Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence

Myriam Dunn Cavelty and Victor Mauer

Security Dialogue 2009 40: 123

DOI: 10.1177/0967010609103071

Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence

MYRIAM DUNN CAVELTY & VICTOR MAUER*

Center for Security Studies, ETH Zurich, Switzerland

Providing strategic warning to policymakers is a key function of governmental intelligence organizations. Today, globally networked challenges increasingly overshadow their historical state-centric counterparts so that warning has become considerably more difficult. It is recognized in parts of the intelligence community that many of the current problems for warning arise from continued reliance on analytic tools, methodologies and processes that were appropriate to the static and hierarchical nature of the threat during the Cold War. However, even though alternative analysis techniques have begun to be applied, this article argues that the intelligence community could benefit from the understanding that more than just the ontology of threats has changed, that in fact it is in the epistemological area that the most meaningful changes have taken place: Society has seen the replacement of the previous means–end rationality by a reflexive rationality. The notion of reflexive security can provide a valuable conceptual framework for understanding the current changes, and it could be instrumental in adapting intelligence sources and methods to a new era. In particular, an awareness of both complexity sciences and postmodernism might increase understanding of the limitations of knowledge and lead to the establishment of a political discourse of uncertainty.

Keywords strategic warning • intelligence community • reflexive security • risk society • new threat environment

Introduction

WHILE THE NATURE OF SECURITY CHALLENGES and the study of security itself have in some ways been transformed by the end of the Cold War and the terrorist attacks on the United States in 2001, the central task for intelligence services has essentially remained the same. As one intelligence veteran observes in a recent article: 'Nothing is more important in the world of intelligence than preventing surprise' (Hulnick, 2005:

SECURITY DIALOGUE

SAGE Publications, http://sdi.sagepub.com
Vol. 40(2): 123–144, DOI: 10.1177/0967010609103071

593). By implication, an intelligence failure is considered all the more severe if a surprise does occur. The fact that the majority of critical intelligence accounts focus on this aspect is thus not remarkable: The attack on Pearl Harbor, the coordinated Egyptian-Syrian attack against Israel on Yom Kippur, the invasion of Afghanistan by Soviet forces, the end of the Cold War and most recently the attacks of 11 September 2001 are just some of the surprises that have been attributed to intelligence failures (Wohlstetter, 1962; Halberstam, 2007; Bar-Joseph & Kruglanski, 2003; Maceachin, 2003; Combs, 2008; 9/11 Commission, 2004). Most of these occurrences have resulted in a series of investigations and reports (9/11 Commission, 2004; Roberts & Rockefeller, 2004) with the explicit aim of identifying the causes of those failures and recommending corrective actions (Warner & MacDonald, 2005; Johnson, 2004).

The view presented in such reports – and also in the academic literature on the topic – is that surprises can be prevented by adequate or 'better' warning (Parker, 2007). In this article, which focuses on the strategic level and refers mainly to the 'US intelligence community', warning is understood in a broad sense: as activities that provide vital support to national decisionmakers in their principal strategic missions – that is, understanding the complex geostrategic environment, facilitating a larger vision of objectives, assessing alternatives, determining strategy and protecting against consequential surprise (Cooper, 2005: 16). Warning is an informative function that assists policymakers both in thinking about issues before they become problems and in creating coherent, contextualized reference frames.[1] Warning is considered the classic strategic intelligence role (McCarthy, 1994) and was also the principal impetus for the creation of the US Central Intelligence Agency in 1947. Therefore, Hulnick's statement above can be adjusted to: 'Nothing is more important in the world of intelligence than providing strategic warning to policymakers.'

Surprises due to a failure of adequate warning have many causes. The dominant notion in the study of surprise attacks is that the problem is not the lack of information per se, but rather an incorrect understanding of what the available information means (Betts, 1982; Wohlstetter, 1962; Bar-Joseph & Kruglanski, 2003: 77), as well as other difficulties and challenges arising from cognitive and organizational issues (Johnston, 2005; Kirkpatrick, 1969; Shiels, 1991; Wirtz, 1991). What is more, the context for warning today seems to have changed considerably, as globally networked challenges increasingly overshadow their historical state-centric counterparts. As one intelligence official puts it, not only the terrorist threat but 'a host of border-spanning trends that challenge our traditional intelligence and law enforcement practices' need to

[1] It is important to note, however, that, according to US National Intelligence Officer for Warning Ken Knight, no standard definition of warning exists. Rather, there are many differing ideas about what constitutes warning, when and how it is effective, and what is needed to do it right (Knight, 2006).

be considered (George, 2007). Owing to the use of a very broad definition of surprise that includes anything that might affect the United States, its allies or its interests around the world (Hulnick, 2005: 595), the list of new transnational challenges also includes organized crime, narcotics-trafficking, illicit sales of weapons, the spread of disease, radicalization and the geopolitical implications of climate change. In other words, intelligence services are tasked with monitoring threats to their country's national security interests that are more diverse, interconnected and dynamic than ever before.

As a consequence, in this new threat environment the task of providing warning (in the sense of generating secured and actionable knowledge about these challenges) has become considerably more difficult, a fact recognized by the US intelligence community itself. An ontological, an epistemological and a methodological dimension are involved: The issue is an ontological one as it is about the nature and shape and structures of the new threats and their relation with the observers; it is epistemological because it is about the nature and scope of knowledge, the production of knowledge, the question of what knowledge is, and because it relates to the nature of the consequences that knowledge claims have on practice; and it is methodological because it is concerned with the rationale and the philosophical assumptions that underlie the study of new threats and the methods that are applied to study them.

This article addresses the question of how the post-Cold War threat environment has transformed the basic parameters and fundamental assumptions of strategic warning. In the first section, it describes both the 'old' and the 'new' threat environments (acknowledging that many of the developments mentioned manifest themselves in an uneven manner) and identifies the challenges for strategic warning today. It then looks at some of the more innovative approaches to warning, pointing out that, despite some steps in the right direction by parts of the intelligence community, intelligence practitioners do not take into account that not only has the environment or the ontology of threats changed, but also this age's rationality – and that therefore more efforts should be made to address epistemological questions. Following the lead of Andrew Rathmell (2002), who coined the term 'post-modern intelligence', this article thus introduces and applies to the topic some recent literature on reflexive security (Rasmussen, 2001, 2004), which can provide a valuable conceptual framework for understanding the current changes and the ways in which intelligence sources and methods could be adapted to a new era, mainly pointing to the fact that an awareness of complexity sciences and postmodernism might help us to better understand the limitations of knowledge and to establish a political discourse of uncertainty.

From Old to New: The New Threat Environment

Organizations are creatures of their times, and they are designed in response to given sets of historical circumstances (Rolington, 2006: 739). The failure to detect North Korea's surprise attack on South Korea in 1950 prompted the establishment of a worldwide warning system, and the United States began to take advantage of its regional military commands around the world. When the Soviet Union emerged as the main rival of the United States, the intelligence community switched to an indicator-based warning system on the premise that the USSR could not mount an attack without some prior effort to gear up for war, and that if certain key intelligence targets were watched carefully, indications that an attack was being prepared would be detected. Thus, the US network of worldwide warning centres became Indications and Warning Centers (I&W), and the discipline of I&W became a major focus for the US intelligence services (Hulnick, 2005: 595).

The organization and practices of the intelligence community were shaped by the particular geopolitical and technical requirements of the Cold War (Rathmell, 2002: 91; Kerr et al., 2005). Not surprisingly, the change in the international system and the nature of the 'new' threats has created some major difficulties for traditional approaches to intelligence collection. In order to better understand these difficulties, this section first looks at the 'old' conception of problems and how they were dealt with. A second subsection then focuses on the character of the 'new' challenges and the challenges that arise from them. However, it is recognized that the discontinuities between the Cold War and post-Cold War environments are not as clearcut as the separation between 'old' and 'new' implies.

The Old: Measurements of the Known

During the Cold War, the two superpowers combined global political objectives with military capabilities. On each side, security threats were directly linked to military capabilities and mainly arose from the aggressive intentions of the other powerful actor in the international system, in accordance with neorealist theory (Waltz, 1979). This theory is predicated on a specific understanding of power as the sum of military, economic, technological, diplomatic and other capabilities at the disposal of the state (Organski, 1968; Singer, Bremer & Stuckey, 1972; Hart, 1976). This distribution of capabilities, which is unequal and shifting, defines the relative power of states and can be observed to predict variations in states' balance-of-power behaviour.

The seemingly clear and straightforward parameters of the Cold War threat implied a sense of certainty through calculability. Although there were numerous surprises during the Cold War, the core intelligence task for the

United States – the monitoring of the USSR's strategic and military posture – remained within predictably limited bounds. The overarching threat meant that other issues, such as post-colonial insurgencies, in other regions such as the Middle East, did not shape the process and profession in the way that the 'Soviet target' did, even though they were taken into consideration. The militarized nature of that target meant that there was a concentration on acquisition of 'tangible' technical military, scientific and economic indicators through clandestine and specialized collection mechanisms (Rathmell, 2002: 91). To identify the level of threat, one looked at the capability or potential of the enemy and its intent or motivation, in addition to one's own vulnerability (Singer, 1958). The monitoring and surveillance method defined a set of indicators – the movement of people and supplies, changes in ship or aircraft deployments, increases in communications – and a possible timeline towards the escalation of a conflict. A warning signal emerged as soon as an indicator had passed a certain threshold.

There was, of course, not always agreement on the exact nature of the Soviet threat. The debate, however, evolved around the threat in terms of what could be measured. In addition, there was a belief that it was possible to defeat the threat and achieve security through known measures (Rasmussen, 2006: 3). The concept of deterrence, which refers to the attempt to create risks that are so high in comparison to a possible gain that opponents refrain from engaging in a certain policy or action (Schelling, 1966), existed as a credible option to prevent the threat from being enacted. The threat (in the form of actor, intention, capability) was, by and large, known; it represented 'available and secured knowledge' (Daase & Kessler, 2007: 419). These characteristics (and the perception thereof) shaped the intelligence community that emerged from the Cold War: 'secretive and divorced from society, emphasizing clandestine and often technical collection, and comfortable with linear predictive reasoning' (Rathmell, 2002: 91).

The New: Key Characteristics and the End of Certainty

The end of the Cold War brought about not only the end of a relatively stable bipolar world order but also the end of the boundedness of threats. The components of the post-Cold War security paradigm are more diverse and diffuse than were their counterparts during the Cold War. This is particularly true in terms of the sources of threats: More nations are involved in managing international affairs than previously, albeit often only on a regional basis. Regional issues have proliferated and threaten wider international peace and security. Non-state actors have taken advantage of regional conflicts and insecurities. The security community seems to be facing 'more dynamic geostrategic conditions, more numerous areas and issues of concern, smaller and more agile adversaries' (Cooper, 2005: 24).

The end of the Cold War 'brought about nothing less than the collapse of an international system' (Gaddis, 1993: 53). The breakdown of the international system in turn led to a collapse of previous assumptions and mind-sets. Both these developments have been accelerated by the so-called information revolution, which in turn has had a huge impact on the intelligence community in terms of both threats and opportunities (Rathmell, 2002: 87). Closely interrelated with the information revolution, indeed in part caused by it, is the phenomenon of globalization, which has been seen as a 'process which involves nothing less than the transformation of the world' (Coker, 2002: 18), tying 'local life to global structures, processes and events' (Coker, 2002: 19). The compression of time and space through globalization has led to the easy movement of people, weapons, toxins, drugs, knowledge and ideas across many boundaries (Friedman, 2005), and is partly responsible for the shape and the proliferation of modern threats.

At the same time, the transformation of the international environment is ambiguous and uneven. Globalization empowers individuals as well as elites; it breaks down hierarchies, but also creates new power structures; it has a fragmentizing as well as an integrating effect (Rothkopf, 1998). This ambiguity itself promotes new insecurity, as the co-existence of the old and the new creates great tensions and new security issues (Beck, 1999). We seem to be witnessing scalar changes moving in opposite directions: the power to resist vulnerability moves *outwards* to international markets and international organizations, while the power to cause vulnerability moves *inwards*, through classes and groups to the individual. The concept of 'uneven transformations' implies that the present epoch is marked by persistent opposites and derives its order from episodic patterns with very contradictory outcomes (Rosenau, 1990, 1998).

In a nutshell, the new spectrum of threats is dominated by three interrelated characteristics: complexity, uncertainty and a diminishing impact of geographical space. The phenomena of both the information revolution and globalization accelerate changes and therefore feed the complexity spiral (Merry, 1995; Satyanarayanan, 2003). With greater complexity, the level of uncertainty further increases: The identity and goals of potential adversaries as well as the timeframe within which threats are likely to arise are marked by uncertainty (Goldman, 2001: 45). Further, there is uncertainty concerning the capabilities against which one must prepare, and also concerning the type of conflict or contingency to prepare for. A shift of focus from intended malicious action toward more diffuse and unintended threats like global warming or financial crisis only serves to exacerbate these difficulties further. In fact, 'risk and uncertainty are the hallmark of world politics at the dawn of the twenty-first century' (Williams, 2008: 58).

Warning in the New Threat Environment

Many of the changes brought about by the end of the Cold War still baffle the intelligence community at large. One observer suggests: 'Many of today's principal analytic problems arise from continued reliance on analytic tools, methodologies, and processes that were appropriate to the static and hierarchical nature of the Soviet threat during the Cold War' (Cooper, 2005: 23). The tendency is to press the new, still undefined, highly complex post-modern world into the old Cold-War mind-set with all that implies, exemplified in a high degree of 'spatial fetishism', a tendency to reduce the units of analysis to territorially demarcated national states (Walker, 2006: 154–159).

Despite this general tendency, there is a growing part of the intelligence community that has come to realize that the changing context has significant consequences for strategic early-warning methodologies and methods. However, even though the techniques of alternative analysis have been around for many years, they have only recently (and still only intermittently) been applied in the intelligence community (Fishbein & Treverton, 2004). Below, some of the new approaches used in the US intelligence community are reviewed in two separate subsections according to two distinct types of warning: monitoring and discovery. The traditional indicator systems of the Cold War were geared towards monitoring activities that had been identified as potentially dangerous, such as a hostile missile launch. In the new threat environment, which is the focus of the first subsection, monitoring is moving from an exercise in surveillance-monitoring towards forecasting, understood as a probabilistic assessment focusing on general trends. The second subsection discusses the second type of warning, which can be described as a discovery function and is geared towards assisting decisionmakers in identifying dangerous situations that may not necessarily be obvious (Cooper, 2005: 16). The fact that the history of world politics is littered with strategic surprises points to the fact that the early discovery of the unexpected has always been a major challenge. It can, in fact, be argued that discovery has not become more difficult today, despite the new threat environment. On the contrary, some of the alternative approaches in use might help to open up spaces previously closed. However, epistemological questions that stem from the new threat environment are largely ignored.

Monitoring

Monitoring in the new threat environment means first and foremost that new kinds of methodologies are needed in order to capture the nature of the new threats (networked, transnational, complex) – some of which take into account complex environments. In general, monitoring now focuses on fore-

casting certain activities or patterns. Successful forecasting is only possible, however, if the problem to be confronted has been clearly defined, which of course necessitates that the threat must be recognized in the sense that it is, at least in part, known. Not surprisingly, current monitoring efforts primarily focus on the threat of terrorism. Foresight then requires an awareness and appreciation of the steps and components involved in preparing an attack, but also an awareness of the possibility of randomness and surprise (Sinai, 2003, 2007; Segell, 2005).

Segell (2005: 221) differentiates three broad types of methodologies for predicting and forecasting acts or events that have not been clearly identified: '(1) trends and patterns, (2) frequency, and (3) probability', in what is only a minor variation from traditional approaches. These types have in common that they place data gathered on an ad hoc basis within a specific context to be passed on for an actionable operation. Where information is missing – that is, where no trend, pattern or frequency can be discerned – intelligence data-gathering and analysis should focus on accentuating a risk assessment of the probability of attacks against vulnerabilities (Segell, 2005: 235). Indeed, one reaction of the US federal government to missing information has been to move from the threat-based approach towards vulnerability assessment and to 'play defense' (Hulnick, 2005: 605) in lieu of developing new indication and warning systems. With this approach, missing knowledge is substituted by broadly applying defensive measures.

There are other (mostly quantitative) methodologies that go beyond these general (and well-established) tools. There are at least four methodologies that might enhance the monitoring of terrorism activities: geospatial predictive analysis, data-mining technologies, project management-based approaches and social network analysis (Sinai, 2007). The first of these, geospatial predictive analysis, is the attempt to predict the location and date of future terror attacks by accumulating data on the geographic location of previous incidents. To this end, data is fed into a software application that generates threat signatures, such as trends in tactics, techniques and procedures. Using a geographic interface, this system is then able to identify terrorist hot spots (Dumas, 2007; Smith et al., 2008). The second technique involves data-mining technologies. Here, large volumes of data on known and potential terrorists can be harnessed and analysed using data-mining tools to identify links and patterns in different data repositories, to identify anomalies, and to predict which individuals are likely to carry out terror attacks. Data-mining tools complement human intelligence and signals intelligence surveillance and can help identify key players and their communication tendencies (see Derosa, 2004). A third technique is based on the use of a project management approach. A project management model can be used to characterize terrorist operations in terms of tasks, schedules and lines of responsibility. Understanding this model enables the counter-terrorism

community to delay or disrupt an imminent operation, conduct 'what if?' analyses and guide the systematic search for evidence (Sinai, 2007). The fourth technique is based on social network analysis. This incorporates, correlates and visualizes biographic, religious, demographic and other social data, and identifies the networks of connections and relationships between individual actors, enablers or groups. Such an approach enables one to understand why individuals become radicalized and how they are actually recruited (Sageman, 2004).

Apart from the fact that some of these approaches, like data-mining, have given rise to major concerns about privacy issues (Birrer, 2005), they also have other limitations. To mention just a few: The first approach only considers successful attacks and not aborted operations or failed attempts; insight from high-frequency areas is not necessarily applicable to rare-event regions; and this approach focuses on incidents rather than on people, which limits its ability to predict terrorist behaviour. Data-mining, on the other hand, does not enable effective information-gathering on unknown individuals and does not solve the problems of pattern recognition. The project management approach might generate false positives, because identifying terrorists is harder than identifying suspicious consumer behaviour and because the approach relies on a limited set of technical indicators rather than complementing technical factors such as the characteristics of groups and the nature of their leadership. To take the example of terrorism, the protection of state and society through preventive measures is hampered by the severe limitations on the knowledge that law enforcement agencies have of terrorist actors. Threats or dangerous individuals are usually identified by conspicuous or previous illegal behaviour. Previous illegal behaviour, however, cannot serve as an indicator of the danger emanating from individuals who make a particular effort to live law-abiding lives only to be able to strike more efficiently when the moment is right. Finally, social network analysis, while important, does not complete the big picture. However, with careful consideration of the pros and cons and through careful combination of more than one method, it may be possible to derive attack indicators with some predictive potential.

Other types of indicator-based systems are also developed in the realm of political risk analysis for more complex, diffuse threats in general. The aim of these approaches is to build 'risk data bases that attempt to correlate and/or identify specific trigger points with particular risk events' (Jarvis & Griffiths, 2007: 19). They seek to collect sufficient data to enable the development of indicator models that can identify sequences of events or triggers that are precursors to regime instability, conflict, humanitarian crisis or any series of other severe events. The Canadian Country Indicators for Foreign Policy (CIFP) project is among the more innovative of these approaches, being based on a weighted index of nine composite risk indicators (armed conflict,

governance and political stability, militarization, population heterogeneity, demographic stress, economic performance, human development, environmental stress, and international linkages) (Carment et al., 2006).

Such models may produce reasonable forecasts when there is good available data and if there is a belief that existing, well-understood and precisely delineated patterns of behaviour will continue into the future despite the fact that many aspects of the particular challenges may still be undiscovered. In other words, for monitoring activities to make sense, it must be believed that the threat is analytically tractable and that cause–effect relationships are identifiable. Clearly, however, there is an inherent danger in this assumption: such a certainty about being able to know might lead to wrong actions based on overreliance on these systems. Where there is doubt that the relationships described in the model will continue or where forecasts of the independent variables are unreliable, different tools are needed.

Discovery

Discovery is a different domain. The concept of strategic early warning is based on the assumption that discontinuities do not emerge without warning. Warning signs have been described as 'weak signals' or as factors for change that are hardly perceptible at present but will constitute a strong trend in the future or can have dramatic consequences. The management of 'unknown unknowns' makes it necessary to gather 'weak signals' and to identify events or developments that could set off alternative dynamics and paths. As noted above, the very broad definition of surprise that includes anything that might impact the United States, its allies or its interests around the world makes it very clear why discovering such signals is a daunting task. Discovery is not about pattern recognition or detections of known patterns: it is about pattern *discovery* or the identification of new patterns (Williams, 2006). Heuer's seminal work on the psychology of intelligence talks about the inherent problems of this: 'we tend to perceive what we expect to perceive' (Heuer, 1999: 8). The author then goes on to say that 'patterns of expectation become so deeply embedded that they continue to influence perceptions even when people are alerted to and try to take account of the existence of data that do not fit their preconceptions' (Heuer, 1999: 9).

The puzzle of discovery and innovation is fundamental in this context: How can we notice a pattern we have never seen before (Crutchfield, 1994)? There is always an *ad hoc* quality to the recognition of new phenomena, and the ontological validity of a perceived novelty remains unclear. Because patterns must be 'recognized' by the observer, any observed structure or pattern may be an artefact of the research question; other patterns may go unnoticed for the same reasons (Mihata, 1997: 32). A substantial body of research in cognitive psychology and decisionmaking analyses cognitive

limitations that cause individuals to employ simplifying strategies to ease the burden of mentally processing information and to deal with complexity and ambiguity. As Snowden (2007) explains, when one is scanning data, only a tiny percentage of the visual range is in sharp focus, but the brain fills in the gaps. This process of pattern recognition can cause patterns to be missed or 'weak signals' – we do not see because we do not expect them – to be overlooked. In a complex system, where the number of possible connections can be very high, the ability to see is overwhelmed with possibilities. Such behaviour leads to predictably faulty judgements known as cognitive biases (see Heuer, 1999: 111–172). In the context of discovery, the type of bias that is of importance is called pattern bias, which makes one look for evidence that confirms rather than rejects a hypothesis and fill in missing data with data from previous experiences (Johnston, 2005: 66). Another problem in this context is the challenge of ethnocentrism (Johnston, 2005: 75), the tendency to judge the customs of other societies by the standards of one's own culture. In the realm of discovery/warning, ethnocentrism affects the way signs are read and will lead to more pattern bias.

How can such problems be overcome? Over the years, public- and private-sector organizations that cope with uncertain futures have developed tools for what is called alternative analysis, 'techniques that seek to help analysts and policymakers to stretch their thinking by broadening the array of outcomes considered or by challenging underlying assumptions that may constrain thinking' (Fishbein & Treverton, 2004). There are many methods that can be used as future methods, and it must suffice to point to the most prominent of them: scenarios, Delphi exercises and environmental scanning for managing the future, and brainstorming, creative imagery and community visioning for creating future images (Performance and Innovation Unit, 2001; George, 2004). Snowden also describes a set of narrative methods that provide a rich context that allows patterns of experience rather than opinion or belief to emerge (Kurtz & Snowden, 2003: 471). One approach that is often heralded to maximize weak-signal detection in a complex system is called horizon scanning (employed by the governments of Singapore and the United Kingdom).

The main advantage of these techniques is that they can stimulate strategic thought and communication, improve internal flexibility of response to environmental uncertainty, and provide preparation for possible system breakdowns. However, they do not bring back certainty. In order to anticipate threats that can suddenly emerge at any time, anywhere and in a variety of forms, 'analysts need to think more in terms of a broad mental readiness to perceive early warning signs of threat than in terms of challenging specific assumptions or identifying specific alternative outcomes' (Fishbein & Treverton, 2004). Alternative analysis is designed to overcome biases: using them does not mean that one can *know* the future. If they are conceived as a set

of tools rather than as an ongoing organizational process aimed at promoting sustained mindfulness, it is unlikely that they will be accepted within the community. Furthermore, there is always the danger that these approaches will be criticized for directing attention to outcomes that, while possible, are almost by definition improbable, potentially diverting policy attention and resources away from more likely threats (Fishbein & Treverton, 2004).

Towards Reflexive Intelligence

While the more innovative approaches described above take into account a change in the new threat environment, these reactions are mainly confined to the dimensions of ontology and methodology, with hardly any reflection on epistemology. In fact, the intelligence community suffers from what Cooper (2005: 26) calls 'the Myth of Scientific Methodology', a cultural orientation towards an 'evidence-based scientism' (Cooper, 2005: 31) that dates back to a time when facts were often considered totally separate and independent of the viewer – exemplified in Sherman Kent's (1965) dream of what intelligence should do (see also Johnston, 2005: 17–20). This orientation, however, represents a key problem, one that can only be overcome if the community accepts that the end of certainty represents not a transitional phase but a reality that is here to stay. As Andrew Rathmell (2002: 97) has pointed out, intelligence's 'grand narrative' ended with the collapse of the Soviet Union. Now, the intelligence community has to understand multiple, overlapping and often contradictory narratives, a world that appears chaotic and developments that display the properties of non-linear, dynamic systems. Whereas Cold War intelligence by and large knew the problem and could envisage an objective reality that it was seeking to comprehend, contemporary intelligence, more often than not, is in the position of not even knowing whether there is a single objective reality out there that it is trying to capture (Rathmell, 2002). In the natural and the social sciences, there are at least two major strands of thought that back up this stance: complexity sciences and postmodernism. If the twin forces of complexity and change are taken seriously, there can be no 'grand' theoretical project that distils complexity, ambiguity and uncertainty into neat theoretical packages and categories.

In this section, it is suggested that the new threat environment has seen the rise of a reflexive rationality. Reflexive rationality exists side by side with the older means–end rationality. This framework, introduced in the first subsection below and, as described in the second, applied to the realm of strategic warning, actually helps to overcome some of the problems that the intelligence community is confronted with. Where it does not, it at least points to the most important issues that need to be addressed in the future.

The Limits of Means–End Rationality in an Age of Reflexive Security

Threats can be defined as problems that are 'consciously and actively created by one security actor . . . for another' (Bailes, 2007: 2), a view that informed the threat paradigm that had a high plausibility during the Cold War. Today, however, the world is no longer confronted with threats alone, but also with risks. Risks are indirect, unintended, uncertain and by definition situated in the future, since they only materialize as real when they 'happen'. Therefore, risks exist in a permanent state of virtuality and are only actualized through anticipation (van Loon, 2002: 2), leading to a state of 'no-longer-but-not-yet – no longer trust/security, not yet destruction/disaster' (Beck, 1999: 137). According to this understanding, any attempt to define risks objectively is inherently futile: their indeterminate nature means that perceptions and definitions of risks will be contested between different social groups, and 'risks cannot be understood outside their materialization in particular mediations, be they scientific, political, economic or popular' (van Loon, 2000: 176).

According to German sociologist Ulrich Beck (1999), we live in a global risk society, in which everything revolves around risks. It is, however, 'not a matter of the *increase*, but rather of the *de-bounding* of uncontrollable risks. This de-bounding is three-dimensional: spatial, temporal and social' (Beck, 2002: 41). At the same time, global risks contradict the language of control in industrial societies (Aradau & van Munster, 2007: 92). Under conditions of extreme uncertainty, decisionmakers are no longer able to guarantee predictability, security and control, so that the real challenge is 'how to feign control over the uncontrollable' (Beck, 2002: 41). At the same time, expert knowledge is exposed as an insufficient and unreliable resource for political decisions (Aradau & van Munster, 2007: 105): The latter appear as ungrounded, arbitrary attempts to subdue the contingency of the future. What emerges is a social awareness of the catastrophic impacts of risks, from which a specific kind of reflexivity can be derived as a form of self-critique and self-transformation in the face of disastrous risks. According to Beck, reflexive modernization is spawned from early modernity and its belief in advancement through 'progress'; but, in a dynamic inversion, reflexive modernity interrogates modernity, the very source of its power. In this day and age, reflexivity becomes the norm.

These notions have recently been applied to the security field. For Mikkel Rasmussen (2001: 288), the national security paradigm after World War II was 'the high tide of means–ends rationality', in which it is believed that an action produces particular (knowable, calculable) consequences. This rationality has been replaced by a reflexive rationality in an age of reflexive security. In this reflexive rationality, 'the ways by which we try to solve our problems . . . become a "theme and a problem in itself"' (Rasmussen, 2004: 395). At the centre of this complex is the fear of the inability to maintain

order, a condition called 'ontological insecurity'. It is 'the hallmark of risk society because it causes reflection on the very nature, the ontology, of the situation we are in' (Rasmussen, 2002: 333). However, it must be said that the means–end rationality has not completely been replaced by a reflexive one; in fact, the means–end rationality can still make perfect sense in certain circumstances today. What has happened is that, during the Cold War, a shared ontology generated a shared epistemology and made linear means–end rationality work rather well. Since 1990, this shared ontology has lost its prominence, allowing for new versions to exist beside it.

Inadvertently, intelligence, in parts, also becomes reflexive. While the collection and dissemination of all information has traditionally been predicated on the belief that there was a separation between subject and object, this certainty has now gone, and 'the consumer of intelligence must ask questions about the very nature of information/intelligence itself' (Rolington, 2006: 749). The myriad reports and articles on the creation of intelligence are a hallmark of this uncertainty. Sherman Kent (1965) is unlikely to have anticipated that his classic definition of intelligence as a kind of *knowledge* would acquire a completely different meaning in an age of reflexive intelligence. Of course, the central business of the intelligence community still is the production of knowledge. But, apart from trying to get targeted, actionable and predictive knowledge for specific consumers (Rathmell, 2002: 88), intelligence has become concerned with how this knowledge can be created.

Warning in an Age of Reflexive Intelligence

How is warning affected by this? The complexity paradigm focuses attention on the concept of the inherently unpredictable situation – a situation that is unpredictable by nature, not just by virtue of the limitations of the observer (Kurtz & Snowden, 2003; Snowden, 2002). Rather than understanding this as a call to end all warning efforts owing to their inherent futility, the task ahead for analysts consists of learning to recognize and appreciate complexity, ambiguity and uncertainty. This will mean that analysts need to start focusing on different methods that might work well in situations where the assumption of order does not hold. The aim should not be to reduce uncertainty, as traditional scientific methods do, but to accept it for what it is.

The discipline of complexity sciences points to the fact that complex systems of any sort exhibit a variety of specific, non-exclusive features and behaviours. For one thing, there are cause-and-effect relationships between the so-called agents that form the system, but both the number of agents and the number of relationships defy categorization or analytic techniques. Cause and effect, or inputs and outputs, are not proportional; the whole does not correspond to the sum of its parts and is not even qualitatively recognizable in its constituent components. Small uncertainties are amplified, so that even

though system behaviour is predictable in the short term, it is unpredictable in the long term (Merry, 1995: 26–27). Thus, extreme sensitivity to initial boundary conditions or historical paths makes detailed prediction impossible (Mihata, 1997: 33–34). Initial behaviour patterns and outcomes often influence later ones, producing dynamics that explain change over time and that cannot be captured by labelling one set of elements 'causes' and another 'effects' (Jervis, 1997). Complexity sciences also state that complex spaces bring forth certain patterns, the details of which are unpredictable. Once a pattern has stabilized, its path appears logical, but it is only one of many that could have stabilized, each of which also would have appeared logical in retrospect. Relying on historically stable patterns of meaning implies that humans will be insufficiently prepared to recognize and act upon such unexpected patterns in the future. However, these patterns are usually recognizable in their basic forms, and with practice one can even learn to stabilize or disrupt them and to shape desirable patterns by creating so-called attraction points (Kurtz & Snowden, 2003).

Most of this resonates well with the postmodern view that no determination of a single truth is possible. The complexity sciences confirm that the observer and the observed cannot be detached from each other, and that observation itself is an ontological event. Additionally, the complex is assigned a specific epistemological meaning: it shows the limits of knowledge due to complexity and unpredictability. The positivist-empiricist idea, which is still dominant in the community, that a trained observer can encapsulate the complexity of the world into neat packages through a variety of rigorous procedures, is antithetical to the current circumstances. This is supported by the postmodernist understanding that no matter how we assess information, knowledge or intelligence, we can never achieve anything other than a mirror of how we see the 'facts' (Rolington, 2006: 749).

At the same time, reflexivity concerning intelligence practices also leads to a different kind of issue. Not only since former US secretary of defense Donald Rumsfeld invoked the notion of unknowns in his often-cited speech at a Department of Defense press conference in February 2002 do we know that 'it is the relationship between what we know, what we do not know, what we cannot know . . . that determines the cognitive frame for political practice' (Daase & Kessler, 2007: 412). Cognitive sciences and the sociology of knowledge tell us that the handling of issues is directly linked to the perception of 'knowledge (or non-knowledge) about things, and knowledge (or non-knowledge) about ways to identify things' (Daase & Kessler, 2007: 413). Or, as the doyen of intelligence psychology observes: 'Comprehending the nature of perception has significant implications for understanding the nature and limitations of intelligence analysis' (Heuer, 1999: 14). In other words, the belief about the nature of a threat (its ontology) and our knowledge or belief about the way we should approach it (epistemologically and

methodologically) shape possible policy responses. This leads to a focus on possible negative effects arising directly from the practices of analysts. In certain circumstances, even the most absurd scenarios can gain plausibility, especially if a chain of reasoning changes beliefs and these scenarios are in consequence included in the realm of the possible, or even the probable (Conetta & Knight, 1998: 38; Daase & Kessler, 2007: 428).

Furthermore, security politics dealing with risks is constituted by 'definitional struggles over the scale, degrees and urgency of risks' (Beck, 1999: 46). This implies that there is no such thing as apolitical analysis: as soon as something is identified as a risk, it is managed and therefore changed. Moreover, because 'risk statements carry consequences, the representation of risk is subject to political manipulation' (Garland, 2003: 56). In this context, a particular style of intelligence analysis has recently emerged that does not rely on the facts at hand, because there are no facts any more, but instead constructs a worst-case scenario by surveying possible options that might be available to adversaries. Worst-case scenarios and the irreversible damages associated with them logically lead to a politics of zero risk (Aradau & van Munster, 2007: 103) and legitimize any kind of action. This so-called hypothesis-based analysis starts with a preferred scenario and then finds data that support such a scenario (Ryan, 2006: 287). Because such an approach can be presented as having the advantage of countering various kinds of unknowns and allows policymakers to contend with uncertainty, it has significant appeal today. However, such an approach would ultimately fail to deal with the basic tenet of the new threat environment, namely, uncertainty. In other words: Extra support for the intelligence services might well double the number of service personnel as compared to the level of 2001. It might result in the monitoring of even more networks and more individuals. It should, however, not result in the flawed assumption that more money, however wisely spent, results in more knowledge. On the contrary, acknowledging the limits of knowledge and allowing for failure in extraordinary circumstances not only will lead to changes in societal mind-sets, but will caution against actions that in fact lead to a deterioration rather than an improvement of the overall security situation.

Conclusion

Following Rathmell's (2002) suggestion of postmodern intelligence, this article has argued that, first, the intelligence community should not only try to embrace postmodern ideas but also make the best out of reflexive practices. This would result in a more widespread recognition of the fact that change is dynamic, non-linear and accelerating. Second, the lessons from

complexity sciences can also be applied to intelligence: one key requirement for effective warning in the 21st century threat environment is sensitivity to complexity. Analysts will need to use fresh assumptions and fresh visions of the future to engage in pattern discovery, to forge closer links with policy-makers in order to enhance their sensitivity to the issues, and to engage in systematic probing strategies to elicit knowledge and understanding of adaptive responses. In addition, the assessment and monitoring of multiple watch-points in disorderly spaces will be essential, as will the use of open sources of intelligence and multiple indicator sets. It is important to recognize the dynamism and co-evolution of complex systems. Therefore, constant refinement and adaptation is necessary to ensure that warning itself becomes a complex adaptive system (Williams, 2006).

Clearly, this means that horizontal knowledge networks need to be embraced, even at the expense of vertical integration. Knowledge must be sought where it resides, whether by topic or by source (George, 2007). The traditional model of the individual analyst at the centre of the intelligence process is receding. Expertise will matter more in terms of how it describes the complete expertise of a collaborative group (Medina, 2007). In fact, all alternative approaches described above work best if a mixed group of people with diverse backgrounds is brought together. But, rather than trying to revolutionize the entire system, the intelligence community should try to separate more traditional threats from the less understood problems (Rolington, 2006: 752). This in turn would result in the training of two kinds of analysts: Sherman Kent types and postmodern scenario planners (Rolington, 2006: 754).

Arguably the most important conclusion to be drawn is that a political discourse of uncertainty is required. The tension between having to know (and wanting to know) and the end of certainty is linked to a 'functional and political need to maintain myths of control and manageability, because this is what various interested constituencies and stakeholders seem to demand' (Power, 2004: 10). The myth of perfect manageability must be laid to rest and an explicit discourse of possible failure started. In other words, the 'new politics of uncertainty must generate legitimacy for the possibility of failure' (Power, 2004: 62). Governments and government agencies would then not need to act as though all risks were controllable and would contest media assumptions to that effect. This may sound rather simple, if not outright naïve. However, it may be the only way to escape the vicious circle that uncertainty has created for organizations built for the creation of actionable knowledge. Also, it would counter at least part of the danger of uncertainty being instrumentalized politically to legitimize actions.

* Dr Myriam Dunn Cavelty is a Lecturer at ETH Zurich and head of the New Risks Research Unit at the Center for Security Studies, ETH Zurich. She specializes in security studies and the impact of the information revolution on security issues. Her most recent publications include *Cyber-Security and Threat Politics: US Efforts To Secure the Information*

Age (Routledge, 2008); *Securing the Homeland: Critical Infrastructure, Risk, and (In)Security* (Routledge, 2008; co-edited with K. S. Kristensen); and *Handbook of Security Studies* (Routledge, 2009; co-edited with Victor Mauer). E-mail: dunn@sipo.gess.ethz.ch. Dr Victor Mauer is Deputy Director and Head of Research at the Center for Security Studies, ETH Zurich, and heads the Center's European Security and Defence Policy (ESDP) project. He specializes in security studies in general and in European security, European integration and transatlantic relations in particular. He is co-editor (with Myriam Dunn Cavelty) of the *Handbook of Security Studies* (Routledge, 2009); and (with Daniel Möckli) of *European-American Relations and the Middle East: From Suez to Iraq* (Routledge, 2009). E-mail: mauer@sipo.gess.ethz.ch. The authors would like to thank J. Peter Burgess and three anonymous reviewers for *Security Dialogue* for their useful comments, and Christopher Findlay for his editorial assistance.

References

9/11 Commission, 2004. *Final Report of the National Commission on Terrorist Attacks upon the United States*. Washington, DC: National Commission on Terrorist Attacks; available at http://www.9-11commission.gov/report/911Report.pdf.

Aradau, Claudia & Rens van Munster, 2007. 'Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future', *European Journal of International Relations* 13(1): 89–115.

Bailes, Alyson J. K., 2007. 'Introduction: A World of Risk', in Stockholm International Peace Research Institute, ed., *SIPRI Yearbook 2007: Armaments, Disarmament and International Security*. Oxford: Oxford University Press (1–20).

Bar-Joseph, Uri & Arie W. Kruglanski, 2003. 'Intelligence Failure and Need for Cognitive Closure: On the Psychology of the Yom Kippur Surprise', *Political Psychology* 24(1): 75–99.

Beck, Ulrich, 1999. *World Risk Society*. Cambridge: Polity.

Beck, Ulrich, 2002. 'The Terrorist Threat: World Risk Society Revisited', *Theory, Culture & Society* 19(4): 39–55.

Betts, Richard K., 1982. *Surprise Attack: Lessons for Defense Planning*. Washington, DC: Brookings Institution.

Birrer, Frans, 2005. 'Data Mining To Combat Terrorism and the Roots of Privacy Concerns', *Ethics and Information Technology* 7(4): 211–220.

Carment, David; Souleima El-Achkar, Stewart Prest & Yiagadeesen Samy, 2006. 'The 2006 Country Indicators for Foreign Policy: Opportunities and Challenges for Canada', *Canadian Foreign Policy* 13(1): 1–35.

Coker, Christoph, 2002. *Globalization and Insecurity in the Twenty-First Century: Nato and the Management of Risk*, Adelphi Paper 345. London: International Institute of Security Studies.

Combs, Dick, 2008. *Inside the Soviet Alternate Universe: The Cold War's End and the Soviet Union's Fall Reappraised*. University Park, PA: Penn State University Press.

Conetta, Carl & Charles Knight, 1998. 'Inventing Threats', *Bulletin of the Atomic Scientists* 54(2): 32–38.

Cooper, Jeffrey R., 2005. *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency; available at http://www.fas.org/irp/cia/product/curing.pdf (3 December 2008).

Crutchfield, James P., 1994. 'Is Anything Ever New? Considering Emergence', in George Cowan, David Pines & David Melzner, eds, *Complexity, Metaphors, Models, and Reality*. Boulder, CO: Westview (479–497).

Daase, Christopher & Oliver Kessler, 2007. 'Knowns and Unknowns in the "War on Terror": Uncertainty and the Political Construction of Danger', *Security Dialogue* 38(4): 411–434.

Derosa, Mary, 2004. *Data Mining and Data Analysis for Counterterrorism*. Washington, DC: Center for Strategic & International Studies.

Dumas, Mark, 2007. 'Crime, Security and Terrorism: A Geo-Intelligent Fix', *Directions Magazine*, 2 October; available at http://www.directionsmag.com/article.php?article_id=2563&trv=1 (accessed 3 December 2008).

Fishbein, Warren & Gregory Treverton, 2004. 'Making Sense of Transnational Threats', *The Sherman Kent Center for Intelligence Analysis Occasional Papers* 3(1); available at https://www.cia.gov/library/kent-center-occasional-papers/vol3no1.htm (accessed 3 December 2008).

Friedman, Thomas, 2005. *The World Is Flat: A Brief History of the Twenty-First Century*. New York: Farrar, Strauss & Giroux.

Gaddis, John Lewis, 1993. 'International Relations Theory and the End of the Cold War', *International Security* 17(3): 5–58.

Garland, David, 2003. 'The Rise of Risk', in Richard Ericson & Aaron Doyle, eds, *Risk and Morality*. Toronto: University of Toronto Press (48–86).

George, Roger, 2004. 'Fixing the Problem of Analytical Mind-Sets: Alternative Analysis', *International Journal of Intelligence and Counter-Intelligence* 17(3): 385–405.

George, Roger, 2007. 'Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm', *Studies in Intelligence* 51(3); available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no3/building-a-global-intelligence-paradigm.html (accessed 3 December 2008).

Goldman, Emily O., 2001. 'New Threats, New Identities and New Ways of War: The Sources of Change in National Security Doctrine', *Journal of Strategic Studies* 24(3): 12–42.

Halberstam, David, 2007. *The Coldest Winter: America and the Korean War*. New York: Hyperion.

Hart, Jeffrey, 1976. 'Three Approaches to the Measurement of Power in International Relations', *International Organization* 30(2): 289–305.

Heuer, Richards J., Jr., 1999. *Psychology of Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency; available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf (accessed 3 December 2008).

Hulnick, Arthur S., 2005. 'Indications and Warning for Homeland Security: Seeking a New Paradigm', *International Journal of Intelligence and Counter Intelligence* 18(4): 593–608.

Jarvis, Darryl S. L. & Martin Griffiths, 2007. 'Learning To Fly: The Evolution of Political Risk Analysis', *Global Society* 21(1): 5–21.

Jervis, Robert, 1997. 'Complex Systems: The Role of Interactions', in David S. Alberts & Thomas J. Czerwinski, eds, *Complexity, Global Politics, and National Security*. Washington, DC: National Defense University Press (45–72).

Johnson, Loch K., 2004. 'The Aspin–Brown Intelligence Inquiry: Behind the Closed Doors of a Blue Ribbon Commission', *Studies in Intelligence* 48(3): 1–20.

Johnston, Rob, 2005. *Analytic Culture in the US Intelligence Community: An Ethnographic Study*. Washington, DC: Center for the Study of Intelligence, Central Intelligence

Agency; available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/analytic_culture_report.pdf (accessed 3 December 2008).

Kent, Sherman, 1965. *Strategic Intelligence for American World Policy*. Hamden, CT: Archon.

Kerr, Richard; Thomas Wolfe, Rebecca Donegan & Aris Pappas, 2005. 'Collection and Analysis on Iraq, Issues for the US Intelligence Community', *Studies in Intelligence* 49(3); available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no3/html_files/Collection_Analysis_Iraq_5.htm (accessed 3 December 2008).

Kirkpatrick, Lyman B., 1969. *Captains Without Eyes: Intelligence Failures in World War II.* New York: Macmillan.

Knight, Ken, 2006. 'Kick-Off: A Practitioner's View of Emerging Challenges for Warning', in Center for Security Studies, ed., *Workshop Report, Global Futures Forum: Emerging Threats in the 21st Century, Seminar 1: The Changing Threat Environment and Its Implications for Strategic Warning.* Zurich: Center for Security Studies; available at http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=27872 (accessed 3 December 2008).

Kurtz, Cynthia F. & David J. Snowden, 2003. 'The New Dynamics of Strategy: Sense-Making in a Complex and Complicated World', *IBM Systems Journal* 42(3): 462–483.

McCarthy, Mary, 1994. 'The National Warning System: Striving for an Elusive Goal', *Defense Intelligence Journal* 3(1): 5–19.

Maceachin, Douglas J., 2003. *Predicting the Soviet Invasion of Afghanistan: The Intelligence Community's Record*. New York: Diane Publications.

Medina, Carmen, 2007. 'Warning and Communication: New Approaches', in Center for Security Studies, ed., *Workshop Report, Global Futures Forum: Emerging Threats in the 21st Century, Seminar 3: Warning for Readiness in the New Threat Environment.* Zurich: Center for Security Studies; available at http://www.crn.ethz.ch/publications/crn_team/detail.cfm?lng=en&id=47345 (accessed 3 December 2008).

Merry, Uri, 1995. *Coping with Uncertainty: Insights from the New Sciences of Chaos, Self-Organization, and Complexity*. Westport, CT: Praeger.

Mihata, Kevin, 1997. 'The Persistence of "Emergence"', in Raymond A. Eve, Sara Horsfall & Mary E. Lee, eds, *Chaos, Complexity, and Sociology: Myths, Models, and Theories*. Thousand Oaks, CA: Sage.

Organski, A. F. K., 1968. *World Politics*, 2nd edn. New York: Alfred A. Knopf.

Parker, Charles F., 2007. 'The Warning–Response Gap', in Center for Security Studies, ed., *Workshop Report, Global Futures Forum: Emerging Threats in the 21st Century, Seminar 3: Warning for Readiness in the New Threat Environment.* Zurich: Center for Security Studies; available at http://www.crn.ethz.ch/publications/crn_team/detail.cfm?lng=en&id=47345 (accessed 3 December 2008).

Performance and Innovation Unit, 2001. *A Futurist's Toolbox: Methodologies in Futures Work*. London: Cabinet Office; available at http://www.cabinetoffice.gov.uk/media/cabinetoffice/strategy/assets/toolbox.pdf (accessed 3 December 2008).

Power, Michael, 2004. *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. London: Demos.

Rasmussen, Mikkel V., 2001. 'Reflexive Security: Nato and International Risk Society', *Millennium: Journal of International Studies* 30(2): 285–309.

Rasmussen, Mikkel V., 2002. '"A Parallel Globalization of Terror": 9–11, Security and Globalization', *Cooperation and Conflict* 37(3): 323–349.

Rasmussen, Mikkel V., 2004. '"It Sounds Like a Riddle": Security Studies, the War on Terror and Risk', *Millennium: Journal of International Studies* 33(2): 381–395.

Rasmussen, Mikkel V., 2006. *The Risk Society at War: Terror, Technology and Strategy in the*

Twenty-First Century. Cambridge: Cambridge University Press.
Rathmell, Andrew, 2002. 'Towards Postmodern Intelligence', *Intelligence & National Security* 17(3): 87–104.
Roberts, Pat & John D. Rockefeller, eds, 2004. *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq: Conclusions*. New York: Diane Publications.
Rolington, Alfred, 2006. 'Objective Intelligence or Plausible Denial: An Open Source Review of Intelligence Method and Process Since 9/11', *Intelligence & National Security* 21(5): 738–759.
Rosenau, James N., 1990. *Turbulence in World Politics: A Theory of Change and Continuity*. Princeton, NJ: Princeton University Press.
Rosenau, James N., 1998. 'Global Affairs in an Epochal Transformation', in C. Ryan Henry & Edward C. Peartree, eds, *Information Revolution and International Security*. Washington, DC: Center for Strategic and International Studies (33–57).
Rothkopf, David J., 1998. 'Cyberpolitik: The Changing Nature of Power in the Information Age', *Journal of International Affairs* 51(2): 331–356.
Ryan, Maria, 2006. 'Filling in the "Unknowns": Hypothesis-Based Intelligence and the Rumsfeld Commission', *Intelligence & National Security* 21(2): 286–315.
Sageman, Marc, 2004. *Understanding Terror Networks*. Philadelphia, PA: University of Pennsylvania Press.
Satyanarayanan, Mahadev, 2003. 'Coping with Uncertainty', *IEEE Pervasive Computing* 2(3): 2.
Schelling, Thomas C., 1966. *Arms and Influence*. New Haven, CT: Yale University Press.
Segell, Glen M., 2005. 'Intelligence Methodologies Applicable to the Madrid Train Bombings, 2004', *International Journal of Intelligence and Counter Intelligence* 18(2): 221–238.
Shiels, Frederick L., 1991. *Preventable Disasters: Why Governments Fail*. Savage, MD: Rowman & Littlefield.
Sinai, Joshua, 2003. 'How To Forecast and Preempt al-Qaeda's Catastrophic Terrorist Warfare' (revised version), *Journal of Homeland Security*; available at http://www.homelandsecurity.org/journal/Articles/sinaiforecast.htm (accessed 3 December 2008).
Sinai, Joshua, 2007. 'Quantitative Models and Foresight', in Center for Security Studies, ed., *Workshop Report, Global Futures Forum: Emerging Threats in the 21st Century, Seminar 2: Sense-Making and Warning – How To Understand and Anticipate Emerging Threats*. Zurich: Center for Security Studies; available at http://www.crn.ethz.ch/publications/crn_team/detail.cfm?lng=en&id=30019 (accessed 3 December 2008).
Singer, David J., 1958. 'Threat-Perception and the Armament–Tension Dilemma', *Journal of Conflict Resolution* 2(1): 90–105.
Singer, David J.; Stuart Bremer & John Stuckey, 1972. 'Capability Distribution, Uncertainty, and Major Power War, 1820–1965', in Bruce Russett, ed., *Peace, War, and Numbers*. Beverly Hills, CA: Sage (21–27).
Smith, Brent L.; Jackson Cothren, Paxton Roberts & Kelly R. Damphousse, 2008. *Geospatial Analysis of Terrorist Activities: The Identification of Spatial and Temporal Patterns of Preparatory Behavior of International and Environmental Terrorists*, final report, NIJ Grant 2005-IJ-CX-0200, University of Arkansas; available at http://www.ncjrs.gov/pdffiles1/nij/grants/222909.pdf (accessed 3 December 2008).
Snowden, Dave, 2002. 'Complex Acts of Knowing: Paradox and Descriptive Self Awareness', *Journal of Knowledge Management* 6(2): 100–111.
Snowden, Dave, 2007. 'Cognitive Mapping/Sensemaking', in Center for Security Studies, ed., *Workshop Report, Global Futures Forum: Emerging Threats in the 21st Century, Seminar 2: Sense-Making and Warning – How To Understand and Anticipate Emerging Threats*.

Zurich: Center for Security Studies; available at http://www.crn.ethz.ch/publications/crn_team/detail.cfm?lng=en&id=30019 (accessed 3 December 2008).

van Loon, Joost, 2000. 'Virtual Risks in an Age of Cybernetic Reproduction', in Barbara Adam, Ulrich Beck & Joost van Loon, eds, *The Risk Society and Beyond: Critical Issues for Social Theory*. London: Sage (165–182).

van Loon, Joost, 2002. *Risk and Technological Culture: Towards a Sociology of Virulence*. London: Routledge.

Walker, R. B. J., 2006. 'On the Protection of Nature and the Nature of Protection', in Jef Huysmans, Andrew Dobson & Raia Prokhovnik, eds, *The Politics of Protection: Sites of Insecurity and Political Agency*. London: Routledge (189–202).

Waltz, Kenneth N., 1979. *Theory of International Politics*. New York: McGraw-Hill.

Warner, Michael & J. Kenneth McDonald, 2005. *US Intelligence Community Reform Studies Since 1947*. Washington, DC: Strategic Management Issues Office.

Williams, Michael J., 2008. '(In)Security Studies, Reflexive Modernization and the Risk Society', *Cooperation and Conflict* 43(1): 57–79.

Williams, Phil, 2006. '21st Century Challenges to Warning: The Rise of Non-State Networked Threats', in Center for Security Studies, ed., *Workshop Report, Global Futures Forum: Emerging Threats in the 21st Century, Seminar 1: The Changing Threat Environment and Its Implications for Strategic Warning*. Zurich: Center for Security Studies; available at http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=27872 (accessed 3 December 2008).

Wirtz, James J., 1991. *The Tet Offensive: Intelligence Failure in War*. Ithaca, NY: Cornell University Press.

Wohlstetter, Roberta, 1962. *Pearl Harbor: Warning and Decision*. Stanford, CA: Stanford University Press.