In: Managing Security Concepts and Challenges, Abingdon, UK, Routledge, ed. 1st.
ebook url: https://doi.org/10.4324/9781003137061

2 If You Can't Be Secure, Be Resilient

Edith Wilkinson and Laura R. Cleary

Edith Wilkinson ORCID: 0000-0003-1446-612X

Laura R. Cleary ORCID: 0000-0003-0167-4544

Introduction

We begin our discussion of security and resilience by offering a 'health warning': over the following pages the reader will encounter more questions than answers. Our aim within this chapter is not to tell the reader what to think, but to help identify issues for consideration when developing security capabilities. We acknowledge that the concepts of security and resilience are both contested (Buzan, 1991; Walklate et al, 2014). We also accept that neither security nor resilience are fixed attributes of a society. They are 'multilayered, multifaceted' (Walklate et al, 2014), in variable evidence over time, and rarely the sole responsibility of any one entity.

Over the last 30 years, the concepts and practice of security and resilience have become intertwined, as is evident by the policy pronouncements of both states and intergovernmental institutions alike (see for example the US National Security Strategy, 2015; UK National Security Strategy, 2015; EU Security Strategy, 2016; ASEAN Joint Declaration, 2018). It has been suggested that the change in government focus from state to non-state-based threats (Vasilache, 2019), the emergence of an 'all-hazards' approach to risk management (Walklate et al, 2014), the promotion of the liberal peace-building agenda (De Coning, 2018), and subsequent concerns over its efficacy have resulted in a reconsideration of whether and how security can be provided.

This issue became evident, indeed inescapable, during the course of 2020. As we write this chapter, a global pandemic continues to exact its toll on lives, public health services, economies and political systems. COVID-19 dramatically exposed the fault lines of our societies. The acknowledgement of the fragility of our systems has amplified interest in the concept of resilience and in its relationship with the State and with security.

This is an Accepted Manuscript of a book chapter published by Routledge in Managing Security Concepts and Challenges on 29 November 2021, available online:https://doi.org/10.4324/9781003137061

In Chapter 1, Cleary and Darby presented five questions with which this book is concerned. In conceptualising security through its congruence to resilience, this chapter offers insights to some of those questions, while asking additional ones. The exploration of the security and resilience nexus revolves around two questions which are explored in this chapter:

- If security is elusive can societies become resilient instead?
- What does that mean and what would that actually entail?

In seeking to address these questions we will be highlighting certain themes that are integral to the book as a whole: agency, adaptive capacity, capability, risk and change management. It is through the treatment of these subjects that we engage with the issue of who is ultimately responsible for individual and collective well-being.

It is argued within this chapter that resilience is not solely about how one prepares and responds to a crisis. It is about whether we choose to learn from crises, what we choose to learn, and how we apply that knowledge to the prevention or mitigation of future crises. Ultimately, resilience is about the capacity to learn and adapt; only then can individuals, institutions and states become more resilient and secure.

Defining Security and Resilience

While the questions posed above might appear to be simple ones, the answers are frequently complex, and liable to change over time. When lecturing on security we often begin our sessions by asking our students to define the concept.

What does it mean to be secure? No matter where in the world the class is being held the responses are fairly consistent. Security is described as a 'feeling of safety', as 'freedom from fear, want or threat', as the 'institutions and/or process through which that perception of safety and condition of freedom are achieved'. As our discussions continue our participants often acknowledge their concern that their institutions and processes are no longer capable of providing security to the standard demanded by the public. There are a variety of reasons for why this might be the case, ranging from a consistent lack of policy direction and investment

to the development of sclerotic bureaucratic structures, but certainly one of the reasons has to be a heightened sense of subjectivity as a result of the globalisation of information and the prevalence of 'competing truths'. Back in 1991, Buzan memorably described security as 'an essentially contested concept' (Buzan, 1991). He argued that, although security can be objectively defined as freedom from fear, from want, and from threat, freedom itself is relative, thus a sense of security is ultimately subjective in nature. Therefore, responses to the question of 'what is security' are as varied as the states and institutions tasked with providing it.

Since the end of the Cold War in 1989 we have witnessed a rapid evolution in the discourse and practice of security. During the Cold War, the state was viewed as the referent object of security (Buzan, 1991). The focus of government policy, evidenced in institutional arrangements and budget allocations, was on the defence of territory, be that from invasion or nuclear annihilation. From the perspective of the United States and the Soviet Union, internal unrest in proxy states was either to be encouraged or suppressed depending on whose ally they were. That approach began to change in the last decade of the 20th century. Triumphalist claims regarding the 'end of history' and the supremacy of democracy over communism (Fukuyama, 1992) appeared, warranted given the headlong rush to overthrow authoritarian regimes across Latin America, Eastern Europe and Africa throughout the 1980s and 1990s. The 'new world order' proclaimed by US President George H. W. Bush in 1990 would be one in which democratic and pacific states would take collective action within regional and international organisations to resolve global concerns (Bush, 1990). In the absence of existential threats to national security, governments sought 'peace dividends' by downsizing or right-sizing their armed forces, and either redirecting the money previously spent on defence to other public sector organisations or reducing the rate of tax. These structural adjustments both gave rise to, and were subsequently underpinned by, the belief that a singular focus on the state as the referent object of security was no longer appropriate (Owen, 2004). Academic discourse and international policy increasingly emphasised the importance of the individual as both an agent and object of security.

The term 'human security' was coined by the United Nations Development Programme in 1994 and was quickly embraced within the policies of nations and the strategies and programmes of international organisations. As the term implies, a human-centred, rather than a state-centred,

approach to security is advocated, with emphasis being placed on those elements which allow individuals to survive and thrive (UNDP, 1994). Whether the concept is understood in narrow terms as 'freedom from fear' (e.g., direct violence, displacement) or in a broader sense as 'freedom from want' (e.g., food, poverty and access to education), it is the individual desiring that freedom (Owen, 2004; Sharpe et al, 2020). The individual, however, cannot achieve that freedom on their own or in isolation; a combination of top-down and bottom-up approaches that place an emphasis on both protection and empowerment is required (Sharpe et al, 2020: p. 468). Therefore, the notion of state security has not been abandoned; indeed, in some parts of the world it remains the dominant concern, but in the West an attempt has been made to place the concept in broader context. Preservation of state security became the means to the end of securing individuals and communities (Pettman, 2005). Debate continues as to whether human security is truly the dominant paradigm as states continue to serve as the primary actor in the international environment. However, the rhetorical opening has at least provided an opportunity for neglected concerns and marginalised voices to surface (Cleary, 2016). We are individually and collectively confronted by a host of risks and threats, some the result of the change in the security discourse, others the inevitable consequence of globalisation.

It is worth exploring the distinction drawn between the concepts of 'risk' and 'threat'; while the concepts are complementary, they are not synonymous. Risk is typically defined in terms of probability and consequence and need not be associated with a named agent, whereas threat is defined as existing when an actor or group of actors has the capability and intention to inflict a negative consequence on another actor or group (Rousseau, 2007; Davis, 2000). Consequently, the way in which we seek to manage risks may be very different to the way in which we respond to threats. Yee-Kuang identified the 2002 US National Security Strategy (NSS) as a 'watershed' document in terms of the conceptualisation of security as risk management; in his estimation, that NSS 'crystallised the proactive calculus of risk. Declaring the obsolescence of a "reactive posture" of containment and deterrence, it plumped instead for anticipatory actions even if uncertainty [remained] as to the time and place of the enemy's attack' (Yee-Kuang, 2006: p. 25). From that point onwards until 2015 policy documents produced by the US, the United Kingdom, and other NATO states and Partnership for Peace (PFP) members were notable for the absence of named enemies and the similarities of the risks identified. As will be detailed below, the adoption and advocacy of a risk management

approach to security led a number of countries to frame reform of their own security institutions and those of other countries in terms of resilience (see Example 2.1).

Example 2.1: Reframing Security: the case of Armenia

Since the Republic of Armenia achieved independence from the Soviet Union in 1991 it has published two National Security Strategies (NSS); one in 2007, the second in 2020.

In its assessment of its security context, Armenia's 2020 NSS highlights a number of risks at the geo-strategic, regional, national, and societal levels that present challenges to the sovereignty and/or territorial integrity of the state, but it also identifies countries as posing specific existential threats to the state.

The long-standing dispute with Azerbaijan over the territory of Artsakh, or Nagorno-Karabakh, (erupting violently in 2016 and again in 2020) has, perhaps unsurprisingly, led the Armenian government to place an emphasis on modernising its armed forces, developing its military-industrial complex, and ensuring the political oversight of both. The 2020 NSS, however, additionally 'aims to enhance resilience through a nationwide approach to planning and maintaining national security' (Republic of Armenia, 2020: p. 2). The broadening of the idea of security is noteworthy – the NSS now suggests that the resilience of the defence and security sector, as well as that of the economic, food and health sectors, needs to be enhanced if Armenia's long-term security is to be guaranteed.

What does it mean to be resilient? Identifying a definition which fits the purpose of our discussion is challenging; it needs to reflect the complexity of our societies, the dense interconnections that characterise them, the ever-evolving nature of threats faced and, in turn, the endeavours for coherent and collective response to disturbances. David Omand, a retired British senior civil servant who served as the Security and Intelligence Co-ordinator for the Cabinet Office proposes that,

> national resilience, [is] in other words our ability to detect, prevent and, if necessary, to handle disruptive challenges. The depth and breadth of our resilience governs our ability as a nation to face shocks and disruption and to be able to maintain or to restore normal life as quickly as possible (Omand, 2004).

However, like security, resilience is a contested concept, with individuals, communities, businesses, governments and regional and international organisations attributing different meanings to it. The range of definitions for resilience reflects the variety of objects modern societies have wanted to protect (Edwards, 2009). At various points in time and in different contexts, resilience has been understood as implying stability, durability and adaptability in the face of shock and disruption (Giroux and Prior, 2012).

Like security, resilience, is viewed both as an outcome, something that we wish to create, and as a process, something that we carry out. An evolution in the characterization of the resilience concept from an outcome-oriented to a more process-oriented understanding is noticeable (Manyena, 2006). Yet, 'resilience-as-outcome', inherent within objects, individuals or societies, is more often one for which capacity needs to be actively developed, which in turn leads us to an understanding of 'resilience-as- process'.

Accordingly, the plethora of interpretations of what the concept entails makes it difficult to operationalise strategies for resilience. Many societies, however, appear to agree that resilience is important as it governs a nation's ability to face shocks and disruption and to maintain or to restore normal life as quickly as possible (Omand, 2010). The policy approaches, are, at times, imperfectly defined, and yet they have in common a recognition of the diverse nature of risk against which Resilient Nations must organise and with which they must cope. For many Western governments (such as the UK) resilience is understood as an approach to integrate and coordinate a range of aspects of emergency management, including processes of assessment, prevention, preparation, response and recovery so as to provide guidance to existing entities such as buildings, systems and networks (UK Cabinet Office, 2013). Before we can develop the capacity for resilience, however, we need to have a reasonable understanding of what we need to be resilient in the face of, which is where the assessment of risk comes to the fore.

Risk Approach to National Security

Risk-based strategies are at the heart of implementation of resilience. Conceptual frameworks offered in the literature have steered organisations and governments alike towards the deployment of technocratic approaches to resilience. These rely on a comprehensive assessment process to analyse the likelihood and consequences of potentially disruptive events. Risk management promises manageability and control and offers a ubiquitous decision-making framework for the most intricate situations (Power, 2004).

Among the array of material, textbooks and manuals, an international standard (ISO 31000, 2018) stands out as a repository for best practice in risk management. It defines it as a set of

'coordinated activities to direct and control an organization with regard to risk'. The standard describes a systematic process, which, through the execution of a set of iterative activities allows the effective managing of risks at various levels within organisations. Risk management is conceived as a continuous cycle carried out to improve organisational processes, policies, practices and, in turn, learning.

To begin with, risk management requires a framework to clarify how its activities and functions are embedded within the governing structures of the organisation (i.e., the commitment made by top management, the support from stakeholders, the oversight mechanisms, the resources available, and so on). Integration of risk management necessitates statements on mandate, accountability, and roles and responsibility of those involved in the process. Establishing this framework seeks to align strategy and culture of the organisation with its view on risk.

It follows, that the risk management process *per se* is implemented through phases of a risk management cycle.[1]

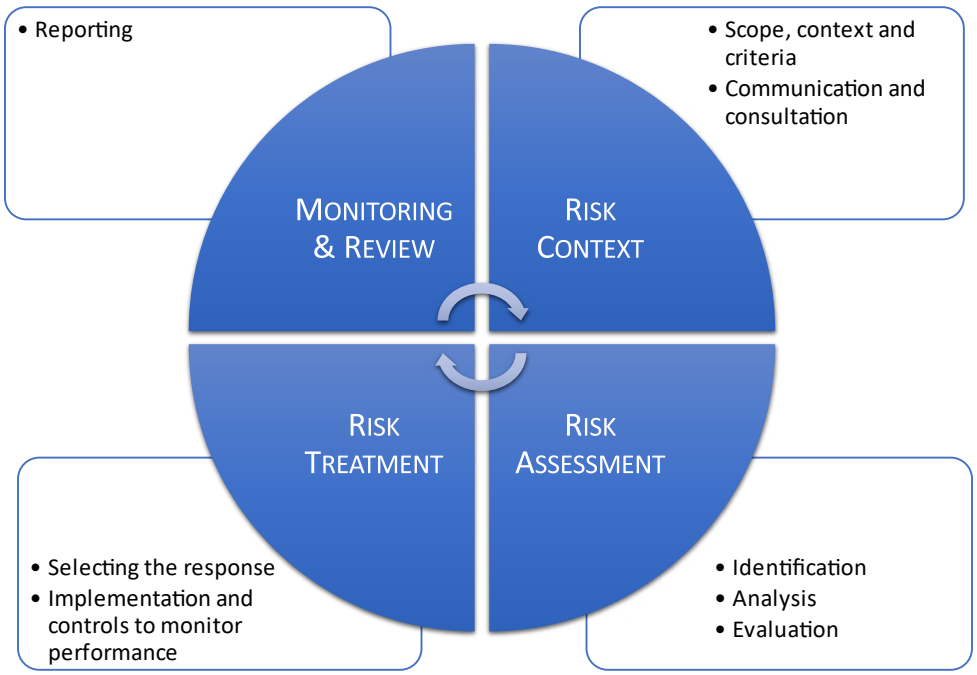


Figure 2.1: The Risk Management Cycle (Source: Authors)

The Risk Management Cycle depicted above was adapted from ISO 31000 (2018) and BS 31100 (2008); it highlights the generic phases in the risk management process which are as follows:

Setting the risk context

This phase concentrates on establishing the scope, context and criteria of the risk management focus (including whether to envisage risks at the strategic, operational, programme or project levels) and determining internal and external factors which influence the management of risks. Determining the organisation's strategic objectives is key at this stage. In doing so, the organisation will also require the determination of programmes which need to be protected as well as the tasks that need to be performed successfully to achieve the strategic objectives.

Relevant stakeholders, those essential to the understanding of the risk, able to promote awareness of it, and to support decision-making need to be found and placed at the heart of communication and consultation approaches. In addition, as the context is clarified, some ground rules and activities may be established. These include for instance: selecting appropriate tools and techniques, determining a schedule for the process and considering questions of risk appetite.

Assessing risks

This phase is concerned with the identification of risks, their analysis and their evaluation. These three activities are not always combined under the banner of 'risk assessment'; yet they feature in the standards considered in this iterative order. Identifying risks consists in uncovering, characterising, and listing elements of risk which can affect the organisation's ability to achieve its objectives. The careful selection of sources of up-to-date information and approaches to identify risks is essential and it is the pre-cursor to the detailed and accurate description of the found risks. Approaches to the identification of risks are numerous: ranging from conventional management tools such as Horizon Scanning, SWOT (strengths, weaknesses, opportunities and threats), PESTLE (political, economic, sociological, technological, legal and environment) analyses to more risk-oriented instruments such as the Delphi technique or structured 'What if?' workshops.

Subsequently, risk analysis consists of the systematic use of information (be it historical data, theoretical models, expert opinions, or stakeholders' insights) to determine the probability and impact of the risk. The analysis process considers the nature of the risk from multiple aspects: uncertainties, risk sources, events, scenarios, controls and their effectiveness. The outcome of the analysis will usually be quantitative whereby consequences and their likelihood are assigned values (although qualitative approaches may also be employed).

The risk evaluation that follows aims to combine, aggregate analysed risks, and compare levels of risk with the risk appetite. This prioritisation process seeks to pave the way for subsequent decisions and treatment options. At this stage, visualisation tools such as risk matrices are used to communicate the outcome of the risk assessment to internal as well as external stakeholders.

Treating risks

Treatment comprises selecting from a set of options available to address risks and then implementing the measure selected. There are numerous treatments of risk – Figure 2.2 shows some archetypal options.



Figure 2.2: Options for the treatment of risk (Source: Authors)

Acceptance of risk can give rise to much discussion within an organisation or a society. This option could be chosen 'because no further worthwhile actions can be devised and the risk is within the risk appetite, or it might be because the only remaining responses are unacceptable for some reason' (BS 31100, 2008: p.30). It can also be associated with the retention of risk which implies retaining the residual risk (including the gains or losses it brings about) without planning for further action or response to it. Reduction or mitigation involve measures to modify risks through actions to control the source, alter the likelihood or dampen consequences. Whilst the option to share the risk involves a contractual re-distribution of the risk with other parties (covering burden of loss or benefit of gain). Lastly, there is the option to take risks in order to realise a positive outcome. This positive outlook on risk is founded on the appreciation of opportunities, and produces responses intended to result in desirable consequences.

Once the treatment options have been selected, their implementation requires planning (implementing risk management decisions is referred to as risk control). The arrangements for implementing mitigation measures normally describe the sequence of actions, the resources required, the list of those who are responsible and accountable, and the performance measures expected in the control of the risk. The implementation plan refers to the review processes to track individual risks and the effectiveness of the measures in place.

Monitoring and Review

In this phase, the necessary information is gathered, compiled and communicated to the relevant stakeholders. Risk reports capture and document risk information. In turn, reports allow the characterisation of the actual residual risk – which should then be assessed in the subsequent iteration of the cycle. The importance of risk reports should not be underestimated as they provide valuable insights on underlying causes, nature and manifestations of risk as well as the effectiveness of treatments. Consistent reporting can than feed into the review of risks in search of continual improvement of processes.

National risk assessments have become ubiquitous strategies to support a country's overall resilience. Risk analyses have become a universal guide to decision-making, covering phases

of anticipation of disruptions through to preparedness, emergency planning and response as well as recovery. Policy makers within governments in many nations use the risk framework to inform them:

> The outcomes have been that national risk assessments have helped to give perspective to the risks facing nations, and to elevate national resilience as a policy priority. As objective, dispassionate, inventories of what would have to be reckoned with in a disaster they have helped to make the case for investment in resilience in an increasingly competitive national security field, and informed the optimal allocation of scarce resources (OECD, 2017: p.57).

However, the risk approach has detractors. Adams (2002) argues that risk management is a 'balancing act', or 'risk thermostat', in which 'perceptions of risk are weighed against the propensity to take risk' (Adams, 2002: p. 15). Yet, institutionalisation of risk management emphasizes practices of risk reduction (Adams, 2002), and if precaution is applied systematically it tends to deny possibilities of seizing worthwhile opportunities, process or activity (Sunstein, 2003). In addition, one should recognise that cost-benefit calculations, which underpin risk analyses, are constrained by the limits of quantification. This point was made by Slovic, Fischhoff and Lichtenstein in 1979. They noted that psychology matters greatly to the comprehension of risk and people's reactions to it. If managers and decision-makers are to manage risk effectively, they need to understand what shapes the perception of risk. Whilst risk assessments bring systematic reasoning and evidence, 'hard facts go only so far and then human judgement is needed to interpret the findings and determine their relevance for the future' (Slovic, et al, 1979: p.14).

Exercise 2.1:

When performing a PESTLE analysis in relation to the impact of COVID-19 on security, one could focus an assessment of risks by concentrating on the TECHNOLOGICAL dimension.

By and large, the global pandemic has altered the risk context; examples include:

- Negative effect on raw material supply and the electronics value chain, potentially leading to disruptions in the manufacturing of weapon systems and platforms;
- Increased use of cloud-based services and teleconferencing software; this, in turn, raises concerns over the routine access to IT capability, the security of end-to-end communications and the increase in cybersecurity risks;
- Changes to the ways in which employers (including governments) manage the workload, wellbeing of and communication with their staff. Some people have been disturbed by disinformation circulating on sharing platforms, whilst others have strongly perceived the impingement of new working conditions on their lives.

Although the identification of risks relevant to security sectors is incomplete, it presents a start-point to the risk assessment process. Can you add details to the analysis of risks relevant to the security sector of your country? Can you the perform the next steps in the risk cycle?

Adaptation for Security

Although national risk assessments have facilitated the resilience of nations, the culture of control these approaches denote does not fully embrace the evolutionary understanding of resilience[2] highlighted in Holling's notions of 'adaptive cycles' and 'panarchy':

> A management approach based on resilience ... would emphasize the need to keep options open, the need to view events in a regional rather than a local context, and the need to emphasize heterogeneity. Flowing from this would be not the presumption of sufficient knowledge, but the recognition of our ignorance; not the assumption that future events are expected, but that they will be unexpected (Holling, 1973: p.21).

Holling's (1973) seminal work inspired much of the social ecological literature upon which the concept of resilience is based (Brand & Jax, 2007). He introduced the notion that the resilience of a system was, in fact, its dynamic capacity to remain in its current 'basin of attraction' - also referred to as its 'stability domain'. Since then, ecologists have directed discussion and thinking in terms of Complex Adaptive Systems. In this framework, another set of assumptions was brought into consideration: that multiple stability domains exist, and that disruption or

stress will move systems from one basin to another (such movement can also be referred to as 'regime shift'). Acknowledgment of regime shifts subsequently leads to an increased interest in the associated 'thresholds' or tipping points. When critical levels of 'driver' variables are reached, the 'normal' functioning of the system is no longer possible or sustainable. Beyond the tipping point, abrupt changes are triggered, and systems head towards alternative system states (Chapin et al, 2009). This has significant importance as some of these thresholds can be irreversible, but are not necessarily detectable.

These issues brought about another trend in resilience thinking that diverged from the idea of stability and single equilibrium: the management of adaptive capacities. At the heart of which is the question: 'how much adaptation needs to (and can realistically) be administered to prevent a system or its parts switching into an alternative state or dynamic stability?' (Davoudi et al, 2012: p. 326). In the Social Sciences, debates emerged as to what was a return to normality and whether it was desirable. In its colloquial use, the term resilience implies stability, but recently the increasing prevalence of the social-ecological school of thought has resulted in an understanding of resilience centred on periodic cycles of change.

For Holling, 'the adaptive cycle therefore embraces two opposites: growth and stability on the one hand, change and variety on the other' (Holling, 2001: p.395). Adaptive cycles depict (metaphorically) the perpetual fluctuations of systems between periods of exploitation, crisis, learning and renewal (Carpenter et al, 2001). The dynamics of this cycle combine across temporal and spatial scales in the idea described as 'panarchy' (Gunderson & Holling, 2002). Gunderson & Holling invented this word as a reaction to the rigid and top-down connotation of hierarchies. In doing so, they acknowledge and refer to the evolutionary hierarchies of nested adaptive cycles operating at different temporal and spatial scales. Dynamic in nature, panarchies imply that a critical change in one cycle at one level can cascade up or down to other levels of the hierarchy through interaction and feedbacks.

The implications for the concept of resilience of 'adaptive cycles' and 'panarchy' are considerable. Through them, scholars have inferred a system's approach to resilience – which, in turn led them to differentiate between 'specified' and 'general' resilience (Folke et al, 2010). Specified approaches to resilience tend to focus on specific adversities or risks and prescribe

protection or mitigation against one or a range of specific scenarios. In so doing, they seek to answer the question in terms of the 'resilience of what to what' (Carpenter et al, 2001). Illustrations of such specified approaches permeate various disciplines interested in resilience. For instance, in psychology this involves individuals' response to stress, trauma or mental illness, and so on; in disaster studies it consists of building defences in communities prone to local risks (be they flooding, drought or other natural hazards); in economics and management studies it relates to business-centric outlook contained within 'Business Continuity Management' (Giroux & Prior, 2012). Thus, for many of these traditions, resilience has come to mean a practice of planning for adversity with risk management at its heart. Often, the stated aim for research is to investigate how to: anticipate and mitigate or reduce risk; improve responses if the risk materialises; and speed up recovery so as to allow systems to stay functioning (Davoudi, 2012).

Example 2.2: COVID-19 as an illustration of 'panarchy'

Post-traumatic stress disorder (PTSD) is a recognised psychiatric disorder that may occur in people who have experienced or witnessed a traumatic event.

The COVID-19 pandemic has been classified as a 'traumatic event of exceptional magnitude that transcends the range of normal human experience with exposure to risk of death' (Dutheil et al 2020: p. 1). Recent studies of healthcare workers (HCW) on the frontlines of COVID-19 treatment have noted increasing susceptibility to acute stress and PTSD. They have been confronted by unprecedented demands, professionally and personally, as they endeavour to manage a disease with unclear aetiology and pathology, no cure, until recently no vaccine, and a high mortality rate (Ibid.). For many healthcare providers there is an urgent requirement to review the support and care given to those who are in the caring profession.

Amongst other things, COVID-19 has highlighted the dependency relationship between the resilience of individuals and the resilience of systems.

The Security-Resilience Nexus: living with uncertainty

So, what does this all mean for our understanding and pursuit of security? Managers of risk, be it to achieve security or resilience, face a fundamental problem of uncertainty – in the face of which their knowledge is incomplete, inadequate, or lacking in some way. Yet, risk management thrives on data and systematic gathering and analysis of information. Boin and Lodge (2016) suggest that it is time for public institutions, including security institutions, to adopt designs that will help them deal more effectively with today's complex threats and

ensuing crises. The model depicted in Figure 2.3 presents a layered approach to Security Sector Resilience. Derived from work dealing with complex adaptive systems, our model categorises three layers, or domains of uncertainty, and the corresponding coping strategies. We acknowledge that the current trends in security and resilience, based overwhelmingly on the management of risk, offer a specified approach to resilience. In the interest of embracing change, we suggest this alternative perspective.

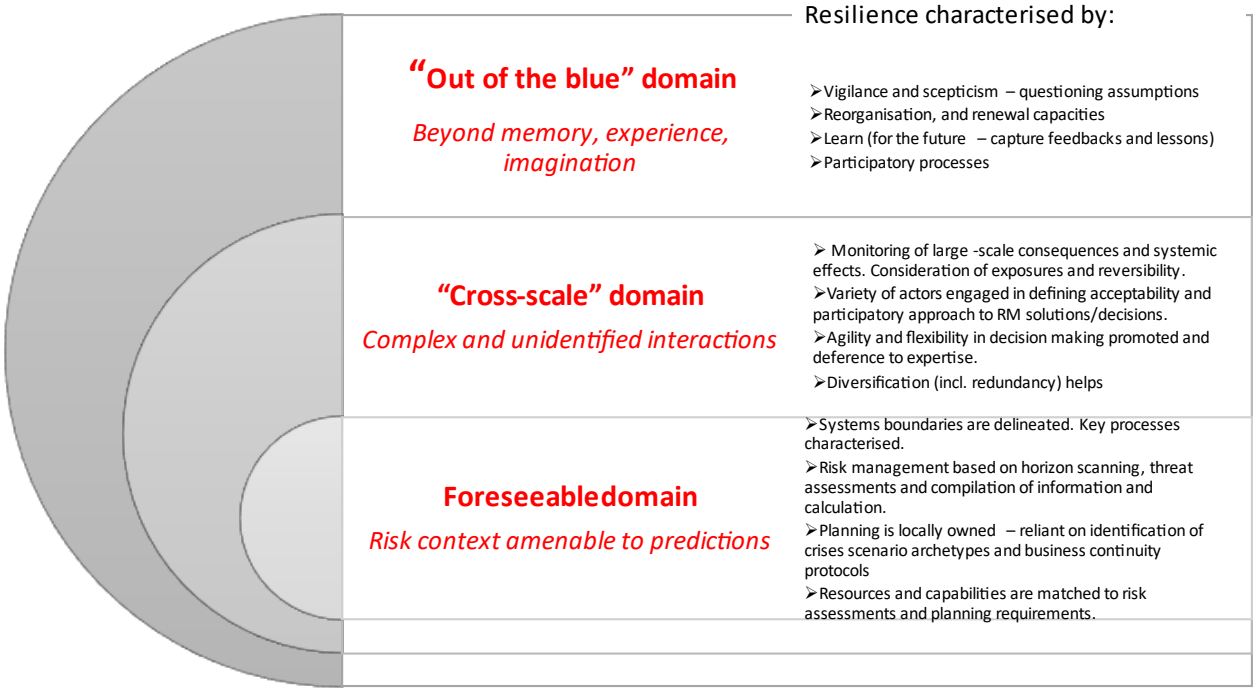


Figure 2.3 – Layered Approach to Resilience of the Security Sector (Source: E. Wilkinson)

The first tier of such a Resilience approach applies to the 'foreseeable domain' where risks are to some extent known and controllable (Kaplan & Mikes, 2012). It is characterised by the development of strategies that answer the question 'resilience of what to what'. Some control is possible because at this domain level there is a degree of predictability. Not all issues will be foreseeable, there will be 'local surprises'. Broader observation and gathering of historical information can help to fill the knowledge gap (Gunderson, 2003). Risk management processes are applicable, but the ignorance of underlying causes or longer-term developments may not allow this type of event to disappear altogether. Adaptations (although limited in their scope) will be possible, but overall, the efforts at this level are geared to maintaining the status quo

(Davidson-Hunt & Berkes, 2003). The key lines of Security Sector resilience activities will be around prevention (through horizon scanning, risk assessment and planning), the development of capabilities, rules-based compliance, and monitoring the effectiveness of measures. Goble et al (2017) suggest that management strategies to deal with the knowledge gap of this tier consist in the reframing or redefining of the risks in recognition, for instance, 'that the original presentation of the hazard was arbitrarily narrow and it is better viewed as embedded in a more inclusive set of problems that should be dealt with all together or the hazard might have a different look when the passage of time is taken into account. Reframing may bring in information from other contexts or alter the questions that are posed' (Goble et al, 2017: p.50).

The second tier of a layered Resilience approach applies to the domain of 'complex and unidentified interaction'. In this domain, cross-scale interactions and complexity dominates. Risk management approaches have limited effect as the nature of the risks cannot be well anticipated and, combined with system's complexity, there is an imperfect understanding of the effectiveness of responses. Although some factual information may exist about the risk problems, interpretations vary on predictions, tolerability and management priorities. Thus, the participation and engagement of appropriate stakeholders is necessary for a sound risk governance framework (Renn, 2017). In addition, proposed interventions need to adopt an adaptive stance by attempting to learn from experience (i.e., interventions are designed to produce knowledge and learning). The heart of the development of a portfolio of adaptive responses is obtaining information on how situations might evolve over time and on what works (Goble et al., 2017). In this domain, the impact of an event is likely to spread between different parts of the system with non-envisioned interactions emerging. Lack of understanding or visibility of interconnections leading to contagion and loss of control are likely to be the dominant challenges in the coordination of any response. Typically, a range of stakeholders will need to contribute to resolving issues. (Davidson-Hunt & Berkes, 2003). Thus, resilience will be provided by improved decision-making based on enhanced institutional flexibility and agility. At times, authority and decisions will need to shift towards those with expertise to allow errors to be spotted and dealt with prior to harmful or needless escalation. Diversity and redundancy are part of the resilience portfolio at this level.

The third of these resilience layers applies to the 'out-of-the-blue' domain, where predictions are precluded due to the sheer fact that no exposure exists to the surprises in this domain. The magnitude of disruption will call for different questions to arise: 'Resilience for whom?' and even 'Why Resilience?' At this level, however, resilience will be characterised by capacity to reorganise and renew. In this context, persistence (in terms of efficiency of return to a previously known status or equilibrium) may not be as important as dynamics (referring to the capacity to change) (Gunderson, 2003). The ability to learn for the future is fundamental to resilience at this level. In short, lesson capture, experimentation and similar activities will be the predominant tools to allow learning beyond present scale (i.e., beyond the here and now). This domain requires a form of 'vigilance' - not simply relating to emerging risks but also in relation to viable strategies. Goble et al. (2017) explain that vigilance involving a mix of scepticism and questioning of existing assumptions can be seen as a pre-requisite to the search for novel strategies. For them, social 'trust and credibility' is equally important as it is threatened by high uncertainty. Institutions can manage this erosion through enhanced participation of major stakeholder's and their engagement in decision-making or negotiation processes.

Exercise 2.2:

Using the layered approach to resilience model, how would you categorise the risks that your country or your security sector institutions face? Do they reside in one domain or several? Are current approaches likely to enhance resilience? If not, what needs to change?

Conclusion

In this chapter we have argued that, beyond our ability to manage risks, the security of our systems is contingent upon the flexibility of our management structures, our willingness to share information vertically *and* horizontally, a recognition of the 'high permeability of institutional boundaries to external environments', as well as an acknowledgement that across state and society there are 'multiple centres of learning' that require active engagement with stakeholders (Goble et al., 2017: p. 52). Over the last two decades alone there have been numerous events that have highlighted the interconnectedness of our societies. We only need to think of the impacts of any one of the following: conflicts such as those in Iraq (2003 -2011), Syria (2011 to present), or Ukraine (2014 to present) to name only a few; the 2008 global

financial crisis; or epidemics such as Ebola (2013-2016) to become conscious of the way in which events, responses and outcomes have the ability to affect us all. The COVID-19 pandemic is simply the latest and loudest alarm bell to ring.

Over the same time frame, recognising the myriad ways in which globalisation has made the security of any one nation dependent upon the decisions taken by its own government, as well as those taken by other states, non-state actors, international organisations and multinational corporations, there has been a concerted effort to promote whole-of-government and whole-of-society approaches to security. Increasingly, there have been calls for whole-of-world approaches to contend with the current and future pandemics, and global warming. The success of any of those approaches requires dialogue and collaboration in order to determine and share the risk and to balance it over time. That will require changes in institutional and political culture. Far too many ministries and security services remain 'stovepiped', hoarding information and knowledge. They simply do not know how to share it. The atomisation of responses to security challenges results in the diminishment of trust in and credibility of government. In the following chapters, our co-authors will return to the themes of governance, policy formation, security architecture, strategic, knowledge, and change management (see Chapters 3, 5, 7, 8, 10 and 14). We need to adapt to survive. From the perspective of one West African civil servant in 2018, that means that resilience should be the ultimate goal of security sector reform.

Notes

1 Although there are differing standards for managing risks, they share common principles. This chapter uses established risk management standards (ISO 31000:2018, ISO/IEC Guide 73:2002 and BS 31100:2008) which are relevant to the context of governance and management of risks across an organisation.

2 In their collection of papers Davoudi et al. explain that 'evolutionary resilience challenges the whole idea of equilibrium and advocates that the very nature of systems may change over time with or without an external disturbance […]. In this perspective, resilience is not conceived of as a return to normality, but rather as the ability of complex socio-ecological systems to change, adapt, and, crucially, transform in response to stresses and strains' (2012, p.302).

Questions to Consider

1. Where does the responsibility for risk assessment reside within your government system?
2. How is that risk assessment employed in the process of policy formation *and* policy implementation?
3. Does your nation pursue a specified or general approach to resilience?

Suggested Reading

Gunderson, L.H. and Holling, C.S., eds., (2002) *Panarchy: Understanding Transformations in Systems of Humans and Nature,* Washington DC: Island Press.

Omand, D. (2010) *Securing the State*, London: Hurst & Co.

References

Adams, J. (2002) *Risk*, Abingdon: Routledge.

Association of Southeast Asian Nations (2018) 'Joint Declaration of the ASEAN Defence Ministers on Strengthening Cooperation, Building Resilience' *12th ASEAN Defence Ministers' Meeting,* 19 October 2018. Available at: https://asean.org/joint-declaration-asean-defence-ministers-strengthening-cooperation-building-resilience/?highlight=Resilience. [Accessed on 27 January 2021].

Boin, A., & Lodge, M. (2016) 'Designing resilient institutions for transboundary crisis management: A time for public administration', *Public Administration*, 94(2), pp. 289-298. DOI: 10.1111/padm.12264.

Brand, F. S., and K. Jax. (2007) 'Focusing the meaning(s) of resilience: resilience as a descriptive concept and a boundary object', *Ecology and Society,* 12(1), p. 23. Available at: http://www.ecologyandsociety.org/vol12/iss1/art23/ [Accessed on 1 February 2021].

British Standard - European Standard (BS 31100) (2008) *Risk management: Code of practice*, London: British Standards Institution (BSI). Available at https://doi.org/10.3403/30191339.

Bush, George H. W. (1990) 'Speech to the Joint Houses of Congress 11 September 1990'. Available at https://www.c-span.org/video/?c4528359/user-clip-george-bush-defines-world-order. [Accessed on 25 January 2021].

Buzan, B. (1991) *Peoples, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era,* 2nd ed., Boulder, CO: Harvester Wheatsheaf.

Carpenter, S., Walker, B., Anderies, J. M., & Abel, N. (2001) 'From metaphor to measurement: resilience of what to what?', *Ecosystems*, 4(8), pp. 765-781.

Chapin III, F. S., Folke, C., & Kofinas, G. P. (2009) 'A framework for understanding change' in *Principles of Ecosystem Stewardship,* New York: Springer, pp. 3-28.

Cleary, Laura R. (2016) 'Half-Measures and Incomplete Reforms: the breeding ground for a hybrid civil society in Ukraine', *Southeast European and Black Sea Studies,* 16(1), pp. 7-23. DOI:10.1080/14683857.2016.1148410.

Davidson-Hunt, I. J., & Berkes, F. (2003) 'Nature and society through the lens of resilience: toward a human-in-ecosystem perspective'. In: *Navigating social-ecological systems: Building resilience for complexity and change*. Cambridge: Cambridge University Press, pp. 53-82.

Davis, James W (2000) *Threats and Promises: the pursuit of international influence,* Baltimore, MD: Johns Hopkins University Press. DOI: 10.2307/798046.

Davoudi S., Shaw K., Haider L.J., Quinlan A.E., Peterson G.D., Wilkinson C., Fünfgeld H., McEvoy D., Porter L. (2012) 'Resilience: A Bridging Concept or a Dead End?', *Planning Theory & Practice,* 13(2), pp. 299-333. DOI: 10.1080/14649357.2012.677124.

De Coning, C. (2018) 'Adaptive Peacebuilding', *International Affairs*, 94(2), pp. 301-317. DOI: 10.1093/ia/iix251.

Dutheil F, Mondillon L, Navel V (2020) 'PTSD as the second tsunami of theSARS-Cov-2 pandemic', *Psychological Medicine 1–2*. DOI: 10.1017/S0033291720001336.

Edwards, C. (2009) *Resilient Nation*, London: Demos.

European Union (2016) *Shared Vision, Common Action: A Stronger Europe, A Global Strategy for the European Union's Foreign and Security Policy*. https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf. [Accessed on 8 February 2021].

Folke, C., Carpenter, S., Walker, B., Scheffer, M., Chapin, T., & Rockström, J. (2010) 'Resilience thinking: integrating resilience, adaptability and transformability', *Ecology and Society*, 15(4), pp. 20. Available at http://www.ecologyandsociety.org/vol15/iss4/art20/. [Accessed on 25 February 2021].

Fukuyama, Francis (1992) *The End of History and the Last Man*. London: Penguin Books. DOI: 10.1177/03058298920210010701.

Giroux, J. and Prior, T. (2012) 'Factsheet: Expressions of Resilience: From "bounce back" to adaptation'. Zurich: Risk and Resilience Research Group, Center for Security Studies (CSS).

Goble, R., Kasperson, R. E., & Ratick, S. (2017) 'How can we best deal with the unexpected?' in: *Risk Conundrums: Solving Unsolvable Problems*, 47. Abingdon: Routledge.

Gunderson, L. H. (2003) 'Adaptive dancing: interactions between social resilience and ecological crises' in: *Navigating social-ecological systems: Building resilience for complexity and change*. Cambridge: Cambridge University Press, pp. 33-52.

Gunderson, L.H. and Holling, C.S., eds., (2002) *Panarchy: Understanding Transformations in Systems of Humans and Nature,* Washington DC: Island Press.

Holling, C. S. (1973) 'Resilience and stability of ecological systems', *Annual Review of Ecology and Systematics*, 4(1), pp. 1-23.

Holling, C. S. (2001) 'Understanding the complexity of economic, ecological, and social systems', *Ecosystems*, 4(5), pp. 390-405.

HM Government (2015) *National Security Strategy and Security and Defence Review: A Secure and Prosperous United Kingdom*. London: Crown Copyright. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data

/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf [Accessed on 8 February 2021].

International Standards Organisation (ISO 31000) (2018) 'Risk Management – Guidelines. International Organization for Standardization – ISO'. Geneva, Switzerland. Available at https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en [Accessed on 17 February 2021].

International Standards Organisation (ISO Guide 73) (2002) 'Risk Management—Vocabulary. International Organization for Standardization – ISO', Geneva, Switzerland. Available at https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en. [Accessed on 17 February 2021].

Kaplan, R., & Mikes, A. (2012). 'Managing risks: a new framework', *Harvard business review*. Available at https://www.nsf.gov/oirm/bocomm/meetings/spring_2018/Managing_Risks_A_New_Framework.pdf [Accessed on 26 February 2021].

Manyena, S. B. (2006) 'The concept of resilience revisited', *Disasters,* 30(4), pp. 434-450.

OECD Publishing (2017) *National Risk Assessments-A Cross Country Perspective*. OECD Publishing. Paris. DOI:10.1787/9789264287532-en.

Omand, D. (2004) 'National Resilience Priorities for UK Government'. Speech of 19 May 2004. London: Royal United Services Institute (RUSI). Available at https://rusi.org/commentary/national-resilience-priorities-uk-government-sir-david-omand [Accessed on 26 February 2021].

Omand, D. (2010) *Securing the State*, London: Hurst & Co.

Owen T. (2004) 'Human Security – Conflict, Critique and Consensus: Colloquium Remarks and a Proposal for a Threshold Based Definition', *Security Dialogue,* 35(3), pp. 373-385. DOI: 10.1177/0967010604047555.

Pettman, R. (2005) 'Human Security as Global Security: Reconceptualising Strategic Studies,' *Cambridge Review of International Affairs,* 18(1), pp. 137–150. DOI:10.1080/09557570500059878.

Power, M. (2004) '*The risk management of everything: Rethinking the politics of uncertainty'*. London: Demos. Available at https://www.demos.co.uk/files/riskmanagementofeverything.pdf [Accessed on 16 February 2021].

Renn, O. (2017) 'Risk Governance: Concept and application to Systemic Risk' in *Risk Conundrums: Solving Unsolvable Problems*, 47. Abingdon: Routledge.

Rousseau, David L (2007) 'Identity, Power and Threat Perception: a cross-national experimental study', *Journal of Conflict Resolution,* 51(5), pp. 744 - 771. DOI: 10.1177/0022002707304813.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1979) 'Rating the Risks', *Environment*, 21(3), pp. 14-39.

Sunstein, C. R. (2003) 'Beyond the precautionary principle', *University of Pennsylvania Law Review*, 151(3), pp. 1003-1058. Available at: https://core.ac.uk/reader/194863940. [Accessed on 15 February 2021].

UK Cabinet Office (2013) 'Resilience in society: infrastructure, communities and businesses'. Available at: https://www.gov.uk/guidance/resilience-in-society-infrastructure-communities-and-businesses [Accessed on 24 February 2002].

UNDP (1994) *Human Development Report 1994*, New York and Oxford: Oxford University Press. Available at: http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf. [Accessed on 24 April 2020].

United States of America (2015) *National Security Strategy*. Available at: https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf. [Accessed on 25 January 2021].

Vasilache, A. (2019) 'Security in the Sovereignty Governmentality Continuum', *Cambridge Review of International Affairs*, 32(6), pp. 681-711. DOI: 10.1080/09557571.2019.1632797.

Walklate, S., McGarry, R. and Mythen, G (2014) 'Searching for Resilience: A Conceptual Excavation', *Armed Forces and Society*, 40:3, pp. 408-427. DOI: 10.1177/0095327X12465419.

Yee-Kuang Heng (2006) *War as Risk Management*, London: Routledge. DOI: 10.4324/9780203970072



https://dspace.org/

Chapter 2: If you can’t be secure, be resilient

Wilkinson, Edith; Cleary, Laura R.

2021-11-29
Routledge
https://doi.org/10.4324/9781003137061
Wilkinson E, Cleary LR. (2021) Chapter 2: If you can’t be secure, be resilient. In: Managing Security Concepts and Challenges, Abingdon, UK: Routledge

Downloaded from a DSpace repository. https://dspace.org/