Deterrence - Concepts and Approaches for Current and Emerging Threats,
Switzerland: Springer, Cham, p. 19-33.
DOI:10.1007/978-3-030-29367-3_2

# Resilience and Deterrence: Exploring Correspondence Between the Concepts

EdithWilkinson 1✉Email e.m.wilkinson@cranfield.ac.uk
1 Cranfield University Shrivenham UK

## Abstract

Classic theories of deterrence do not envisage the concepts of resilience and deterrence as even remotely connected. However, these two notions may not be poles apart and may, in fact, offer complementary perspectives in envisioning options for dealing with the security challenges of the twenty-first century. This chapter explores the correspondence between the two concepts. Firstly, it discusses definitions and key tenets of these concepts in relation to security. Then, it goes on to review what differentiates and what links these concepts in terms of the risk approach each presents; this includes an examination of rationality in deterrence and resilience frameworks as well as looking at the growing acknowledgement that their evolution is influenced by systems thinking. The chapter then considers in what way *deterrence theory* and the emerging *resilience theory* display areas of complementary and mismatch. This is achieved by examining how, on the one hand, both approaches may be able to support one another and, on the other hand, how the significance of change and transformation in both frameworks can provide pointers to where future thinking might lead.

Classic theories of deterrence do not envisage the concepts of resilience and deterrence as even remotely connected. However, these two notions may not be poles apart and may, in fact, offer complementary perspectives in envisioning options for dealing with the security challenges of the twenty-first century. This chapter explores the correspondence between the two concepts. Firstly, it discusses definitions and key tenets of these concepts in

relation to security. Then, it goes on to review what differentiates and what links these concepts in terms of the risk approach each presents; this includes an examination of rationality in deterrence and resilience frameworks as well as looking at the growing acknowledgement that their evolution is influenced by systems thinking. The chapter then considers in what way *deterrence theory* and the emerging *resilience theory* display areas of complementary and mismatch. This is achieved by examining how, on the one hand, both approaches may be able to support one another and, on the other hand, how the significance of change and transformation in both frameworks can provide pointers to where future thinking might lead.

## 1. Deterrence and Resilience Are Contrasting Cornerstones of Security

Deterrence is not new, nor did it start in the Cold War when the balance of power characterising the era was based on the notion central to this concept: that punishment or threats discourages wrongdoers (Bendiek and Metzger 2015). States have long used deterrence amongst other standard practices such as diplomacy or espionage to shape their relations. The turn of the twentieth century sees growing interest and efforts to qualify the use and value of deterrence as an instrument for security policy. Studies and considerations have multiplied in an effort to clarify what the Chinese strategist Sun Tzu described as "*the successful practice of deterrence […] the highpoint of skill – superior even to winning military victories*" (Payne 2010; p. 217). Research into the topic became widespread during the Cold War era when investigations broadened to issues of "*motives and perspectives that incite preparations to use attacks and war in conflicts; things that make deterrence work or fail; how best to apply it, and what to avoid; the circumstances in which it is most properly used or not; and how to reduce chances of deterrence failures*" (Morgan 2012; p. 87). Still today – and perhaps even more so in the post-Cold War and 9/11 world of asymmetric threats – the search for the place of

deterrence in the twenty-first century security environment still attracts academic attention.

Defence doctrine, often where deterrence has gained prominence, explains the military instrument of power and its utility and locates it against government's means to secure policy ends. Deterrence and coercion are both strategies by which a nation can respectively dissuade or encourage another's course of action. However, the pursuit of strategic goals involving Defence or the 'military instrument' will ultimately fit in a broader political setting (UK Chief of the Defence Staff 2014). Time and again, the absence of wars between great powers has been upheld as the confirmation of the success of deterrence strategies, noting that "*deterrence did not just prevent wars but was achieved via war*" (Morgan 2012; p. 86). According to Morgan (2012) deterrence represented such an underpinning to national security management that approaches to its strategic (relating to nuclear threats) and non-strategic (relating to more conventional threats) implementation attracted more attention and resources than many other instruments in international politics. The reality of the post-Cold War era has seen a redefinition of international security management by a coalition of Western powers being sought. Deterrent instruments in the hands of these powers prove to be of little value in an age of terror groups and unconventional conflicts. Interestingly, advice once given by military experts is increasingly provided by security specialists.

Nevertheless, the United States still appears to be committed to the idea that deterrence should remain the cornerstone of global and regional security – notwithstanding their willingness to spread the burden of leading the provision of such core deterrence capabilities. This is all the more noticeable in the light of recent news headlines, such as Russian interventions in Crimea and Ukraine or the development of the DPRK (Democratic People's Republic of Korea) missile technology and strike capabilities. For the US, the danger is not so much one of a "*nuclear attack against the U.S. homeland but from the possibility that nuclear-armed adversaries will use the threat of escalation to the nuclear level to act more aggressively in their regions and prevent the United*

*States from coming to the defense of its allies and partners*" (Einhorn and Pifer 2017; p. iv).

Turning to resilience, its documented Latin roots ('resilire' meaning 'spring' or 'bounce back') give the concept a sense of being established – yet it is very much seen as a current political catchword and still evolving as a concept in the security domain. To better grasp the concept Giroux and Prior (2012) identify five key dimensions, reflecting the various disciplines of the study of resilience. For them, there are five fundamental areas of resilience and, together, they encapsulate the relationships and dynamics of modern society:

*The "**engineering/physical** [dimension] refers to physical infrastructure and systems while the **psychological** dimension refers to the social domain that focuses on the individual. We then turn to perceptions of 'bouncing back' within the **business/economic** world – drawing from debates on business continuity management and business leadership/management. […]. This relates to the overall operations of businesses and the role of management. The final two sub-sections on **ecological** […] looks at how research on ecological systems has found that bouncing back from shocks can be both static (strict ecological process) or dynamic (in socio-ecological systems) and the expression of resilience is dependent largely on the scale of enquiry (predator-prey interaction versus human interaction in natural ecosystems). Similarly, […] research on **community** resilience reveals the importance of adaptive learning and transformation."* (Giroux and Prior 2012; p. 6)

On the whole, from a social science outlook and away from its origins in the natural sciences, the most commonly found definitions refer to the characteristics of societies to deal with disruptions – normally global threats such as economic crisis, climate change and international terrorism (Haimes 2009). Focusing on the UK as an example, the concept of resilience evolved predominantly in the public policy sphere of civil contingencies (under the auspices of the Cabinet Office). For the UK government, in 2004, the idea for building resilience was "to reduce the risk from emergencies so that people can go about their

business freely and with confidence" (Cabinet Office 2011a). The government's activities focused on assisting civil protection practitioners to support the work that goes on across the United Kingdom to improve emergency planning and preparedness (Cabinet Office 2013). It is worthy of note that the events of 9/11 greatly influenced resilience thinking by introducing "*a form and severity of terrorism not previously encountered in the UK – a dimension where the terrorist has no concern for their own life and is intent on causing as many fatalities as possible*" (O'Brien and Read 2005; p. 354). The consequence of this is that international terrorism has become an obvious priority for resilience strategies, not just in the UK, but throughout the Western world.

Although a recent addition, resilience features prominently at the heart of contemporary national security. Resilience is thought of as an antidote to new risks and threats from diverse origins – from natural disasters to cyber-attacks – and is thus a critical component of national security strategies in Western powers. Resilience is envisaged as a capability in the hands of public authorities, but also more broadly in society because the protection of critical infrastructure is largely dependent on the private sector – companies that operates and often own such infrastructure (Omand 2008). The broadening of resilience beyond the idea of just 'securing the functioning of the state' is noted by Joseph in his comparison of UK and French implementation of the concept and who remarks "*Resilience is said to have a social dimension, located not only in the state but also among the actors of civil society. Resilience is both an objective of the state and a state of society*." (Joseph 2013; p. 257). Such an understanding of resilience, one promoting a new relation between government and society based on a more proactive culture towards security issues, is, according to Joseph (2013), a contentiously neoliberal concept that has to do with governing populations and assigning responsibilities to different actors.

In examining the definitions and understandings of both deterrence and resilience, it is noticeable that both concepts are key components of modern national security. Perhaps the former is more attached to external manifestations of security, whilst the

latter is fundamentally focussed on internal national mechanisms. By embracing approaches that involve a broad set of stakeholders and actors (which goes beyond what has hitherto been the sole domain of State actors), resilience provides new thinking and new instruments for managing uncertainty and security challenges. In many ways, resilience can be understood as a pragmatic way to tackle globalised threats to national security.

## 2. Deterrence and Resilience as Risk Approaches

Albeit in differing ways, deterrence and resilience theories have risk at their core. The fundamental processes at the heart of UK resilience[1] relate to on-going risk identification and analysis that is essential to the anticipation and management of disruptive events. In practical terms, these processes allow the UK government to define its capabilities programme through which the government seeks to build resilience across all parts of the UK. To all intents and purposes, the 2008 National Security Strategy explains the Government's approach to resilience entailing in a risk management process set out in the 2004 Civil Contingencies Act. The Act lays out "*responsibilities of frontline responders to assess local risks and publish them in community risk registers; to prepare plans; to make arrangements to warn and inform the public in the event of emergencies; and to promote business continuity*" (Cabinet Office 2008; p. 41). Resilience has, since 2004, grown beyond the domain of emergency response and it is now the responsibility of risk managers in organisations of all types and sizes, public and private, to plan and prepare their outfits or systems to return to a normal functioning state quickly after a disturbance. To a great extent, resilience is approached in a holistic manner involving stakeholders from all parts of society – be they governance structures, civil society, communities and individuals – to play their role in the mitigation and response to current and future threats. The novelty in the approach to risk relies on the expertise and judgement of practitioners who perform risk

assessments and then prioritise those risks and publish their written justification to allow public scrutiny. The communications relating to risks taking place between authorities and the public at local level has, therefore, become a condition of building resilience (O'Brien and Read 2005).

Equally, traditional deterrence strategy relies on leaders considering rationally the risks and costs of war (Fearon 1995). The frequently cited definition (found in US doctrine) sees deterrence as the "prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits." (U.S. Joint Chiefs of Staff 2016). Essentially, the mechanism relies on calculations of what gains and consequences follow a certain course of action. Thus, a fundamental assumption underpinning this framework is that actors involved act rationally and will weigh up their options so as to optimise their outcomes (Achen and Snidal 1989). Here the risk approach consists of calculating how much is enough to deter our adversaries from action against us and to fulfil our security needs. At the height of the Cold War the calculations led the US to determine the adequate[2] nuclear capability to "assure destruction" of the Soviet threat (Payne 2010; pp. 217–218). Here, an interesting difference can be noted, in that deterrence is an instrument predominantly framed from the perspective of the role of the state. Admittedly, non-state actors are increasingly the subject of interest of new forms of deterrence as it is thought that they too can be subject of political 'influence' if not deterrence in the customary sense (Brimmer 2008). Here the issue of "un-deterrability" of some adversaries is paramount. Much research has been geared to understand this phenomenon and some link it to issues of communication (Rhodes 2000). Hence, in a comparable way to resilience, the achievement of deterrence relies in part on credible calculations supported by effective communications.

## 2.1. Rationality in Deterrence and Resilience Frameworks

The importance of perception in people's sense and judgement of

dangerous situations has been the focus of much research in the past 40 years. Stein (2009) refers to this trend as the 'cognitive revolution'. Seminal papers have pointed to limits to rationality and the existence of heuristics used when thinking and making decisions under uncertainty (Tversky and Kahneman 1974; Slovic 1987). This area of research has shown how much richer than expected by experts is the conceptualization of risk by lay people. Calculations reflect sophisticated and compounded concerns on the voluntariness, dread, knowledge, controllability of the risk. In addition, biases introduce errors in decision making and affect the assessment of probability or impact of events. Ultimately, they lead to judgments based on information of limited validity.

The rationality of states waging war (or preparing to do so) has been long discussed and rationalist arguments appear deficient. War is costly and risky, so, why do rational states fail to favour negotiated settlements (Fearon 1995). Understanding some of the flaws of rationality leading to conflicts will provide some insights as to why deterrence fails. A number of studies point to the paradoxical irrationality described as "*the propensity of leaders to go to war in conditions where they are likely to lose*" (Lebow 2007; p. 12). Lebow further argues that in the 30 wars fought since 1945 less than a third had achieved their war aims and as was the case the Vietnam War "*the United States won every battle but still lost the war*." Lebow's interpretation is that imperfect or incomplete information is not always the root cause of deficient decision-making processes. All too often leaders focus on their own political goals and subsequently offer justification to their opponent's tactics: "o*nce committed to challenges, they engaged in bolstering and other forms of post-decisional rationalization, and became even more insensitive to information and warnings that suggested their challenge was likely to end in disaster*." (Lebow 2007; p. 8). Fearon (1995) also expressed similar views on miscalculations about relative power that only war can resolve. Such miscalculations reflect the existence of incentives to misrepresent, the belief of an opponent's (un)willingness to fight or a broken-down commitment to peace negotiations. For Rhodes (2000),

rational calculations are imperfect not only in the assessment of risks of a course of action but also in the estimation one has of the control the risks of any option. That is to say that the "*desire to control risks and avoid policies that threaten open-ended commitments and costs has important implications for the kinds of military options that risk-averse potential aggressors find attractive or unattractive.*" (Rhodes 2000; p. 244). Defence doctrine encapsulates the limits to rationality in a short warning to its military commanders: "*Deterrence and coercion strategies will be contested and commanders must understand the weight of effort an opponent will apply to achieve their aims."* (UK Chief of the Defence Staff 2014). Opponents' interests, their perception of the balance of power, awareness of bargaining space and alternative outcomes available to them, as well as their sense of gains and losses are all part and parcel of calculations. Stein (2009) points out that at the heart of rational decision making lies a careful examination of evidence and a thorough information screening and management process. However, she notes that neuroscience and psychology studies tend to converge in showing the difficulty decision makers have in practice to be logical and to weigh the evidence (without biases and intuitive processes often used to interpret evidence[3]) in a coherent and consistent manner.

As seen earlier, risk management can be envisioned as an entry point in the implementation of resilience (Mitchell and Harris 2012). It is argued that the very essence of managing risks presents weaknesses. Jaeger (2010) suggests that applying general principles and formulas in defining preventative actions to guard against particular risk contexts is laden with difficulties. Mitigation measures are the result of the computation of hypothetical scenario and complex calculations combining probability and utility. Defining rational decisions in the context of disaster management and resilience policies, argues Jaeger, will require more research.

Another significant matter is that the illusion of rationality when dealing with risks deceives societies. This view is one put forward by Adams (1999) who refers to risks, particularly those that are not intuitive or directly perceptible (such as climbing a tree), being left to the judgement of "experts" whose analyses are informed by

scientific information. The authority of scientific and rational expert views has led risk management to be concerned predominantly with the conversion of all risks into numerical forms disregarding the notions of rewards. This institutionalisation phenomenon of risk management is far reaching and has profound effects, which Adams summarises in writing: "*Institutions – government departments or large commercial enterprises – usually assign the job of risk management to particular people or departments who have no (or very little) balancing responsibility and rarely consider rewards to be gained from particular actions*." (Adams 1999; p. 12). This view builds on the idea of social construction put forward by Douglas and Wildavski (1982).

The fundamental question behind the issue of social selection is one that focuses on who would carry out such selection and prioritisation of risks and why. According to this argument, the mobilisation around certain risks allows certain directions and public concerns be prioritised – thus risk acceptability is a political issue (also referred to as a construction of risks). Similarly, Furedi (2002) denounces a culture of fear, arguing that greater security and safety in modern societies has developed through innovation and experimentation rather than via risk avoidance and obsessive quantification.

Amongst the numerous works on biases and influences on risk perception, Slovic (1987) describes how the perception and acceptance of risk is influenced by social and cultural factors such as friends, family and other respected public or private individuals. Slovic's research on risk from a psychological perspective exposes that mental strategies – heuristics – often developed in order to deal with uncertainty and assist in decision-making are, in fact, persistent biases in the perception of risks. This has fundamental consequences on the public management of risk through the forecasting of acceptance and oppositions. Whilst additional information about hazards will influence public assessments, it is also important to take into account heuristics such as: risk and benefit tend to be positively correlated[4] (Slovic and Peters 2006). Consequently, this calls for the inclusion of risk communication about prevention and treatment of risk as integral part of risk

management.

## 2.2.
## Deterrence and Resilience Frameworks and Systems Thinking

Systems thinking has permeated in the resilience domain. The frameworks attached to systems theory relate to the examination of processes, linkages and interactions between the parts (or components) of a system. Defining the system also requires delineating its boundaries and, thereafter, allows the investigation of relations with its environment (open systems that have recognised links with their environment are thought to be more common and realistic).

Although this had long been the case in the ecological tradition, the exploration of systemic processes and complex interactions that generate resilience is a more recent trend in social science; the broadening of perspectives led to looking at resilience in terms of change and adaptation. This emanated from the ecological and social ecological traditions (Walker and Salt 2012; Folke 2006) where "*resilience is the capacity of a system, be it an individual, a forest, a city or an economy, to deal with change and continue to develop. It is about how humans and nature can use shocks and disturbances like a financial crisis or climate change to spur renewal and innovative thinking*". (Stockholm Resilience Centre 2017). Giroux and Prior note the importance of this outlook: "*From this perspective, resilience is an adaptive process characterised by systemic re-organisation, renewal and development – where equilibrium or a steady-state response is neither anticipated nor desired*" (2012; p. 10).

For Joseph (2013) the growing literature on the adaptation of social systems presents challenges. It encourages citizens to take active role and responsibility in ensuring the needed changes take place in order to meet face and absorb shocks. For him, the concept of resilience shows its liberal side through its fundamental acceptance of a situation and its leaning on individuals and not only on institutions to maintain an 'acceptable' level of function. Nevertheless, the notion of the 'dynamics of systems' fits with a

growing consensus that today's societal challenges are globalised and are exacerbated by complex interconnections. Unsurprisingly, the study and further implementation of resilience goes beyond mere crisis management, it entails the grasp of the system's internal complexity and of the interconnection the system has with its environment. Giroux and Prior encapsulate the intricacy of building systemic resilience: "*It likely calls for a multi-layered approach to resilience development (or maintenance) since it is concerned not only with ensuring infrastructures are resilient, but that these are operated and used by resilient communities, who in turn are buoyed and serviced by resilient businesses and economies*." (2012; p. 14).

The broadening of resilience strategies beyond emergency management is noticeable in the UK. The government recognises that resilience in society concerns infrastructure, communities and businesses; thus, the delineation of the system boundaries now includes entities such as buildings, systems and networks (Cabinet Office 2014). It is also visible in the realm of security. Prior (2017) explains that new security challenges for NATO members are to be considered in the light of 'hyper-connectivity' and interdependence. It is, therefore, vital that NATO is coherent in its drive for increased resilience and that "*it recognizes the need for distributed responses across the large number of actors responsible for managing and protecting critical infrastructures: a space where threats are not dealt with by solely relying on a military monopoly*." (Prior 2017; p. 2). Hence, the effect of system thinking and broader approaches is a shift in emphasis away from purely military solutions to security. Equally, the broadening of perspective induces a change in security management approaches based on prevention and acknowledging the limited power of centralised structures. The latest resilience approaches attempt to be less specific (than traditional risk management would normally prescribe) and more generic by acknowledging "*the existence and persistence of existing risks (anticipating) and the necessity of understanding systemic vulnerability in order to prepare for potential future shocks and disturbances (adapting)*" (Prior 2017; p. 3).

As noted earlier, deterrence theory evolved through waves of questioning and conceptual development. Knopf (2010) reminds readers of the initial three waves[5] in deterrence research and suggests that the fourth wave finds its origin in the events of 9/11 and focuses on the problem of asymmetric threats and great powers dealings with rogue or weak states and terrorists (including in the context of regional rivalries). Consequently, deterrence moved away from attempts to calculate and measure the number of weapons or a specific capability to deter against a particular threat at a particular time (Payne 2010). As opponents and contexts change, there has been renewed interest for 'deterrence by denial',[6] which fits well with the idea that resilience and flexibility in society meets more appropriately today's deterrence requirements. Knopf affirms that "*bolstering societal resilience is especially important. When a society can demonstrate the ability to withstand terrorism, it sends a message that using this tactic will not enable terrorist organizations to achieve their goals*." (2010, p. 12).

In a sense, this is an acknowledgement that specified approaches (e.g. deterrence by retaliation or punishment) are deemed as being too narrow and require clear positioning as to what threat is acceptable and what is not. In contrast, 'deterrence by denial' allows a form of systemic thinking and denotes the need to redefine boundaries of the systems in focus (the deterred as well as the deterrent). Just as 'deterrence by denial' broadens the approaches to deterrence, so does the concept of 'extended deterrence'. Such arrangements allow states to extend deterrence through formal and informal alliances – such as the EU and NATO. The extension of boundaries is problematic in that it flags up issues of credibility[7] at the heart of a deterrent posture.

## 3.
## Correspondence Beyond Risk – Complementarity and Mismatch

Risk tools have matured over centuries of mathematical discoveries and have offered humanity methodologies to understand their

environment and to some extent how the past could inform the future (Bernstein 1996). However, in today's reality of a globalised and highly interactive world, the effectiveness of strategies based on scenario planning is debated. Not surprisingly, both deterrence and resilience have evolved towards a broader scope to underpin their approaches. Accordingly, the conceptualisation of both deterrence and resilience is moving away from risk and its technocratic and formulaic risk management tools now perceived to be restrictive in their offer.

## 3.1. Areas of Complementarity

Building on the above, suggestion that the two concepts are, in fact, complementary is to be expected.

For Juncos (2017), complementarity is fundamental: building resilience of the developing world is a way to increase the security of the developed world – hence reducing its need for deterrence. Gearson (2012) actually contends that resilience can be considered as an element of deterrence. For him, resilience strategies – through their effect on society, businesses and infrastructure – can be likened to the hardening of targets.[8] Communication or messaging become particularly important in this respect; the challenge being to convey that resilience measures (here understood as the ability to cope with unexpected events) offer protection and long-term benefits to society by convincing would-be terrorists that their desired effect will not be achieved. Bendiek and Metzger (2015) also converge with that view and propose the term 'deterrence-by-resilience'. In the context of cyber security, Bendiek and Metzger argue that the new domain of cyber-defence is so fast evolving and complex and, consequently, there is a lack of clarity and impunity for attackers, which acts as a major block for the implementation of effective deterrence strategies.[9]

Again, in the cyber context, Bologna et al. (2013) suggest moving from a protective approach, referred to as "fortress", where all acceptable precaution is taken, to one of "resilience" where protective, preventive, and deterrent safeguards are in place, but have limitations. In recognising that mitigation and protection

measures are not always effective, Bologna et al. point to the importance of response, recovery, and restorative action in a resilience approach. This resigned admission is one deplored by Joseph when he criticises the UK National Security Strategy's fatalistic claim that because risks are unpredictable, and cannot all be prevented, society at large should be involved in the process of risk management and responsible precautionary action. For him, although, "*this sounds like a positive approach, but it actually encourages a rather passive attitude. It uses the idea of an external threat to encourage individual adaptation. People are encouraged to engage actively with a wider situation that is deemed beyond their control. Hence the emphasis is on adapting to and exploiting a situation, rather than trying to change the wider social condition. Resilience, in contrast to something like resistance, implies the acceptance of a situation*." (Joseph 2013, p. 262). In a similar vein, Prior notes that in the context of NATO whilst "resilience is sometimes viewed almost as a panacea to anticipating uncertainty, reducing vulnerability and adapting to events – but it must be considered as a transformative process" (2017, p. 4).

## 3.2.
## Areas of Mismatch or Divergence – The Significance of Change and Transformation in Deterrence and Resilience Theories

It is noticeable that the recent broadening of the deterrence and resilience concepts has meant that both concepts are now turning to adaptive and transformative outlooks. In the resilience domain, there are many debates on how far prevention, quick response and recovery constitute 'measures' of resilience when in fact capacity to adapt and transform are potentially better indicators systems resilience. Giroux and Prior talk of a continuum of the expression of resilience with 'bouncing back' at the 'static' end; where the systems' functions are characterised by stability. At the other end of the continuum, where resilience is expressed through system dynamics and is demonstrated by the ability of system to change as a result of learning (2012; p. 11).

With regards to deterrence theory, change and transformation is not so prominent conceptually, yet, Morgan notes *"… with respect to actually using deterrence, much more interesting and innovative is how the western bloc is no longer status quo-oriented, fending off challenges to the established order. Instead, the West vigorously promotes democracy, open societies and economies, market systems and respect for human rights, in keeping with democratic peace theory and related liberal notions in which spreading those values and practices is the fundamental basis for a peaceful and secure international politics"* (2012; p. 90).

Makarenko (2008) points to two areas for the development of adaptive capacities relevant to deterrence. Makarenko's primary focus is on the dynamic nature of the relationship between crime and terrorism and how the study of their interaction reveals networks that extends from an international to community contexts.[10] She argues that the nature of terrorist and criminal organisations is adaptive and flexible; but that counter-measures nations adopt are not. Hence her suggestion is to adopt a more flexible approach context of anti-crime and counter-terrorism policies. In particular, Makarenko submits the idea that valuable intelligence and insight would be gained through the observation of crime patterns particularly with regards to financing.[11] Perhaps, the proposition to introduce delays in an approach based on 'deterrence-by-punishment' to allow an approach of 'deterrence-by-denial' to emerge is believed to bring about adaptation and benefits in the long run.

The study of resilience in the socio-ecological tradition provides interesting pointers in relation of adaptive and transformative capacity of systems. Davidson-Hunt and Berkes (2003) remind us of a typology of responses to surprises. The socio-ecological literature suggests that there are three types of surprises. The first type is described as 'local' and is generated by lack or narrow exposure (in time or space) by a particular system. Response strategies to these surprises involve broadening observation and information locally about the surprise (Gunderson 1999; Folke et al. 2007). Accumulation of knowledge is generally sufficient to allow risk-management-based strategies to deal with these surprises

that are believed to have a statistical distribution. The second type of surprise, referred to as ‘cross-scales’, occurs in the context of interconnection amongst scales when “local variables coalesce to form a regional or global pattern, or when a process exhibits contagion” (Folke et al. 2007).[12] Adaptations to this type of surprises require the coordinated effort of many stakeholders and although they may be common, they are controversial in that they require ad hoc policy measures if appropriate institutions are not available or are readily formed (Folke et al. 2007). The third type of surprises precludes predictions because of the genuine novelty the present. As such, the ‘never-seen-before’ phenomena experienced means that preparation, prevention or pre-adaptation is impossible (Berkes et al. 2003). Coping with this type of surprise requires systems to have developed capacities to reorganise, learn and renew.[13]

## 4. Concluding Comments

This chapter has offered a review of deterrence and resilience, an undertaking which is topical – as both concepts have developed independently of each other, albeit in similar ways. On closer examination, it appears that both are cornerstones of security strategies – perhaps with their most significant difference being their referent object (deterrence being almost exclusively a matter for States). They both have risk at their heart and involve the management of risks and uncertainty. Consequently, their shared major shortcoming is the limitation of rationality upon which risk management is built. New patterns have seen increasing references to system thinking in both concepts (although for resilience, ecology and other natural sciences had adopted system theory from the outset – the principles have only permeated recently into the social science understanding of resilience). As a result, issues of system boundaries and system dynamics have influenced the evolution of current thinking. The conceptual approaches have broadened and are impacting upon current practice. It is clear that the concepts can be seen as complementary, in particular in the

light of a globalised world with hybrid or asymmetric threats. Complementarity may be useful to policy makers, yet it is the notion of change that will bring about the biggest promises in the evolution of these concepts. How are the ideas of adaptation and transformation embraced in these concepts? There, the study of resilience may provide some interesting pointers for the future.

# References


Achen CH, Snidal D (1989) Rational deterrence theory and comparative case studies. World Polit 41(2):143–169

Adams J (1999) Cars, cholera, and cows. Policy Anal 335:1–49

Bendiek A, Metzger T (2015) Deterrence theory in the cyber-century. Lecture notes in informatics for INFORMATIK 2015. *Gesellschaftfür Informatik*, Bonn. Retrieved on 22 December 2017 at https://dl.gi.de/bitstream/handle/20.500.12116/2216/553.pdf?sequence=1

Berkes F, Colding J, Folke C (eds) (2003) Navigating social-ecological systems: building resilience for complexity and change. Cambridge University Press, Cambridge

Bernstein PL (1996) Against the gods: the remarkable story of risk. Wiley, New York

Bologna S, Fasani A, Martellini M (2013) From fortress to resilience. In: Martellini M (ed) Cyber security. Springer briefs in computer science. Springer, Cham

Brimmer E (ed) (2008) Five dimensions of homeland & international security. Center for Transatlantic Relations, Johns Hopkins University, Washington, DC

Cabinet Office (2008) The National Security Strategy: security in an interdependent world. Cabinet Office, London. Retrieved on 22 January 2018 at www.official- documents.gov.uk/document/cm72/7291/7291.pdf

Cabinet Office (2011a) Keeping the country running: natural hazards and infrastructure. Cabinet Office, London. Retrieved on 22 January 2018 at http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61342/natural-hazards-infrastructure.pdf

Cabinet Office (2011b, September 7) UK resilience. [Website]. Retrieved on

20 June 2019
at http://webarchive.nationalarchives.gov.uk/20110907105059/http://www.cabinetoffice.gov.uk/ukresilience

Cabinet Office (2013, February 20) Guidance: emergency response and recovery. Website. Retrieved on 3 August 2017
at www.gov.uk/guidance/emergency-response-and-recovery

Cabinet Office (2014, December 14) Guidance: Resilience in society: infrastructure, communities and businesses. Gov.uk website. Retrieved on 23 January 2018 at https://www.gov.uk/guidance/resilience-in-society-infrastructure-communities-and-businesses#history

Davidson-Hunt IJ, Berkes F (2003) Nature and society through the lens of resilience: toward a human-in-ecosystem perspective. In: Berkes F, Colding J, Folke C (eds) Navigating social-ecological systems: building resilience for complexity and change. Cambridge University Press, Cambridge, pp 53–82

Douglas M, Wildavsky A (1982) Risk and culture: an essay on the selection of technical and environmental dangers. University of California Press, Berkeley

Einhorn R, Pifer S (2017) Deterrence requirements: toward a sustainable national consensus, Working Group Report, edited by Brookings Institution, September 2017. Retrieved on 22 January 2018
at https://www.brookings.edu/wp-content/uploads/2017/09/fp_20170920_deterrence_report.pdf

Fearon JD (1995) Rationalist explanations for war. Int Organ 49(3):379–414

Folke C (2006) Resilience: the emergence of a perspective for social–ecological systems analyses. Glob Environ Chang 16(3):253–267

Folke C, Pritchard L, Berkes F, Colding J, Svedin U (2007) The problem of fit between ecosystems and institutions: ten years later. Ecol Soc 12(1):30. Retrieved on 22 January 2018
at http://www.ecologyandsociety.org/vol12/iss1/art30/

Furedi F (2002) Culture of fear. Risk-taking and the morality of low expectation. Continuum, London

Gearson J (2012) Deterring conventional terrorism: from punishment to denial and resilience. Contemp Secur Policy 33(1):171–198

Giroux J, Prior T (2012) Factsheet expressions of resilience: from “bounce back” to adaptation. Report. Risk and Resilience Research Group Center for Security Studies (CSS), ETH Zürich. Retrieved on 22 December 2017

at https://doi.org/10.3929/ethz-a-009978930

Gunderson L (1999) Resilience, flexibility and adaptive management – antidotes for spurious certitude. Conserv Ecol 3(1):7. Retrieved on 22 January 2018 at http://www.consecol.org/vol3/iss1/art7/

Haimes YY (2009) On the definition of resilience in systems. Risk Anal 29:498–501. Retrieved on 22 January 2018 at https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1539-6924.2009.01216.x

Jaeger C (2010) Risk, rationality, and resilience. Int J Disaster Risk Sci 1(1):10–16

Joseph J (2013) Resilience in UK and French security strategy: an Anglo-Saxon bias? Politics 33(4):253–264

Juncos AE (2017) Resilience as the new EU foreign policy paradigm: a pragmatist turn? Eur Secur 26(1):1–18. Retrieved on 22 January 2018 at www.tandfonline.com/doi/full/10.1080/09662839.2016.1247809

Knopf JW (2010) The fourth wave in deterrence research. Contemp Secur Policy 31(1):1–33. Retrieved on 22 January 2018 at www.tandfonline.com/doi/full/10.1080/13523261003640819

Lebow RN (2007). Coercion, cooperation, and ethics in international relations. Taylor & Francis

Makarenko T (2008) Criminal and terrorist networks: gauging interaction and the resultant impact on counter-terrorism. In: Brimmer E (ed) Five dimensions of homeland & international security. Center for Transatlantic Relations, Johns Hopkins University, pp 15–27

Mitchell T, Harris K (2012) Resilience: a risk management approach. ODI Background Note. Overseas Development Institute, London

Morgan PM (2012) The state of deterrence in international politics today. Contemp Secur Policy 33(1):85–107. Retrieved on 22 January 2018 at www.tandfonline.com/doi/full/10.1080/13523260.2012.659589

O'Brien G, Read P (2005) Future UK emergency management: new wine, old skin? Disaster Prev Manag 14(3):353–361

Omand D (2008) The international aspects of societal resilience: framing the issues. In: Brimmer E (ed) Five dimensions of homeland & international security. Center for Transatlantic Relations, Johns Hopkins University, pp 15–27

Payne KB (2010) Future of deterrence: the art of defining how much is enough. Comp Strateg 29(3):217–222. Retrieved on 22 January 2018 at www.tandfonline.com/doi/abs/10.1080/01495933.2010.494127

Pifer S, Bush RC, Felbab-Brown V, Indyk MS, O'Hanlon M, Pollack KM (2010) US nuclear and extended deterrence: considerations and challenges. Brook Inst Arms Control Ser 3:1–63

Prior T (2017) NATO: Pushing boundaries for resilience. ETH Zurich Research Collection. Center for Security Studies (CSS), ETH Zurich. Retrieved on 22 January 2018 at https://doi.org/10.3929/ethz-b-000184886

Rhodes E (2000) Conventional deterrence. Comp Strateg 19(3):221–253. Retrieved on 22 January 2018 at www.tandfonline.com/doi/abs/10.1080/01495930008403210?tab=permissions&scroll=top

Slovic P (1987) Perception of risk. Science. New Series 236(4799):280–285

Slovic P, Peters E (2006) Risk perception and affect. Curr Dir Psychol Sci 15(6):322–325

Stein JG (2009) Rational deterrence against 'irrational' adversaries? In: Paul TV, Morgan PM, Wirtz JJ (eds) Complex deterrence: strategy in the global age. University of Chicago Press, Chicago, pp 58–82

Stockholm Resilience Centre Explaining core concepts: what is resilience?. Website. Retrieved on 3 August 2017. www.stockholmresilience.org/research/research-news/2015-02-19-what-is-resilience.html

Tversky A, Kahneman D (1974) Judgment under uncertainty: heuristics and biases. Science 185(4157):1124–1131

U.S. Joint Chiefs of Staff (2016) Joint publication (JP) 1–02, Department of Defense Dictionary of Military and Associated Terms. Retrieved on 03 August 2017 at https://fas.org/irp/doddir/dod/jp1_02.pdf

UK Chief of the Defence Staff (2014) UK Defence Doctrine, Joint Doctrine Publication 0–01, 5th edn. Development, Concepts and Doctrine Centre, Swindon, November 2014. Retrieved on 03 August 2017 at https://www.gov.uk/government/publications/jdp-0-01-fourth-edition-british-defence-doctrine

Walker B, Salt D (2012) Resilience thinking: sustaining ecosystems and people in a changing world. Island Press, Washington, DC

[1]

‘UK Resilience’ was the initial designation by the Civil Contingencies Secretariat of its activities relating emergency planning in the UK within the framework of the 2004 Civil Contingencies Act. (Cabinet Office 2011b)

[2]

Under McNamara, pentagon analysts worked out that the “assured destruction” of 20–25 percent of Soviet population and 50 percent of Soviet industrial base would provide an adequate U.S. retaliatory threat which ensured the deterrence of the Soviet Union attacks. The analysts calculated that the standard metric for measuring how much was enough for such effect was 400 equivalent megatons (EMT). (Payne 2010)

[3]

Stein uses the example of “When President George W. Bush was considering whether or not to go to war in Iraq, he was told that Saddam Hussein had sought to buy yellow cake uranium from Niger. That was new information to the president – he had not heard it before – and it was diagnostic; it signalled that Saddam was likely seeking to develop unconventional weapons. What the information was not was reliable or valid, and therefore it should have been excluded from any kind of consideration. The reliability and validity of information is a threshold barrier that any piece of evidence should cross on its way into the decision-making process.” (Stein 2009; p. 62)

[4]

Slovic and Peters use the example of Nuclear radiation showing “how information about benefit [e.g. benefits to nuclear power is high] or information about risk [risk relating to nuclear power is low] could increase the positive affective evaluation of nuclear power and lead to inferences about risk and benefit that coincide affectively with the information given. Similarly, information could make the overall affective evaluation of nuclear power more negative, resulting in inferences about risk and benefit that are consistent with this more negative feeling.” (2006, p. 323)

[5]

“The initial wave of deterrence theorizing came after World War II and was driven by the need to respond to a real-world problem – the invention of the atom bomb. The second wave emerged in the 1950s and 1960s. It applied tools like game theory to develop much of what became conventional wisdom about nuclear strategy (at least in the West). Starting in the 1960s but really taking off in the 1970s, the third wave used statistical and case-study methods to empirically test deterrence theory, mainly against cases of conventional deterrence. The case-study literature also challenged the rational actor assumption employed in second-wave theory.” (Knopf 2010; p. 1)

[6]

Knopf defines this concept as a strategy aiming to “dissuade a potential attacker by convincing them that the effort will not succeed, and they will be denied the benefits they hope to obtain.” (2010; p. 10)

[7]

“Extending deterrence in a credible way proved a more complicated proposition than deterring direct attack. It was entirely credible to threaten the Soviet Union with the use of nuclear weapons in response to a Soviet attack on the United States. But how could the United States make credible the threat to use nuclear weapons against the Soviet homeland in response to a Soviet attack on U.S. allies in Europe?” (Pifer et al. 2010; p. 1)

[8]

Borrowing from the military-like jargon, Gearson explains that “Target hardening of the sort seen initially in London and in recent years across other world cities, and defensive measures taken in response to specific intelligence as a means to deter terrorists from carrying out specific attacks have had quite a good record in the UK and elsewhere.” (Gearson 2012; p. 186)

[9]

“Given the offensive advantage, the number of attackers using cheap, readily available tools will continuously rise, empowering non-established powers such as Iran, North Korea or even Daesh/IS. Reversing this trend requires getting serious about agreeing on international norms and improving both defences, especially employees’ and citizens’ “cyber-hygiene”, and about enforcement.” (Bendiek and Metzger 2015; p. 557)

[10]

Makarenko has devoted much of her research to the investigation of the convergence between organized crime and terrorism. She claims “Criminal and terrorist networks which have emerged from a state of perpetual conflict and instability blatantly reveal the ultimate danger of the crime-terror connection to international security.” (2008; p. 60)

[11]

“Although the importance of blocking criminal opportunities is important in both the context of anti-crime and counter-terrorism, the ability to identify crimes which are of interest to both criminal and terrorist networks provides an invaluable intelligence tool. Thus prior to implementing a policy of denial, it is essential to use knowledge of crime-terror interaction to collect more insight regarding organizational design of both groups, including the fundamentals of the acquisition and movement of criminal financing. Such knowledge not only contributes to the building of solid cases for prosecution services, but it also helps develop adaptive forecasting models which allows law enforcement and the

security services to focus their resources." (Makarenko 2008; p. 71)

[12] Folke et al. (2007) refer to the contagion from one system domain to another (such as fire, insect outbreak, and disease) where the intersection of slowly and fast variables create alternative states.

[13] Berkes et al. (2003) *claim that the* latent processes that are valuable in coping with this type of surprise are normally undiscovered in "normal" times.