example, if knowledge is being treated as a resource, then questions need to be asked whether it would be more appropriate (and operationally effective) to treat knowledge as a support to strategy, a contribution to objectives and, with knowledge sharing, being a defined capability in its own right.

Another emergent theme is that of context, both operational and organisational contexts, within which KM is happening. For KM, the operation tends to form the immediate context for knowledge (e.g., KM within a HQ), which then forms the context for the organisation and its people and processes responsible for managing and sharing and protecting knowledge.

Further, KM principally supports access to new knowledge and sharing of knowledge. A traditional KM lifecycle tends to be represented as an end-to-end process; starting with creation of 'information-based' knowledge and ending with a composed, collated view of 'the situation out there'. So, in a KM lifecycle, the movement from knowledge acquisition to learning outcomes (e.g., 'lessons identified' captured in managed knowledge bases) sits within a context of constraints consisting mainly of extant organisational ways of thinking and ways of working (which may be outdated and outmoded).

The new context for KM, will tend to be formed first by individuals involved, according to their prior knowledge and experience, then by the organisation and finally by the operational environment (about which much of the knowledge will be gained and formed). As such, the organisation (and individuals) tend to form the immediate context, within which the operational setting forms the framing context for the use of knowledge to support understanding and

decision-making. However, as highlighted in Chapter 9, the significant amount of knowledge in people across the organisation must be kept up to date and made available to relevant parts of the organisation. Also, the requisite set of cyber-related information must be kept current and coherent; and, any changes in policy, or new vulnerabilities or potential attack methods must be made available to relevant parts of the organisation in order to update policy and implement technology. Consequently, KM is essential in maintaining a cyber-secure viable organisation.

Adopting an end-to-end process view can neglect the open-ended nature of 21st Century Defence and Security challenges, where feedback and effective learning must form a key part of an essential framework. Here is where shared knowledge techniques open-up new ways to re-frame and then to gain new knowledge; and where cybernetic models such as VSM become essential organisational diagnostic tools to ensure cyber resilience. Technology solutions to KM tend to focus principally on the 'texts' in the form of content of the knowledge. Non-technology KM good practice would suggest the need to look outwards to contexts and self-wards to organisational constraints.

What can be inferred from this chapter is that the future for Cyber Security is very uncertain and difficult to predict. This can be exemplified by some of the current trends and threats faced by security forces across the world today; including, threats to *digital security,* which comprise the use of polymorphic malware that adapts its identifiable characteristics to evade detection, or the automation of social-engineering attacks to target individuals. Palpable threats to *political security* include the use of 'deep fake' technology to generate synthetic media and disinformation, with the objective of manipulating public opinion or interfering with electoral processes; leading to what was identified in the introduction as the threat of 'cognitive warfare'. Threats to *financial security* are of immediate concern. Furthermore, increased adoption of the Internet of Things (IoT) technology, artificial intelligence (AI), autonomous vehicles, 'smart cities' and interconnected critical national infrastructure will create numerous cyber vulnerabilities which could be exploited to cause damage or disruption. Additionally, emerging from the novel research areas (see *US Defense Advanced Research Projects Agency (DARPA))* are biomimetic nature-imitating weapons, which cannot be ignored as a techno-military

fantasy. This could lead to the danger of lethal autonomous ‘swarm’ weapon systems and the question of laws to control such arms.

This chapter also links to the interesting question related to international humanitarian law, which is highlighted in Chapter 4. Key ethical principles of warfare have covered discrimination and proportionality that require aggressors to distinguish between combatants and civilians. In the modern defence space, soldiers and cyber-warriors could face many difficulties in distinguishing neutrals from enemies and pose greater risks when robotic weapon systems are increasingly utilised.

Of course, it should never be forgotten that the weapons industry has always been very big business, as discussed in Chapter 11. The military-industrial complex supporting cyber defence and security has accelerated an arms race including research and development into, for example, the lucrative world of AI. This all produces a double-headed hydra allowing for burgeoning domestic use as well as external foreign use of AI surveillance with nebulous apparatuses of control.

The final point links with Chapters 1 and 2 in this volume; namely, how do governments and leaders respond to new weapon technology? A simple binary choice between ban or regulate may not suffice because new ‘cyber weapons’ can be deployed without discernible attribution and they can operate ‘below the legal radar’ to create disruption. A more measured discourse is needed around the issue of reform, and the importance of accountability within the *real-politik* of cyber warfare and the use of autonomous weapons. The fog-of-war is often used as an excuse. However, national governance and international legal systems must impose more accountability and responsibility on states and forces who use such weaponry that has the potential to cause untold civil damage in the future.

Questions to consider

1. What skills sets are required for cyber warriors to be effective today and in the future?

2. Identify the different ways in which non-state actors might pose cyber threats in future?
3. How might the sensitivities around cyber vulnerabilities be navigated to allow for more sharing of knowledge about how to remain cyber resilient?
4. How would you regulate the control of the use of autonomous weapons in your country's security forces?

Suggested further reading

Choo, W., and Bontis, N., eds., (2002) *The Strategic Management of Intellectual Capital and Organizational Knowledge*. Oxford: Oxford University Press.

Hislop, D., Bosua, R. & Helms, R. (2013) *Knowledge Management in Organizations.* 3rd ed. Oxford : Oxford University Press .

References

Adler, P. (2007) 'The future of critical management studies: a Paleo-Marxist critique of labour process theory', *Organization Studies*, 28, pp. 1313-45, DOI: 10.1177F0170840607080743.

Alavi, M., & Leidner, D. (2001) 'Knowledge management and knowledge management systems: Conceptual foundations and research issues', *MIS Quarterly* 25(1): pp. 107–136. DOI: 10.2307/3250961.

Allee, V. (2002) *The Future of Knowledge: Increasing Prosperity Through Value Networks.* Newton, MA: Butterworth-Heinemann.

Bogenrieder, I., & Nooteboom, B. (2004) 'Learning groups: What types are there? A theoretical analysis and an empirical study in a consultancy firm'. *Organization Studies*, 25(2), pp. 287–313. DOI: 10.1177/0170840604040045

Bouthillier, F. & Shearer, K. (2002) 'Understanding knowledge management and information management: The need for an empirical perspective', *Information Research*, 8(1), paper no. 141.

Caravelli, J., Jones, N. and Kozup, J.C. (2019) *Cyber Security: Threats and Responses for Government and Business***.** London: Praeger .

Choo, Chun Wei (2006) *The Knowing Organization: How Organizations Use Information to Construct Meaning, Create Knowledge, and Make Decisions*, Second Ed. Oxford**:** Oxford University Press. DOI:10.10162006.03.011.

Collison, C. and Parcell, G. (2004) *Learning to Fly. Practical Knowledge Management from Leading and Learning Organizations.* Chichester: Capstone Publishing Limited.

Conant, R.C. and Ashby, R.W. (1970) 'Every Good Regulator of a system must be a model of that system', *International Journal of Systems Science.* 1(2), pp. 89-97.

Dalkir, K. (2005) *Knowledge Management in Theory and Practice*. Oxford: Elsevier.

Dalkir, K., & Wiseman, E. (2004) 'Organizational story-telling and knowledge management: A survey'. *Storytelling, Self, Society*, 1(1), pp. 57-73, DOI:10.10801550534040949025 8.

Darby, R. (2012) 'Cyber Defence in Focus: Enemies near and far – or just behind the firewall. The case for Knowledge Management.' *Defence Studies*, 12(4), pp. 523-38. DOI: 10.1080/14702436.2012.745964.

Darko, G., Darko, M. and Guberina, B. (2017) 'Cybersecurity and cyber defence: national level strategic approach', *Automatika*, 58(3), pp. 273-286, DOI: 10.1080/00051144.2017.1407022.

Davenport, T, and Prusak, L. (1998) *Working knowledge: How Organizations manage what they know*, Boston, MA: Harvard Business School Press.

Davis, J., Miller, G.J. & Russel, A. (2006) *Information revolution: using the information evolution model to grow your business*, Hoboken, New Jersey: John Wiley & Sons, Inc.

Debowski, S. (2006) *Knowledge Management*, Wilton, Australia: Wiley.

Dewar, J. (2002) *Assumption-Based Planning: A Tool for Reducing Avoidable Surprises*, RAND Corporation, New York: Cambridge University Press.

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J.W. and Winkelman, Z., (2018) *Estimating the global cost of cyber risk: methodology and examples*, Santa Monica, CA: RAND Corporation. DOI:10.7249/RR2299

Espejo, R. and Gill, A. (1997) 'The Viable System Model as a Framework for Understanding Organizations', Malhotra, Y., ed., *Knowledge Management and Virtual Organizations, Idea Group Publishing*, 2000., pp. 350–364.

Flood, R.L. and Jackson, M.C. (2004) *Creative Problem Solving: Total Systems Intervention*, Hoboken, NJ: Wiley.

Frappaolo, C. (2006) *Knowledge Management*, Chichester: Capstone Publishing Limited.

Gold, A.H. and Arvind Malhotra, A.H.S., (2001) 'Knowledge management: An organizational capabilities perspective', *Journal of Management Information Systems*, 18(1), pp.185-214, DOI:10.1080/07421222.2001.11045669.

Girard, J. (2004) 'Defence Knowledge Management: A Passing Fad', *Canadian Military Journal*, Summer, 2004, pp. 17-28.

Gherardi, S. (2000) 'Practice-based theorizing on learning and knowing in organizations'. *Organization* 7(2), pp. 211–223, DOI:10.1177%2F135050840072001.

Hsiao, R., Dun-Hou Tsai, S., and Lee, C.F. (2012) 'Collaborative knowing: the Adaptive nature of cross-boundary spanning,' *Journal of Management Studies*, 49, pp. 463-491. DOI:10.1111/j.1467-6486.2011.01024.x.

Hsiao, R., Dun-Hou Tsai, S., and Lee, C. F.(2006) 'The Problems of Embeddedness: Knowledge Transfer, Coordination and Reuse in Information Systems,' *Organization Studies*, 27(9), pp. 1289-1317, DOI:10.11772F0170840606064108.

Hubert, C., Newhouse, B and Vestal, W. (2001) 'Building and sustaining communities of practice', *Knowledge Management, Enabling Business Processes*, Houston, USA.

International Standards Organisation (2017) *ISO 27001 Information Technology-Security Techniques-Information security management systems-requirements.* Available at: https://www.iso.org/isoiec-27001-information-security.html. [Accessed on 11 October 2018].

International Standards Organisation (2018a) *ISO 31000 Risk management*. Available at: https://www.iso.org/iso-31000-risk-management.html [Accessed: 11 October 2018].

Jacobs, J. (1992) *Systems of Survival*, New York: Random House.

Jullien, F. (2004) *A Treatise on Efficacy*. Honolulu: University of Hawaii Press.

Lam, A. (1997) 'Embedded firms, embedded knowledge: Problems of collaboration and knowledge transfer in global cooperative ventures, *Organization Studie,s* 18(6), pp. 973–996. DOI:10.1177%2F017084069701800604.

Malhotra, Y. (2004) 'Why knowledge management systems fail: enablers and constraints of knowledge management in human enterprises,' *Handbook on Knowledge Management 1*. Springer Berlin Heidelberg, pp. 577-599.

Marr, B., Gupta, O., Pike, S., and Roos, G. (2003) 'Intellectual Capital and Knowledge Management Effectiveness', *Management Decision*, 41(8), pp. 771-781.

NCSC (2016) *Risk management and risk analysis in practice*. Available at: https://www.ncsc.gov.uk/guidance/risk-management-and-risk-analysis-practice [Accessed: 1 October 2018].

NCSC (2020) Available at: https://www.ncsc.gov.uk/information/understanding-vulnerabilities. [Accessed on 1 November 2020].

Nonaka, I., Toyama, R. and Hirata, T. (2008) *Managing Flow: A process theory of the knowledge-based firm*, London: Palgrave Macmillan, DOI:109.151.224.215.

Novak, J. D. and Cañas, A. J. (2008) 'The Theory Underlying Concept Maps and How to Construct and Use Them, Technical Report IHMC CmapTools 2006-01 Rev 01-2008', Florida Institute for Human and Machine Cognition. Available at: http://cmap.ihmc.us/Publications/ResearchPapers/TheoryUnderlyingConceptMaps.pdf . [Accessed on 1 November 2020].

Orlikowski, W. (2002) 'Knowing in practice: Enacting a collective capability in distributed organizing', *Organization Science* 13(3), pp. 249–273, DOI:10.128713.3.249.2776.

Oxford English Dictionary (2018) 'Definition of Risk'., *Oxford English Dictionary* Available at: https://en.oxforddictionaries.com/definition/risk [Accessed: 9 October 2018].

Polanyi. M. (1962*) Personal Knowledge*. Chicago: University of Chicago Press.

Prusak, L., (1996) 'The knowledge advantage', *Planning Review*, 24(2), pp.6-8.

Purvis, R., Sambamurthy, V., and Zmud, R. (2001) 'The assimilation of knowledge platforms in organizations: An empirical investigation', *Organization Science* 12(2), pp. 117–135. DOI:10.1287/orsc.12.2.117.10115

Rumizen, C, M. (2002) *The Complete Idiot's Guide to Knowledge Management*. Washington: Alpha Publishing.

Sambamurthy, V., and Subramani, M. (2005) 'Special issue in information technologies and knowledge management', *MIS Quarterly* 29(1), pp. 1–7. DOI: 10.2307/25148665

Starbuck, W. (1992) 'Learning by knowledge-intensive firms', *Journal of Management Studies*, 29, pp. 713-40. DOI:10.1111/j.1467-6486.

Stroh, L. and Caligiuri, P. (1998) 'Increasing global competitiveness through effective people management', *Journal of World Business,* 33(1), pp1-16, DOI:10.1016/S1090-9516(98)80001-1.

Sveiby, K.E., (2001) ‘A knowledge-based theory of the firm to guide in strategy formulation’ *Journal of Intellectual Capital*, 2(4), pp. 344-358.

Tyre, M. and von Hippel, E. (1997) ‘The situated nature of adaptive learning in organizations’. *Organization Science*, 8, pp. 71–83, DOI:10.1287/orsc.8.1.71

Wiig, K.M., (1993) *Knowledge management foundations: Thinking about thinking – How people and organizations create, represent, and use knowledge,* Arlington, TX: Schema Press.

Chapter 10: cyber security and knowledge management

Darby, Roger

2021-11-29

Darby R, Dodd L, Hilton J. (2021) Chapter 10: cyber security and knowledge management. In: Managing security: concepts and challenges, London: Routledge, November 2021, pp. 140-159
https://doi.org/10.4324/9781003137061