Chapter 1
Military Intelligence: From *Telling Truth to Power* to Bewilderment?

Floribert Baudet, Eleni Braat, Jeoffrey van Woensel and Aad Wever

Abstract This introductory chapter discusses 100 years of military intelligence and outlines the main changes that distinguish the post-Cold war period from the preceding one. This is characterised by a blurring of the boundaries between civilian and military intelligence, between investigative services and the intelligence community, and the foreign and domestic realms. The chapter also discusses the rise of oversight mechanisms. All these combined with unprecedented technological change to produce a challenging environment for intelligence services that is more unpredictable than ever before, and at the same time requires adequate, even pre-emptive responses on the part of the intelligence community. The dazzling level of adaptivity required largely obscures the fact that such adaptations were required in earlier periods as well, and intelligence professionals could profit by studying them.

Keywords Military intelligence · Globalisation · Adaptation · Learning organizations

F. Baudet (✉)
Netherlands Defence Academy, Breda, The Netherlands
e-mail: FH.Baudet@mindef.nl

E.C. Braat
University of Utrecht, Utrecht, The Netherlands
e-mail: e.c.braat@uu.nl

J. van Woensel
Centre of Research and Expertise, Veterans Institute, Doorn, The Netherlands
e-mail: jtwh.v.woensel@veteraneninstituut.nl

A. Wever
Enschede, The Netherlands
e-mail: ajmwever@hotmail.com

F. Baudet et al. (eds.), *Perspectives on Military Intelligence from the First World War to Mali*, DOI 10.1007/978-94-6265-183-8_1

Contents

1.1 Introduction

'The world is changing at an unprecedented pace. The present-day world is not necessarily more dangerous than it was during the Cold War but it has become more unstable and more unforeseeable', the former head of the French Military Intelligence Service (DRM) lt. gen. (ret.), André Ranson, summarized conventional wisdom as to the key challenge for today's intelligence community at a Conference to commemorate the 100th anniversary of the establishment of Dutch military intelligence in 2014.[1]

This book, which brings together scholars and practitioners, argues that although the intelligence community has indeed come to face new and complex challenges after the end of the Cold War, the key issue has been the intelligence community's (in)ability to adapt to changes in the environment in which it has to operate. In making this point, it does not offer a continuous narrative spanning a century's worth of intelligence successes and failures from the start of the First World War to the contemporary endeavours in Afghanistan and Mali. Instead, the book contains a collection of chapters that can be read individually, but which, implicitly or explicitly, address the issue of adaptivity. They show that changes in the operational environment are not unique to the post–1989 era. The operational context is constantly changing. It is adaptivity or the lack of it that in large part determines whether the intelligence community is able to deliver. Seen from this perspective, the end of the Cold War though of course important, is unjustly treated as a watershed between the present troubled times and the former conflict that in hindsight at least is often construed as a hallmark of stability where the profession of intelligence was an easy and simple one. In truth, the profession has never been easy and the cherished dictum of the intelligence community, 'telling truth to power', vastly simplifies reality.

To be sure, the post-Cold War period is characterised by a blurring of traditional boundaries, such as the one between civilian and military intelligence, between investigative services and the intelligence community, and the foreign and domestic

[1] Lt. gen. (ret.) André Ranson, keynote speech at the NISA/MIVD conference 'Telling truth to power', September 2014.

realms. All these combined with unprecedented technological change to produce a challenging environment for intelligence services that on the one hand is more unpredictable than ever before, and at the same time requires adequate, even pre-emptive responses on the part of the intelligence community. At the same time, a considerable part of this community feels that the legal limitations that have been put in place from the 1980s, do not suit present intelligence needs. As clear-cut dichotomies have faded, threats now seem to arise anywhere, demanding actionable and timely intelligence on a scale not seen before. Throughout the 20th century practitioners of military intelligence have had to come up with products that enabled military staffs, policy makers and officers to make sound judgments, and this has not changed. The number of policy options has multiplied though. In addition, it seems, calls for better control of the activities of the intelligence community are more vocal now than they were in earlier periods.

However, the dazzling level of adaptivity required today to a large extent obscures the fact that such adaptations were required in earlier periods as well. The intelligence community has always had to respond to change, develop new procedures and methods and reinvent itself. As today, it encountered failure when it identified the wrong lessons from earlier experiences. Leaving aside for the moment the question of whether it is possible to learn clear-cut lessons from the past at all, it is clear that today, as intelligence professionals struggle to come to grips with the challenges posed by transnational terrorism, hybrid opponents and complex stabilization missions, they, their customers, and academics, might profit from studying earlier adaptation processes. These could help identify best practices and perhaps more importantly, pitfalls. This, however, is not a recipe for success. There is at least a grain of truth in the old saying; *incidit in Scyllam qui vult evitare Garybdim.*

This introductory chapter outlines the changes in the environment in which the intelligence community operates, and then goes on to discuss how they affected this community. In the next sections, this analysis will be augmented by an analysis of learning processes, and especially the way past experiences are internalized. The case studies presented in this volume will provide insight in the complexities involved.

1.2 A Changing Environment

At first sight, the end of the Cold War is a watershed indeed. The spectacular collapse of the Soviet empire and its ideology in 1989–1991, ended a geopolitical confrontation that had lasted nearly five decades, and according to some, even longer.[2] While these momentous events initially seemed to guarantee a dominance of liberal-democratic values, the wave of neo-liberalism that swept across the globe also promoted distrust of state institutions in general, and stressed free and

[2] Vanden Berghe 2008.

unchecked enterprise. For some the post-1989 high-tide brought unprecedented opportunities, yet globalisation in many parts of the world eroded traditional structures and loyalties and left millions without shelter, especially in states whose leaders had until then been sponsored by one of the two sides in the Cold War. These processes resulted in the fragmentation of a significant number of states that now were labelled weak, failing or even failed states. Having lost legitimacy and relevance in the eyes of their population they became a recruiting ground for all kinds of radical groups, including ultranationalist and terrorist ones.[3]

After the end of the Cold War, international institutions and international law initially gained more prominence and many placed their hopes on an effective United Nations, but the tragic inability of this institution and the mostly western states that dominated it to prevent large-scale bloodshed in Rwanda, Somalia and the former Yugoslavia dealt a crushing blow to the initial optimism.[4] Today, the UN is often considered powerless if not outright irrelevant in the face of many of the challenges that have risen since.

The rise of new global players such as China, and to a lesser degree, India, seemed to cause, or at the very least coincide with, a relative decline of the West whose leading nations for centuries had dominated the world and in large part shaped the international system and its accompanying rules of behaviour.[5] These rules and supra-national norms came to be questioned in many western countries as well, especially in the greatly expanded EU where citizens started to 'reclaim' national sovereignty and stressed national rights, identities and particularism in a way not seen since the Second World War.[6] Meanwhile, the Pacific has become a new hotspot, whereas the Middle East, partly as a result of Western interventionism, has destabilized on a scale hardly imaginable in the mid-1990s when peace between Israel and its Arab neighbours seemed a real possibility.

At the same time technological innovations such as the invention and then stunning advance of the internet have created unprecedented opportunities. Especially when combined with the liberal democratic dogmas of freedom of speech and freedom of information, the technological advances of the last two decades have also created a powerful brew that erodes traditional sources of power. The fact that it is relatively easy to reach millions of people in one mouse click, transcending borders and circumventing controls, gave rise to the argument that the internet would spell the end for dictatorships and oppression, as ideas of democracy and human

[3] Scholte 2000.

[4] Cf. Fukuyama 1992. The UN critically evaluated its performance in 2000.

[5] See Ferguson 2011. On some of these contenders: Kaplan 2010; Brewster 2014; Segers 2008; Kingah and Quiliconi 2016; Stuenkel 2015. For a contrary view: Beausang 2012.

[6] Witness calls in Britain, France, The Netherlands and Switzerland to renege the European Convention on Human Rights, and such international treaties as the Convention on the Status of Refugees.

rights could now spread to the four corners of the world. The role of internet-based new media during the Arab Spring has been put forward as a case in point.[7]

Sound-bites and 140-sign messages have overtaken the slower, printed media whose formats offer more room for longer analyses and nuance, reinforcing a trend that had started with the rise of television. Real-time coverage of real-time events demands real-time responses as journalists and politicians in democratic states have discovered and every individual may become a news network if he or she so desires and finds an audience. For most young people classic media i.e., newspapers, radio and television that by their format more or less channelled access to information and selected what audiences would be exposed to, have become utterly irrelevant. Vertical relations between media and audiences have eroded while horizontal relations have multiplied beyond count.

This development could be termed democratization although it was not only democracy that benefited from it, to say the least. A key consequence of the accompanying over-supply of information is that people 'settle for 'blips' of information, which they then attempt to string together in a sensible manner to account for changes in their environment.'[8] Overarching narratives and traditional authority have lost appeal, but individuals' need for sense-making has not disappeared. Moving beyond the boundaries of the digital world, it has given weight to the *vox populi* in a way unthinkable before. As the a priori legitimacy of popular sentiment is a key element in democracy,[9] it has become a distinctly destabilizing element in many of today's democracies.

The rise of violent non-state actors has brought with it new applications. These actors use social media as a means of political communication, as with ISIL clips that show beheadings and the destruction of non-Sunni cultural heritage it considers pagan. The internet is also used for recruitment and training and ISIL for one operates a large number of Twitter accounts.[10] There are indications that at least some of these violent non-state actors have been developing offensive technical cyber capabilities as well. ISIL is suspected to have attacked the US Department of Defense which resulted in the theft of addresses of US military personnel and calls to kill those. Other examples include groups such as the Cyber Caliphate.[11] Today, intelligence services consider 'cyber terrorism' a real possibility although as yet recognized examples of terrorist cyber-attacks are absent.[12]

[7] Witness A Human Right 2014 and Howard 2011. For a discussion of the threats and opportunities offered by new technologies, see Kalathil and Boas 2003; Klang and Murray 2005. See further Salih 2013, pp. 185–203; Soengas 2013, pp. 147–155; Etling et al. 2010, pp. 2–10; Safranek 2012, pp. 2–10. Similar claims have been made about the end of the Suharto era: Mahdi 2002. See also Conversi 2012, pp. 1357–1379.

[8] Toffler 1980, p. 165.

[9] For an insightful discussion see Cunningham 2002.

[10] Gladstone 2015.

[11] Ingram 2015. On the rise of cyber Jihadis: Berton and Pawlak 2015; Atwan 2016.

[12] States may prefer to attribute damage to vital infrastructure and networks to bad luck, accidents and technical problems rather than admit weakness.

The so-called dark web—that part of the world-wide web that cannot easily be accessed using traditional search engines—has become a market-place of, among other things, instruction manuals and weaponry and a meeting place for people and groups whose aims and activities often are cause for serious concern.

In addition, both democratic and authoritarian states have been tempted to use the internet for their own purposes; intelligence services engage in cyber espionage, and in computer network exploitation on a daily basis. They, just like companies, make ample use of trolls to favourably influence popular sentiment through social media.[13] More worrying still, revelations such as those by Edward Snowden show that intelligence services make use of internet-based technologies to survey the movements and communications of hundreds of thousands of individuals.[14] At the same time, hacks, bots and other electronic means are used to influence the outcome of electoral processes as the 2016 US Presidential Election showed.[15]

Especially the revelations about large-scale indiscriminate surveillance caused a public outcry and reinvigorated discussions about (the lack of) control of the intelligence community. In the modern era such interest had earlier manifested itself in the aftermath of the 9/11 attacks when services were believed to have failed to 'connect the dots'; after the invasion of Iraq that was justified on the basis of what turned out to be faulty and manufactured evidence on this country's programme of weapons of mass destruction; and again as a result of a number of revelations about less than savory activities of intelligence services, such as the CIA's rendition programme that involved the abduction of suspected individuals and their transfer to facilities in states that, unlike the US, allow torture as a means to obtain information, and the role of a number of European services in this.[16] Policy makers currently face the challenge to strike a balance between the contradictory public demands for better protection against terrorist attacks and protection from infringements on their privacy. Practitioners often argue that any limitation on their work poses a risk to national security whereas human rights campaigners and numerous others feel that to grant more powers to the intelligence community undermines their constitutional rights and such legal principles as *nulla poena sine lege*.[17] It is a discussion that as yet has not reached a satisfactory outcome.

[13] For Russia's use of these means F-Secure Labs 2015. Cf. Bellingcat 2016; Gathmann et al. 2014.

[14] MacAskill et al. 2013.

[15] See for instance http://www.nytimes.com/interactive/2017/01/06/us/politics/document-russia-hacking-report-intelligence-agencies.html?_r=0; Glaser 2016; Markoff 2016; Mozur and Scott 2016.

[16] Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe 2006.

[17] Hill 2016; Eijkman and Van Ginkel 2011, p. 16; Council of Europe. Commissioner for Human Rights 2015.

1.3 Precedents

The changes outlined in the previous paragraph are indeed spectacular and adaptation to them may indeed have proven particularly difficult. Still, the 20th century has seen many more occasions of fundamental change, even though its fundamental impact nowadays seems largely forgotten as the world it shaped is taken for granted. Then, as now, adaptation to (sudden) changes in the environment was difficult, and, as now, at times it was less than adequate. And then, as now, intelligence practitioners and their customers have reacted atavistically when they had better reviewed the available information once more and be more imaginative. Intelligence communities have been outsmarted by their adversary counterparts; military establishments and policy makers have rejected analyses because they did not fit their frame of reference or policy preferences, and imminent attacks were considered unimaginable. In such cases what can be termed 'Noise Barriers' occur.[18]

The invention of the telegraph, for instance, not only stimulated interception techniques and the rise of signals intelligence, it made long-distance communication, and with it colonial rule, incomparably more effective. It gave colonial powers the upper hand and enabled direct control from the 'motherland'. During the same period advances in naval technology, in particular the advent of steam-powered warships, gave them a distinct technological edge, not to mention staying power, over indigenous opponents. Both developments, however, took time to digest, and the Dutch, to give but one example, trusted their newly acquired technological edge over their previous intelligence-based means of dominating their vast colonial holdings in present-day Indonesia. It was only after they had rediscovered the value of good intelligence, however, that they managed to gain the upper hand in the Aceh War (1873–1912).[19]

It also took time to fully grasp the potential of the aeroplane. While initially it was believed to fit for reconnaissance only, over time the aeroplane acquired additional roles, ranging from aerial bombardments to (strategic) surprise attacks using airborne troopers.[20] Aircraft thus reduced the relevance of fixed ground defences and, especially, waterways, and the possibility to freely manoeuvre ground forces. The full implications however were largely overlooked until the catastrophic events of May–June 1940 when Germany defeated France and Britain in a mere six weeks. Another consequence of the invention of the airplane was that the classic distinction between civilians and combatants became more difficult to maintain; in fact, even before the invention of aircraft, writer H.G. Wells predicted aerial bombardments on cities and industrial centres that would be decisive, as they would

[18] See, for instance, Metselaar 1997.

[19] Kitzen 2016.

[20] House 1993, p. 6.

result in breaking a population's will to resist.[21] While the fear of aerial bombardment was a key feature of the Inter-war years, it proved difficult to accurately assess its impact during the Second World War. It was either over-estimated or downplayed and intelligence did both—expecting German morale to break in strategic bombardments when British evidently had not.

Even the current surge in public concern over intelligence services' activities and calls for a better control of them, has its historical counterparts. Earlier decades have also witnessed a period of marked increase in interest in the intelligence community's doings. In the 1970s for instance, the CIA's operations during the preceding twenty-five years led to a Congressional inquiry that put certain limits on what the US intelligence community could and could not do.[22] As today, at the time practitioners felt that tighter controls would fatally hamper their work, yet during the 1980s and early 1990s in many Western countries steps were taken to place intelligence and security services on a statutory footing. It is fair to say that these may have indeed demanded considerable adaptation on the part of the intelligence community. Yet, a statute also provided a clear demarcation of tasks and responsibilities.[23]

1.4 A Revolution in Intelligence Affairs?

While intelligence may be dubbed the second oldest profession in the world and early literature such as the *Iliad* and the *Bible* contains examples of intelligence operations,[24] especially during the last century or so the nature and practice of intelligence has changed tremendously. Humint, which dominated most of the intelligence practice before 1900, gradually receded as aerial surveillance and telegraph intercepts gained prominence. Intelligence itself was professionalised and institutionalised and many states acquired specialized units capable of collection and analysis of foreign military data. With it came the assumption that enemy capabilities were crucial in assessing threats, if only because intentions can change overnight. During the Cold War for instance Kremlin watchers spent years trying to assess the Soviet Union's intentions, but while this spawned a whole new type of scholarship—sovietology—the main focus of military intelligence remained the Soviet Union's military capabilities if only because it proved difficult to gauge, for instance, whether the Soviets actually were guided by Lenin's teachings. 'Bean counting', assessing Soviet capabilities, therefore remained the core business of military analysts.

[21] Douhet 1921; for a discussion, see Hippler 2013. Cf. Black 2016.

[22] Hancock and Wexler 2014; Immerman 2010; Olmsted 1996.

[23] Lander 2004.

[24] See Iliad, X, 195 ff and the Bible, Numbers, 13: 1–33.

After the end of the Cold War, and especially after 9/11, as a result of the multi-faceted process of globalisation and the rise of new technologies and new threats, as outlined above, a new type of conflict arose. Intelligence requirements changed; time-tested approaches proved no longer sufficient to provide early warning or trustworthy information. As before, intelligence will have to be timely and actionable, but unlike in previous periods states face threats that to a large extent are de-territorialized and networked. And while adversaries generally do not have state-of-the-art weaponry, it is their ability to strike anywhere that is cause for concern. Often, such adversaries are millenarian in nature, and could not care less about threats of retaliation. They are also prone to hide among the population.[25] Taken together, this means that 'bean counting' is not only much more difficult than before, it is no longer sufficient. Finding the enemy has become a challenge, and he is only identified through his actions. Given the disruptive potential of terrorism, (real-time) intelligence has to be able to provide trustworthy information about intentions and it has to be pre-emptive rather than merely predictive. Yet new technologies and analytical methods, or simply a huge increase in analytical capacity did not necessarily produce the intelligence products needed to meet the new challenges.

This worrying assessment spurred a debate about the necessity of a 'revolution in intelligence affairs', a debate that revolved around the need to devise new methodologies and technologies to maintain the relevance of intelligence in this changing environment.[26] This debate was part of a wider debate on the changing character of war and the ability of (western) states to anticipate and properly react. Some, like Kaldor, identified the changes discussed above as leading to 'new wars', intimating that old ways and habits, and old responses, were rapidly becoming obsolete.[27] Intra-state war rather than interstate war was becoming the norm, and, as Smith argued, Western armed forces had to adapt better or become irrelevant. From Smith's and Kaldor's analyses it transpired that the changes at the turn of the century were fundamental and posed an existential challenge for armed forces and their intelligence apparatus alike.[28]

By contrast, in the wake of the ostensibly successful invasion of Iraq in 2003 an opposing school of thought argued that the West's military supremacy was secure for time to come as a limited hi-tech conventional force could defeat any opponent. State of the art technology in terms of aircraft, reconnaissance equipment and weapon systems would suffice. This would produce near real-time intelligence which, so the argument ran, would lead to 'network-enabled' surgical operations that guaranteed success.[29]

[25] Kaldor 2012 (1st edition 1999).

[26] See for example Denécé 2014.

[27] Cf. Kaldor 2012, pp. 4–5, 72–78.

[28] Smith 2005.

[29] See Cohen 2003.

In between, so to say, was Frank Hoffman's concept of 'hybrid warfare', that acknowledged the occurrence of momentous change but at the same time held that Western armed forces could in fact adapt to counter enemy forces engaged in hybrid warfare.[30] 'Conflict in the 21st century: The rise of hybrid wars', as the report was called, signalled the rise of a wide range of variety and complexity in contemporary and future conflict.[31] Hybrid threats incorporate a full range of modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts that include indiscriminate violence and coercion, and criminal disorder.[32] At the time of writing only one such enemy force could be considered as a 'hybrid' opponent: Hezbollah. Yet, since 2007 the world has seen other 'hybrid' opponents as well, which makes it a useful analytical tool.[33] ISIL, despite its ambitions to be recognized as a state actor, employs a mixture of conventional and irregular tactics, the latter comprising of untempered terror against what it considers infidels and Western agents, and a sophisticated use of modern communication techniques. Actors such as these are often labelled with different terms. Some are called terrorists, others insurgents, yet others engage in organized crime; and for a while 'violent non-state actor' served as a catch-all phrase.[34]

Taken at face value there are considerable differences between them; however, what they have in common is that these terms describe a versatile, intelligent opponent that is often network-based, highly flexible and adaptable, that is primarily non-state in scope, that is able to learn from mistakes at a higher pace than established states can, and that has an ability to exploit social and financial institutions and embed themselves in them. Lastly, they possess a distinct capacity for recovery and regeneration when they are under attack.[35]

Some states, too, have been tempted to engage in hybrid tactics such as the use of widespread disinformation campaigns. A key example here is Russia that employed 'patriotic cyber warriors' in its wars with Georgia (2008) and Ukraine (2014–present).

Against the background of this (apparent) hybridisation of warfare, intelligence requirements changed, but progress was difficult and often uneven. When the Cold War ended and new conflicts that were ostensibly different in nature erupted, public calls to employ military means to stem them were particularly strong. Although this led to a surge in UN peacekeeping operations during the 1990s, these were not

[30] For a discussion, see Duyvesteyn and Angstrom 2004.

[31] Hoffman 2007. Compare Malis 2012, pp. 187–190; McCulloh and Johnson 2013.

[32] Hoffman 2007, p. 36. See also Freier 2007.

[33] De Wijk 2012, p. 358.

[34] Thompson 2014; Manwaring and Corr 2008, pp. 75–77; Bunker 2012, pp. 45–53; Denécé 2014, pp. 29–30.

[35] The description is based on Kuperwasser 2007, p. 4; Hammes 2006, p. 35 and Treverton and Agrell 2009, pp. 2–3.

complemented by a rise in the number of intelligence specialists that were deployed. At the UN level traditionally there was a distinct hostility toward 'intelligence' and the organization was slow to change in this respect. It was only after such catastrophes such as in Rwanda and Srebrenica that the idea that the UN needed some sort of early-warning mechanism and some analytic capability of its own started to permeate the organisation.[36]

After 9/11, the US Government and other Western states intensified their struggle against terrorist groups. The US now proclaimed a 'war against terror'. It responded militarily in Afghanistan in 2001, and then went on to occupy Iraq, but it was not able to eradicate terrorism. In the process it found that its actions spawned new acts of terrorism as its heavy-handed approach—the use of waterboarding, the renditions programme, and its refusal to grant captive suspects a legal status—did much to erode the good will the US could command in the region. It also cost them the sympathy of traditional allies that preferred to treat terrorism not as an act of war but as a crime. Critics also pointed at the Patriot Act and similar legislation that contrasted with civil rights enshrined in the US Constitution. Proponents argue that this is necessary in view of the threats facing the US (and the Western world in general). The discussion is complicated by the fact that especially when confronted with the terrorist threat, the intelligence community faces tremendous pressure, both from policy makers and from society that wants protection. While in most countries the actual number of people killed in acts of terrorism probably does not exceed the number killed in car accidents, the social impact of such acts is such that politicians and policy makers feel compelled to prioritize the struggle against terrorism over the struggle for safer traffic. When a service is found having failed to 'connect the dots', the answer is rarely sought in smarter methodologies. Instead, services face rounds of reorganisations and ask for expanded competences and funding, which they generally receive.[37]

While the fear of terrorism propelled calls for expanded powers for the executive, the classic divide between the foreign and domestic spheres is eroding, just as the divide between investigative services and intelligence is becoming more fluid. This is understandable in that in the end a state's legitimacy is put at risk if it cannot provide security to its population. The need of governments to be seen to be effective (however defined) in the struggle against terrorism has produced a shift toward pre-emption and prevention, hence the need for intelligence.

However, to a large extent this has resulted in an amalgamation of two realms that, at least originally, have had an entirely different function; investigative services are to amass solid proof. They have to enable a prosecutor to open legal proceedings with a fair chance of success. Intelligence services, by contrast, are

[36] Cf. UN 2000.

[37] The tendency to ask for expanded competences does not only derive from the desire to become more efficient, but also from the administrative rationale to increase one's power and as such to secure its administrative 'lifeblood' (Long 1949, pp. 257–264).

about indication and warning. They are about the probability of a certain course of events taking place, not about truth per se. While accuracy is an important criterion, timeliness is even more important. To be able to tell the score of a soccer game after it was played, is nice but from an intelligence perspective it is useless: what matters is to know in advance which players will be on the pitch so that the opposing side may adjust its tactics. For an investigative service, however, accuracy is pre-eminent. The final score matters just as much as the answer to the question which players actually played the match.[38] Put differently, the prime focus of an investigative service is facts; that of intelligence services is likelihood. The blurring of these realms could well result in erosion of the rule of law, and in an increased sense of insecurity.

Since failure is not an option, and hybrid adversaries could be literally everywhere—after all, they do not care for borders—all kinds of information could be held to provide vital data. Accordingly the classic divide between military and non-military intelligence became blurred, a development that manifested itself in such concepts as ‘population-centric intelligence’, and ‘intelligence-led operations’, and in the renewed popularity of the notion of ‘winning hearts and minds’. Though after 9/11 intelligence services were more lavishly funded and states engaged in wars of choice, fighting terrorists around the globe, it was found on numerous occasions that good intelligence rather than sheer numbers was the key to success, however defined.

Still, the adaptation has been markedly uneven. Today, US CENTCOM alone has some 1,500 analysts at its Headquarters, with an additional unknown but certainly larger number deployed in the wider Middle East, its area of operations. Even so, it has been forced to acknowledge that events in Iraq, Afghanistan and Syria ‘surprised’ them.[39] Recent examples include the Taliban offensive that resulted in the capture of Kunduz, and the direct Russian involvement in Syria. With a yearly budget of over 50 billion dollars and employing over 1.5 million personnel and contractors, apparently the US intelligence community faces enormous challenges that cannot be met by an ever-increasing budget, widening the net, outsourcing part or all of the intelligence cycle, or by expanding the authority of intelligence services.

Surprise attacks and intelligence failures will always remain hard to avoid, as the literature on intelligence history overwhelmingly shows. They are, as Perrow argues, ‘normal accidents’.[40] Paradoxically, greater financial means and expanding authorities may have had counterproductive effects. In fact, long-time commentator Engelhardt has suggested that part of the explanation behind these failures in Iraq, Afghanistan and Syria is not only the inability to make sense of the enormous amount of data that US services collect, but also that collection effort itself.[41]

[38] As Bob de Graaff once put it eloquently.

[39] Engelhardt 2015.

[40] Perrow 1999.

[41] Engelhardt 2015.

Equally worrying is that proper collection and analysis can only be done on the basis of requirements that are to the point. Intelligence needs to be timely and accurate to be relevant but so do requirements. All too often intelligence customers still think that intelligence either has the power to predict the course of events, or can be replaced by reading the newspapers. High-quality intelligence reports need to be read to be relevant, and customers need the knowledge to establish what their requirements are. In spite of decades of close cooperation there is still a great deal of misconception about what intelligence can provide, just as there is mistrust between intelligence and other branches of the executive, not least the military.

1.5 Learning

As said, if we look at military intelligence these changes have become manifest especially after the end of the Cold War. The following description, taken from an article in the Washington Post, gives a good insight into practice as developed in Afghanistan:

> The CIA provides intelligence analysts and spycraft with sensors and cameras that can track targets, vehicles or equipment for up to 14 hours. FBI forensic experts dissect data, from cell phone information to the 'pocket litter' found on extremists. Treasury officials track funds flowing among extremists and from governments. National Security Agency staffers intercept conversations or computer data, and members of the National Geospatial-Intelligence Agency use high-tech equipment to pinpoint where suspected extremists are using phones or computers.[42]

All this is markedly different from earlier practice. Nonetheless, the rise of new technologies during the final decades of the 19th century similarly changed the nature of military intelligence and the world it had to report on. Throughout the 20th century the underlying issue has thus been the ability of the intelligence community to adapt to changes in the realms of technology, politics, economy, strategy, and law. This adaptation or the lack thereof impacted directly on the effectiveness and the quality of the intelligence community. Failure to read the signs led to military and political defeat.

While it is beyond the scope of this introduction to discuss the debate on adaptation and innovation in full, a few points need to be made here. Innovation is closely connected with the ability to learn at the organisational level. At this level, individual experiences may combine and produce a synergetic effect.[43] For this to happen, Marsick and Watkins identify a number of preconditions. These are (a) openness across boundaries, (b) resilience or the adaptivity of people and

[42] Warrick and Wright 2008.

[43] Merriam et al. 2012, p. 44.

systems to respond to change, (c) knowledge and expertise creation and sharing, (d) a culture, systems and structures that capture learning and reward innovation.[44] From these characteristics it transpires that military organizations and intelligence organizations are not natural-born learning organizations.

In their recent volume on military adaptation Theo Farrell, Frans Osinga and James A Russell reach a similar conclusion. They outline a number of imperatives for adaption, which they distinguish from innovation. Adaptation is doing new things with existing materiel; adaptation may lead to innovation, or it may not.[45] They hold that history clearly shows that war forces states and their militaries to adapt, as 'states and militaries that fail to adapt risk defeat'.[46] Operational challenges and technological change are the main drivers, but unfamiliarity with the terrain or the political environment may suffice to convince militaries of the need to adapt.[47] Domestic politics, strategic culture, alliance politics and civil-military relations impact on whether a perceived need will translate in actual adaptation.[48] Farrell and his co-editors argue that as conservative institutions armed forces are 'especially disinclined to change' and identify the bi- or tri-yearly rotation as a key impediment for the institutionalization of lessons learned.

Based on the Afghanistan experience, they argue that an open culture is crucial, which ties in with the findings of Marsick and Watkins discussed above. Officers of the German *Bundeswehr* were not expected to express their personal views and, accordingly, the Germans had greater difficulty in adapting to realities on the ground than other contingents. Size, by contrast, may enable adaptation as, in the absence of formal institutionalized learning, personal contacts between consecutive Dutch and Danish officers in the field helped them to identify and disseminate best practices. This informal learning, however, does not find its way into field manuals and lessons tend to be tactical only.[49]

In addition, best practices may be based on mere coincidence. While military organizations generally pride themselves in that they heed 'lessons learned', and hold that military doctrine contains the condensed valuable lessons of past experience, they generally overlook the fact that learning from the past is not a straightforward exercise. In the context of a military operation, it is difficult to make truthful claims about causality. Likewise, it is impossible to establish in advance which 'lesson' is the correct one. Furthermore, the analysis of past experience is often influenced by preferences, corporate interests and personal agendas.[50]

While intelligence services are somewhat different from military establishments they share most of their characteristics. Taking Marsick and Watkins'

[44] Marsick and Watkins 2005, p. 357.

[45] Farrell and Terriff 2002, p. 6.

[46] Farrell et al. 2013, p. 1, 4 (quote).

[47] Idem, p. 4.

[48] Idem, p. 3.

[49] Idem, pp. 305–306.

[50] Baudet 2013.

characteristics of 'healthy' learning organizations as a basis, intelligence organizations are poor learning organizations. They are not open across boundaries, as the secretive nature of their work produces a secretive internal culture. While they do create knowledge, sharing this knowledge is limited to the customer. A complicating factor is the frequent rotation of military personnel within military intelligence organizations. This precludes specialisation. Intelligence organisations perform somewhat better on the last count: they do capture learning (although mostly not in a structured way), and they generally are resilient. Their responsiveness to change is somewhat problematic, however. After all, it was concern for this matter that spurred the debate on the necessity of a revolution in intelligence affairs. Lastly, while individuals may adapt, the secretive culture of intelligence organizations may hamper innovation.

Like any bureaucracy, civilian or military, self-preservation is a primary goal. They need to be relevant in the eyes of their political bosses, who, in turn, do not want to be confronted with unpleasant surprises. This not only impacts the collection and analysis of short-term and often tactical intelligence. As to strategic intelligence this may lead to a focus upon the politician's short-term preferences rather than on mid- to long-term emerging threats.

While Farrell, Osinga and Russell hold that military adaption will most likely be the result of war, it seems that intelligence organization behave in a different way. Past experience is absorbed at a number of levels. At the individual level, as the future is inevitably obscured, past experience and the ideas it has shaped give a body of reference an analyst and a policy maker can turn to. The temptation to turn to this body of reference seems particularly strong in times of sudden change, whereas it is normal routine in periods of relative stability. This may be explained from the fact that intelligence practitioners tend to trust their instincts so to say, and apply these to analyse new information that is handed to them. This 'instinct' is informed and conditioned by past experience in a process that has been termed 'everyday learning'.[51] This need not surprise us, as Niall Ferguson, though writing in a different context, reminds us:

> The past is really our only reliable source of knowledge about the fleeting present and the multiple futures that lie before us, only one of which will actually happen.[52]

The problem of course is, that the study of the past may *suggest* a certain course of events, rather than predict.[53] Accordingly, a focus on past outcomes may well lead to misguided assumptions about the future. The past complicates both the present and future, and it limits our freedom of decision and movement.

At the institutional level, past experience may explain why intelligence organizations face the ever-present phenomenon of groupthink. This, after all is little more than a way to make sense of contradictory data by an over-appliance of a

[51] Illeris 2004, p. 151.

[52] Ferguson 2011, p. xx.

[53] Murray and Sennreich 2006.

common frame of reference that by its very nature is inevitably based on *past* experiences. As such it risks losing sight of the exigencies of the present, let alone the future. Groupthink is an inherent feature of intelligence, or any process in which information is analysed and processed. Scholars tend to judge the quality of new research by their own ideas on the subject. In intelligence this risk is even more present and it may well lead to the smothering of deviating views. It may therefore be tempting to disregard the past altogether and start with a clean slate, which, of course, is utterly impossible. Whether we like it or not, we are a product of our past experience.

Also at the institutional level, the past enhances the corporate identity of an agency. Specific features of intelligence as a profession, such as a penchant for secrecy and compartmentalisation, condensed as 'best practices', result from past experience and certain time-tested methodologies may still provide adequate and timely intelligence. At the same time, successful adaptation may require an overhaul of such time-tested approaches. In short, the uses of the past may engender groupthink and inflexibility.

The contributions to this book serve to illustrate the complexities of dealing with past experience in anticipation of future developments. They are based on original research and in several cases challenge conventional wisdom. Some of them, like Klinkert's and Mahadevan's chapters, highlight both professionalism at the tactical level and naïveté at the strategic. Klinkert discusses the establishment and early successes of a professional military intelligence service in The Netherlands, and outlines how at the political level, in spite of warnings by the army leadership and the intelligence community, a faulty analysis of The Netherlands' experiences in the First World War and the trends in major warfare fatally impacted on the country's preparedness to withstand the German attack of 1940.

A similar analysis is provided by Mahadevan in his discussion of the Indian intelligence community's performance in the run-up to the 1962 border war with the People's Republic of China. Its origins as a domestic security service in the British Raj, and the *savoir-faire* based on its experiences during the last decade or so of British rule, fatally impaired the Indian intelligence community's ability to adequately read Beijing's intentions. Their faulty analysis informed the decisions taken in Delhi, and the result was defeat.

Easter discusses a topic that received little attention in English-language historiography. Taking place just weeks before the better-known Cuba Crisis, the confrontation between Indonesia and The Netherlands over West New Guinea also involved secret supplies to Indonesia of Soviet manned submarines and bombers that Moscow was prepared to deploy in the event of an attack. Allied intelligence found out about their presence but failed to establish whether they would be used. Another interesting aspect is the apparent failure of the Dutch to learn from their defeat against Indonesia in the late 1940s.

Whereas the West-New-Guinea Crisis and the Cuba Crisis were classic crises in that cause and effect relations appeared rather straightforward, Kwa argues that as a result of the momentous changes that have taken place in the international system, a paradigm shift is urgently needed to handle contemporary strategic challenges, and, specifically, crises that spring from strategic surprise.

Boelens, a practitioner, is rather more optimistic about the Intelligence Community's present ability to deliver. Discussing the 2006 conflict between Israel and Hezbollah and the Israeli operation against Hamas in 2008, and experiences with interagency teams in Iraq and Afghanistan, he argues that the Israeli and US Intelligence Communities have in fact adapted to changing circumstances. These cases provide a model that others should follow.

Moving on to the realm of intelligence in peacekeeping operations, this book contains three chapters that, especially when read together, identify the major developments and ongoing challenges in peacekeeping intelligence. Discussing UNPROFOR, Wiebes, Van Woensel and Wever conclude that the fall of Srebrenica in July 1995 resulted from the failure of all intelligence services concerned to timely identify the possibility that the Bosnian Serbs would launch a full-scale attack to conquer it. United Nations intelligence structures were very weak, and the Dutch peacekeepers inside the enclave failed to take measures to redress these deficiencies. In addition, at the political and military-strategic level a belief had developed that peacekeeping operations did not require intelligence.

Theunens, who has been the head of UNIFIL's Joint Mission Analysis Centre (JMAC) since 2009, argues that the UN learned from past experience such as Bosnia and the Great Lakes area, but he identifies a number of area where further development and fine-tuning is possible, notably JMAC's relations with another new type of unit, the All-Source Intelligence Fusion Unit (ASIFU).

Whereas Theunens primarily focuses on JMACs, Rietjens and Dorn, who discuss experiences in MINUSMA, critically review ASIFU. While no doubt the Mali experience provided useful lessons for future intelligence capabilities within peacekeeping operations, the ASIFU experience also shows that lessons from previous operations were not fully internalized.

The last contribution builds upon the assumption that spurred by globalisation, international intelligence cooperation and the blurring of once well-defined and separate realms are here to stay. Braat and Baudet discuss the rise of intelligence oversight and the subsequent development of an accountability gap which resulted from the acceleration of international intelligence cooperation. They present an innovative instrument to systematically assess the quality of intelligence accountability, on a national level and for the purpose of transnational comparisons. This instrument contributes to closing the intelligence accountability gap in the field of international intelligence cooperation and striking a balance between secrecy and public trust. Proper historical research occupies an important place in this assessment instrument.

1.6 Concluding Remarks

While past experience to a large extent shaped present practice, it can never be a justification in itself.[54] Ironically, as the following chapters show it is by studying the past that this becomes evident. Uncritical adherence to best practices—the condensed experiences from the past—may lead to calamities. In fact, today more so than ever, as technologies and concepts are changing fast, analysis of past examples and experiences will need to be more precise, and more critical. Clinging to outdated best practices may be a recipe for failure, but, at the same time, past examples and experiences may also offer inspiration for new best practices, new procedures and new concepts.

Several decades ago, British military commentator Basil Liddell Hart wrote a devastating comment on the way armed forces studied the past. They tended, and to a large extend still do, to embellish their exploits and to gloss over what they did not want to be remembered. This practice produces a corporate identity, but one that is flawed. Furthermore, it may lead to failure:

> Camouflaged history not only conceals faults and deficiencies that could otherwise be remedied, but engenders false confidence—and false confidence underlies most of the failures that military history records. It is the dry rot of armies.[55]

It is no different with intelligence services and governments.

References

ahumanright.org (2014) A human right: Everyone connected http://ahumanright.org Accessed 10 December 2015.

Atwan AB (2016) Das digitale Kalifat: Die geheime Macht des Islamischen Staates. Beck, Munich

Baudet FH (2013) Quelques réflexions sur l'exploitation du passé dans les forces armées. Air and Space Power Journal – Africa and Francophonie 4(4):4–14

Beausang F (2012) Globalization and the BRICs: Why the BRICs Will Not Rule the World For Long. Palgrave McMillan, London

Bellingcat (2016) Behind the Dutch terror threat video: the St. Petersburg "Troll Factory" connection. Bellingcat 3 April 2016. https://www.bellingcat.com/news/uk-and-europe/2016/04/03/azov-video/

Berton B, Pawlak P (2015) Cyber jihadists and their web. European Union Institute for Security Studies Brief Issue 2, Brussels

Black J (2016) Air Power: A Global History. Rowman & Littlefield, London

Brewster D (2014) India's Ocean: The Story of India's Bid for Regional Leadership. Routledge, London

Bunker R (2012) Changing Forms of Insurgency: Pirates, Narco Gangs and Failed States. In: Rich PB, Duyvesteyn I (eds) The Routledge Handbook of Insurgency and Counterinsurgency. Routledge, London, pp. 45–53

[54] Idem.

[55] Liddell Hart 1971, p. 27.

Cohen E (2003) Supreme command. Soldiers, statesmen and leadership in wartime. Free Press, New York

Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe (2006) Alleged secret detentions in Council of Europe member states. Information Memorandum II, AS/Jur (2006) 03 rev http://assembly.coe.int/committeedocs/2006/20060124_jdoc032006_e.pdf Accessed 8 February 2016

Conversi D (2012) Irresponsible Radicalisation: Diasporas, Globalisation and Long-Distance Nationalism in the Digital Age. Journal of Ethnic and Migration Studies 38(9):1357–1379

Council of Europe. Commissioner for Human Rights (2015) Intelligence: “French Draft law seriously infringes human rights”.

Cunningham F (2002) Theories of democracy: A critical introduction. Routledge, London

de Wijk R (2012) Hybrid Conflict and the Changing Nature of Actors. In: Lindley-French J, Boyer Y (eds) The Oxford Handbook of War. Oxford University Press, Oxford, pp 358–372

Denécé E (2014) The Revolution in Intelligence Affairs: 1989–2003. International Journal of Intelligence and Counter Intelligence 27(1):27-41

Douhet G (1921) Il dominio dell’aria. C. De Alberti, Roma

Duyvesteyn I, Angstrom J (2004) Rethinking the Nature of War. Routledge, London

Eijkman Q, Van Ginkel B (2011) Compatible or incompatible? Intelligence and human rights in terrorist trials. Amsterdam Law Forum 3(4):3–16

Engelhardt T (2015) The fog of intelligence. http://lobelog.com/the-fog-of-intelligence/ Accessed 23 October 2015

Etling B, Faris R, Palfrey J (2010) Political Change in the Digital Age: The Fragility and Promise of Online Organizing. SAIS Review of International Affairs 30(2):2–10

Farrell Th, Osinga F, Russell JA (2013) (eds) Military adaptation in Afghanistan. Stanford University Press, Stanford

Farrell Th, Terriff T (2002) The sources of military change: culture, politics, technology. Lynne Rienner, Boulder, CO

Ferguson N (2011) Civilization: The West and the Rest. Penguin, New York

Freier N (2007) Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context. Strategic Studies Institute, Carlisle Barracks

F-Secure Labs (2015) The Dukes. 7 years of Russian cyberespionage. F-Secure Labs Threat Intelligence Whitepaper

Fukuyama F (1992) The End of History and the Last Man. Free Press, Glencoe, ILL

Gartmann M, Neef C, Schepp M, Stark H (2014) The Opinion-Makers: How Russia Is Winning the Propaganda War. Der Spiegel 30 May 2014

Gladstone R (2015) Activist links more than 26,000 twitter accounts to ISIS. New York Times, 31 March 2015. http://nytimes.com/2015/04/01/world/middleeast/activist-links-more-than-26000-twitter-accounts-to-isis.html Accessed 27 October 2016

Glaser A (2016) here’s what we know about Russia and the DNC hack. Wired 27 July 2016. https://www.wired.com/2016/07/heres-know-russia-dnc-hack, Accessed 31 August 2016

Hammes TX (2006) The Sling and the Stone: On War in the 21st Century. Zenith, Minneapolis

Hancock L, Wexler S (2014) Shadow Warfare: The History of America’s Undeclared Wars. Counterpoint Press, Berkeley

Hill R (2016) Bulk data collection by intelligence agencies breached human rights law. Public Technology.net 19 October 2016. https://www.publictechnology.net/articles/news/bulk-data-collection-intelligence-agencies-breached-human-rights-law Accessed 23 November 2016

Hippler Th (2013) Bombing the People: Giulio Douhet and the Foundations of Air-Power Strategy, 1884–1939. Cambridge University Press, Cambridge

Hoffman FG (2007) Conflict in the 21st Century: the rise of hybrid wars. The Potomac Institute for Policy Studies, Arlington

House JM (1993) Military Intelligence, 1870–1991. A Research Guide. Greenwood Press, Westport, CN

Howard Ph (2011) opening closed regimes: what was the role of social media during the Arab Spring? http://philhoward.org/opening-closed-regimes-regimes-what-was-the-role-of-social-media-during-the-arab-spring/ Accessed 29 November 2016

Illeris K (2004) Adult education and adult learning. Krieger, Malabar FL

Immerman R (2010) The CIA in Guatemala: the foreign policy of intervention. University of Texas Press, Austin

Ingram Ph (2015) US DoD website hacked by IS. Security News Desk 21 March 2015 http://www.securitynewsdesk.com/us-dod-website-hacked-by-is Accessed 24 September 2015

Kalathil S, Boas TC (2003) Open networks, closed regimes: the impact of the internet on authoritarian rule. Carnegie Endowment, New York

Kaldor M (2012) New & Old Wars: Organized Violence in a Global Era. Stanford University Press, Stanford

Kaplan R (2010) Monsoon: The Indian Ocean and the Future of American Power. Random House, New York

Kingah S, Quiliconi C (eds) (2016) Global and Regional Leadership of BRICS Countries. Springer, New York

Kitzen MWM (2016) The Course of Co-option. Dissertation, University of Amsterdam

Klang M, Murray A (2005) Human rights in the digital age. Glasshouse, London

Kuperwasser Y (2007) Lessons From Israel's Intelligence Reforms. The Brookings Institution, Washington DC

Lander S (2004) International intelligence co-operation: an inside perspective. Cambridge review of international affairs 17(3):481–493

Liddell Hart BH (1971) Why don't we learn from history? Allen Unwin, London

Long NE (1949) Power and Administration. Public Administration Review 9(4):257–264

MacAskill E, Dance G, Cage F, Chen G, Popovich N (2013) NSA files decoded: Edward Snowden's surveillance revelations explained. https://www.theguardian.com/us-news/the-nsa-files Accessed 13 October 2016

Mahdi W (2002) The Internet Factor in Indonesia: Was that All? Paper presented at the 54th Annual Meeting of the Association for Asian Studies, Washington D.C. 4–7 April 2002

Malis C (2012) Unconventional Forms of War. In: Lindley-French J, Boyer Y (eds) The Oxford Handbook of War. Oxford University Press, Oxford, pp 185–198

Manwaring MG, Corr EG (eds) (2008) Insurgency, Terrorism, and Crime: Shadows From the Past and Portents for the Future. University of Oklahoma Press, Oklahoma City

Markoff J (2016) Automated pro-Trump bots overwhelmed pro-Clinton messages, researchers say. New York Times 17 November 2016. http://www.nytimes.com/2016/11/18/technology/automated-pro-trump-bots-overwhelmed-pro-clinton-messages-researchers-say.html?smprod=nytcore-ipad&smid=nytcore-ipad-share&_r=0 Accessed 23 November 2016

Marsick VJ, Watkins KE (2005) Learning organization. In: English LM (ed) International Encyclopedia of Adult Education. Palgrave, London pp 355–360

McCulloh T, Johnson R (2013) Hybrid Warfare, JSOU Report 13-4. Joint Special Operations University, MacDill Air Force Base

Merriam SB, Caffarrella RS, Baumgartner LS (2012) Learning in Adulthood. Jossey-Bass, San Francisco

Metselaar MV (1997) Understanding failures in intelligence estimates – UPROFOR, the Dutch, and the Bosnian-Serb attack on Srebrenica. In: Soeters J, Rovers JH (eds) (1997) The Bosnian Experience. Royal Netherlands Military Academy, Breda, pp. 23–50

Mozur P, Scott M (2016) Fake news in U.S. Election? Elsewhere, that's nothing new. New York Times 17 November 2016. http://www.nytimes.com/2016/11/18/technology/fake-news-on-facebook-in-foreign-elections-thats-not-new.html?smprod=nytcore-ipad&smid=nytcore-ipad-share Accessed 23 November 2016

Murray W, Sennreich R (eds) (2006) The past as prologue. The importance of history to the military profession. Cambridge University Press, Cambridge

Olmsted KS (1996) Challenging the Secret Government: The Post-Watergate Investigations of the CIA and the FBI. University of North Carolina Press, Chapel Hill. New York Times, Intelligence Report on Russian hacking. 6 January 2017. http://www.nytimes.com/interactive/2017/01/06/us/politics/document-russia-hacking-report-intelligence-agencies.html?_r=0 Accessed 9 January 2017

Perrow Ch (1999) Normal Accidents. Living with High-Risk Technologies. Basic Books, New York

Safranek R (2012) The Emerging Role of Social Media in Political and Regime Change. ProQuest Discovery Guide: 2–10

Salih KEO (2013) The Roots and causes of the 2011 Arab Uprisings. Arab Studies Quarterly:185–203. http://www.pinxit.com/page101/page115/downloads-23/files/Arab_Spring_Causes.pdf

Scholte AJ (2000) Globalization: a critical introduction. St. Martin's, New York

Segers RT (2008) (ed) A New Japan for the Twenty-First Century. Taylor & Francis, London

Smith R (2005) The Utility of Force: The Art of War in the Modern World. Allen Lane, London

Soengas X (2013) The Role of the Internet and Social Networks in the Arab Uprisings – An Alternative to Official Press Censorship. Comunicar, 21(41):147–155

Stuenkel O (2015) The BRICs and the Future of Global Order. Lexington Books, Lanham

Thompson PG (2014) Armed Groups: The 21st Century Threat. Rowman and Littlefield, London

Toffler A (1980) The Third Wave. Bantam Books, New York

Treverton GF, Agrell W (2009) National Intelligence Systems: Current Research and Future Prospects. Cambridge University Press, New York

United Nations (2000) Report of the Panel on United Nations Peace Operations

Vanden Berghe Y (2008) De Koude Oorlog. Een nieuwe geschiedenis (1917–1991). ACCO, Leuven and Voorburg

Warrick J and Wright R (2008) U.S. Teams weaken insurgency in Iraq. Washington Post 6 September 2008. http://washingtonpost.com/wp-dyn/content/article/2008/09/05/AR2008090503933.html Accessed 1 October 2016

Author Biographies

Floribert Baudet obtained his Ph.D. from Utrecht University in 2001. He has written extensively on the history of Dutch foreign and defence policy in its broadest sense and on the former Yugoslavia. He has published in *Cold War History,* and in *Air and Space Power Journal—Africa and Francophonie*. Research topics include human rights, strategic communication, covert action, and the use and abuse of the past by (military) establishments. Since 2006 he has been working as an associate professor with the Faculty of Military Sciences of the Netherlands Defence Academy. He has been a member of the Netherlands Intelligence Studies Association since 2014.

Eleni Braat is assistant professor in International History at Utrecht University, The Netherlands. Previously, she served as the official historian of the Dutch General Intelligence and Security Service (AIVD) and lectured at the Institute for History at Leiden University. Her research interests focus on secret government activities, such as intelligence and international diplomacy, and the political tensions they led to in Europe during the 20th century. She obtained her Ph.D. from the European University Institute in Florence, Italy, with a thesis on the disarmament negotiations in the 1920s. She holds an MA with honours in Modern Greek literature from the University of Amsterdam, and a *Diplôme d'études approfondies* (DEA) with the highest distinction in history from the *École des hautes études en sciences sociales* in Paris.

Jeoffrey van Woensel is an MA graduate and reserve first lieutenant of the Regiment Technical Troops (retired), studied history at the Radboud University in Nijmegen. After his studies he was conscripted as ROAG (academically trained reserve officer) in the Royal Netherlands Army. From 2001 to 2015 he worked at the Netherlands Institute for Military History, The Hague. He has published books on a number of topics including chemical warfare, the Explosive Ordnance Disposal Service of the Dutch armed forces, logistics, and the Royal Netherlands Marechaussee. He currently works at the Centre of Research and Expertise of the Veterans Institute on secondment from the Ministry of Defence. Since 2012 he is the Secretary of the Netherlands Intelligence Studies Association.

Aad Wever, a graduate of Utrecht University, taught information security and intelligence at Saxion University of Applied Sciences, Enschede, The Netherlands, and at Ferris State University, Big Rapids, Michigan, USA, until his retirement in June 2016. He has contributed to several publications on the history of the Royal Netherlands Air Force during the Cold War. Since 2004 he has been engaged in educational cruises at Spitsbergen in the Norwegian Arctic. Wever is a member of the Board of the Netherlands Intelligence Studies Association.