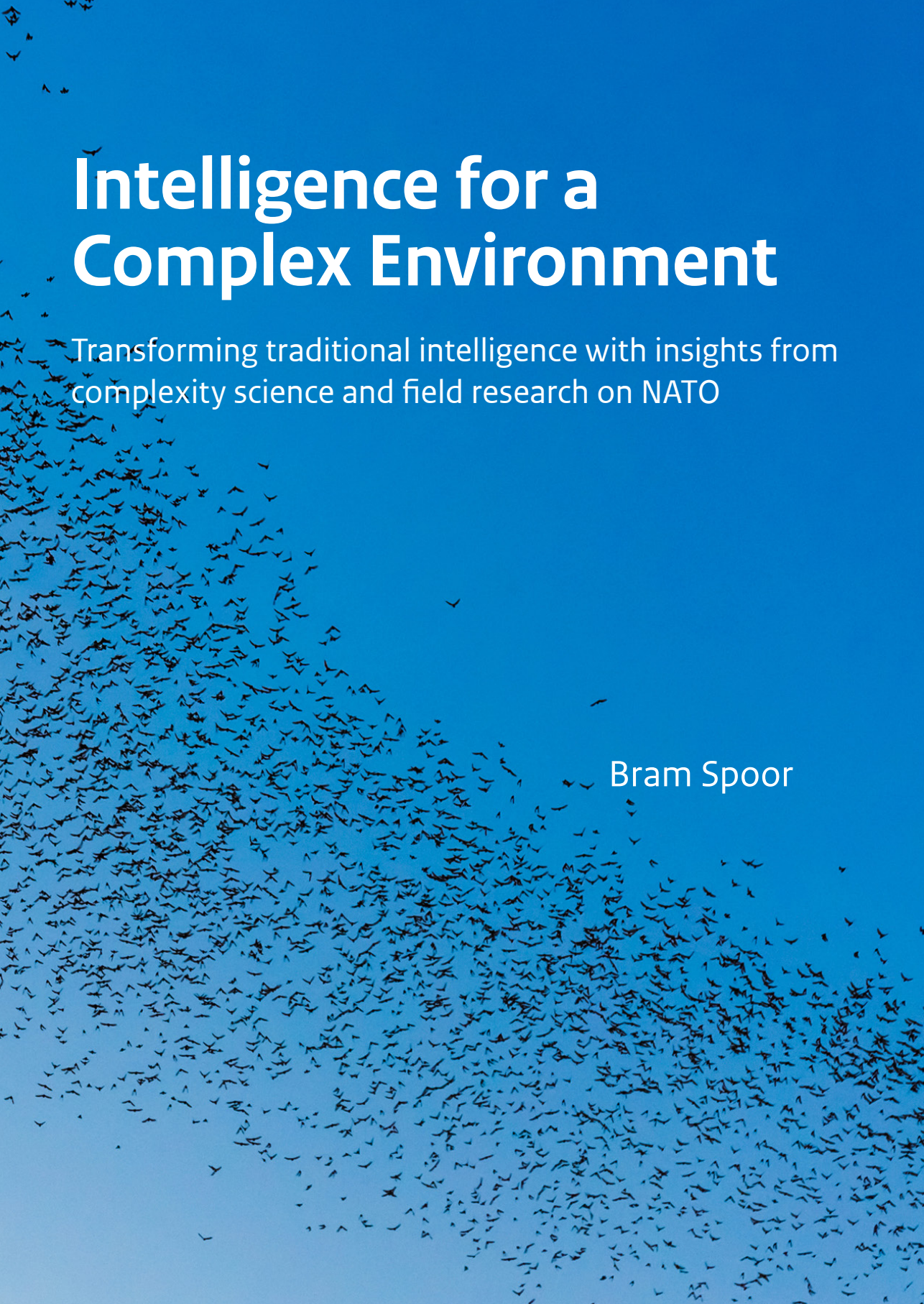
Intelligence for a complex environment: transforming traditional intelligence with insights from complexity science and field research on NATO

Spoor, B.E.P.



Intelligence for a Complex Environment

Transforming traditional intelligence with insights from complexity science and field research on NATO

Bram Spoor

Intelligence for a Complex Environment

Transforming traditional intelligence with insights from complexity science and field research on NATO.

Bram Spoor

Printed by: Repro FBD

ISBN: 9789493124417

Intelligence for a Complex Environment

Transforming traditional intelligence with insights from complexity science and field research on NATO.

Proefschrift

ter verkrijging van de graad van doctor aan de Universiteit Leiden,

op gezag van rector magnificus prof.dr.ir. H. Bijl,

volgens besluit van het college voor promoties

te verdedigen op woensdag 15 januari 2025

klokke 16:00 uur

door

Bram Spoor

Promotor

Prof.dr.ir. S.J.H. Rietjens

Copromotor

Dr. M.G.D. Rothman, Nederlandse Defensie Academie

Promotiecommissie

Prof.dr. K. Caminada (decaan/voorzitter)

Prof.dr. F.P.B Osinga

Prof.dr. P.A.L. Ducheine, Nederlandse Defensie Academie

Prof.dr. P.C van Fenema, Nederlandse Defensie Academie

Dr. C. Hillebrand, Cardiff University

Dr. G.G. de Valk

This dissertation was financially supported by the Royal Netherlands Army and Ministry of Defence. The views and opinions, as well as any faults in this dissertation, are and remain solely the responsibility of the author.

Terzij de Horde

Content

List of figures

List of tables

1. Introduction: Outlining the Research

The international security environment is increasingly complex. An increase in number and type of actors is empowered by fast developing technology and instant worldwide media reach. This is nothing really new. Regardless, intelligence is failing to keep up with these complex security challenges of the 21st century. This research searches a remedy by infusing intelligence with complexity science.

This introduction chapter explains the general outline of this research in four sections. The first section describes how intelligence relates to these security challenges. The second section presents the research aim and what knowledge gaps it addresses. The third section gives the problem statement and accompanying research questions. Lastly, the fourth section presents the research structure with a summary of the chapters and a research model.

1.1 The changing intelligence environment

The Russo-Ukrainian war gives prominent place to intelligence. The invasion of 2022 was preceded by the communication of American and British intelligence services predicting it. While intelligence is traditionally seen as secret, these services disclosed intelligence assessments at an unprecedented scale. In contrast, the German and French intelligence services were caught by surprise when the invasion took place, indicating the complexity of the intelligence task.[1] The war itself shows an unprecedented intensity in intelligence innovation. State intelligence services, private companies, individuals on social media, and think tanks provide daily, up-to-date assessments on territorial gains and losses, casualties and equipment losses, and tactics of the warring parties. Open source intelligence has become mainstream and democratised. The proliferation of drones improves reconnaissance and targeting to the lowest unit level and the Ukrainian government provides an app that its citizens can use to report on Russian military activities.

As such, the Russo-Ukrainian war fits the general realisation within intelligence that the international context and the military operational environment have changed

[1] Michelle Hogendoorn, Bram Spoor, and Sebastiaan Rietjens, "Caught by Surprise: Warning for Russia's Invasion of Ukraine," in *Reflections on the Russia-Ukraine War*, ed. Maarten Rothman, Lonneke Peperkamp, and Sebastiaan Rietjens (Leiden: Leiden University Press, 2024), 41-56.

significantly over the last decades.[2] The bipolar world of the Cold War became a multipolar world with a multitude of actors and alliances that are competing for political, military and economic gain. As a result the world became more interconnected. The acceleration of this process is globalisation: the increased exchange of people, goods, services and ideas across the world. This is intertwined with the Information Revolution, compromising technological developments like the internet, computers and mobile communication.[3]

The cumulative effect of all these drivers causes the decline of the Industrial Age. From a socio-economic system based on the mass production of goods the international order is adjusting to the Information Age; a global system based on the possession and exchange of information. Intelligence, with information traffic at its core, does not adjust well. This shows from the two most formative intelligence failures in the early 2000s; the 9/11 attacks and Iraq's missing weapons of mass destruction. Both failures led to the invasion of a country, Afghanistan and Iraq, that morphed into long and bloody counterinsurgency operations. The ensuing Global War on Terror (GWOT) makes that, despite a variety of drivers of change, intelligence literature identifies the single most important driver as the rise of non-state actors.[4] By definition a manifestation of globalisation, GWOT also meant intelligence became strongly concerned with cross-border insurgencies, international terrorists and organised crime. These non-state actors are often referred to as transnational threats in the literature. They are a very different problem from the relatively static nature of the traditional intelligence focus on states, and are often characterised with terms, or synonyms thereof, as 'adaptive', 'interconnected', 'diverse' and 'complex'.[5] However, the Russian war on Ukraine, and an increasingly assertive

---

[2] Minne Boelens, "The Revolution in Intelligence Affairs: Problem Solved?," in *Perspectives on Military Intelligence from the First World War to Mali: Between Learning and Law*, ed. Floribert Baudet, et al. (The Hague, The Netherlands: T.M.C. Asser Press, 2017), 120.

[3] e.g. Thomas L. Friedman, *The World Is Flat: The Globalized World in the Twenty-First Century* (New York, NY: Farrar, Straus and Giroux, 2005).

[4] William J. Lahneman, *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs* (Lanham, Md.: Scarecrow Press, 2011), 113.

[5] e.g. Warren Fishbein and Gregory F. Treverton, "Making Sense of Transnational Threats," *Sherman Kent Center Occasional Papers* 3, no. 1 (2004); Roger Z. George, "Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm," *Studies in Intelligence* 51, no. 3 (2007); Kristian

China, show state actors still demand the attention of intelligence services. Modern threats come from state and non-state actors, even individuals, alike.[6]

Next to the physical world, these threats operate just as much in the cyber domain and the social world, or 'human environment' in military doctrinal terms. Modern threats use a hybrid strategy, combining military and non-military means. They operate in the grey zone between peace and war, and on a global scale. Information, identity and ideology are weaponised and combined with kinetic force. The highly interconnected world enables these actors, using actions and ideas, to exert much influence fast and on a worldwide scale. The world, driven by all these interconnected developments, is deeply complex and uncertain.[7] The war in Ukraine is but a recent example of this. Today's intelligence issues resemble wicked problems rather than the relatively simple puzzles of the Cold War. However, the organisation of intelligence is still very similar to its Cold War form.

Driven by more recent intelligence failures such as the fall of Kabul or the Hamas attack on Israel in October 2023, the need for intelligence to improve is obvious. How to accomplish this is a more difficult matter. If modern threats, and indeed the whole security environment, are complex, which theories, organisational forms, and processes of intelligence - that have remained largely unchanged since their inception in the former century - are still valid? How to regard intelligence in the twenty-first century? This study asserts that complexity science, the study of complex and adaptive systems, holds many promises for examining the threats in the operational environment as well as intelligence organisations themselves. While this may seem a logical deduction, the study of intelligence has yet to adopt the ideas and methods of complexity science (see Chapter 4). This is striking; There is general agreement on the increased complexity of threats and the security environment in

---

Gustafson, "Complex Threats," *The RUSI Journal* 155, no. 1 (2010); Patrick M. Hughes, "On Convergence, Emergence, and Complexity," *Military Review* 96, no. 2 (2016).

[6] David Omand, "The Future of Intelligence: What Are the Threats, the Challenges and the Opportunities?," in *The Future of Intelligence*, ed. Isabelle Duyvesteyn, Ben De Jong, and Joop Van Reijn (London: Routledge, 2014), 14.

[7] Robert Jervis, *System Effects: Complexity in Political and Social Life* (Princeton, NJ: Princeton University Press, 1997). Emilian Kavalski, ed. *World Politics at the Edge of Chaos: Reflections on Complexity and Global Life* (New York, NY: State University of New York Press, 2015).

general, however the issue is not addressed by taking a complexity turn and adapting intelligence to the changed circumstances. Therefore this study aims to seek insights from complexity science and to apply these to intelligence. The next section will further explain this.

1.2 Research aim & knowledge gaps

Complexity science *'asserts the ontological position that much of the world and most of the social world consists of complex systems'*.[8] Examples of these complex systems include the Internet, financial markets, ecosystems and the human brain.[9] These systems consist of agents that are diverse and connected and that interact and adapt to each other and to their environment.[10] The dynamics between these agents are non-linear. This means the output of these dynamics is disproportionate to the input, whereas in a linear system the output can be predicted or calculated from the input. In other words, the behaviour of a complex system cannot be predicted from studying its constituent agents. This behaviour is not steered by a central controller because the dynamics between the agents are self-organising. As a result complex systems produce completely novel phenomena at system level, referred to as emergence. Each complex system acquires information about its environment and its own interaction with it, identifies regularities in that information which are then recorded into a model, or schema. The system behaviour is based on these schemata and results of its behaviour upon the environment feed back into the models.[11]

The similarities with intelligence are obvious. Like a complex system, intelligence tries to understand the environment and reduce uncertainty in advising decision-making. Therefore a complexity approach to intelligence seems logical and

[8] David Byrne and Gillian Callaghan, *Complexity Theory and the Social Sciences: The State of the Art* (New York, NY: Routledge, 2014), 8.

[9] Murray Gell-Mann, *The Quark and the Jaguar: Adventures in the Simple and the Complex* (New York, NY: Freeman and Company, 1994), 17; James Ladyman and Karoline Wiesner, *What Is a Complex System?* (New Haven, CT: Yale University Press, 2020), 19-63.

[10] Scott E. Page, *Diversity and Complexity* (Princeton, NJ: Princeton University Press, 2011), 25.

[11] Gell-Mann, *The Quark and the Jaguar: Adventures in the Simple and the Complex*, 17.

promising.[12] However, the attention for complexity in intelligence literature is marginal, as Beebe and Beebe state *'relatively little work has been done to date on the potential practical applications of complexity science to the field of intelligence analysis. Complexity rarely receives direct mention in the intelligence literature'*.[13] The volume of publications on the intelligence-complexity nexus is small, and many publications only treat complexity superficially (see section 4.1). Existing literature on the nexus mainly comes from scholars outside the intelligence and security field.[14] Intelligence, it can be stated, missed the complexity turn.[15]

Furthermore, complexity science offers much theory and methods that help to truly move beyond any traditional notions of intelligence. It offers a comprehensive and fundamental perspective where most intelligence studies on improvement have a narrow focus, e.g. technology, intelligence failure, bureaucratic reorganisation. Bay even states there is *'a lack of explicit meta-theoretical awareness'*.[16] De Werd observes: *'Most intelligence scholars refrain from explicitly articulating the theoretical roots of their revolutionary new thinking in philosophical terms'*.[17] This

[12] See also: Committee on a Decadal Survey of Social and Behavioral Sciences for Applications to National Security, "A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis," (Washington, D.C.: National Academies of Sciences, Engineering, Medicine, 2019), 90-92, 117-22; Myriam Dunn Cavelty and Jennifer Giroux, "The Good, the Bad, and the Sometimes Ugly. Complexity as Both Threat and Oppertunity in National Security.," in *World Politics at the Edge of Chaos: Reflections on Complexity and Global Life*, ed. Emilian Kavalski (New York, NY: State University of New York Press, 2015).

[13] Sarah Miller Beebe and George S. Beebe, "Understanding the Non-Linear Event: A Framework for Complex Systems Analysis," *International Journal of Intelligence and Counterintelligence* 25, no. 3 (2012): 510.

[14] Thomas E. Copeland, "Intelligence Failure Theory," in *Oxford Research Encyclopedia of International Studies* (2010).

[15] Bram Spoor and Peter de Werd, "Complexity in Military Intelligence," *International Journal of Intelligence and CounterIntelligence* 36, no. 4 (2023): 1125.

[16] Sebastian Bay, "Intelligence Theories: A Literary Overview," *Lund, Sweden: Lund University* (2009). From; Stephen Marrin, "Evaluating Intelligence Theories: Current State of Play," *Intelligence and National Security* 33, no. 4 (2018): 480.

[17] Peter de Werd, "Critical Intelligence: Analysis by Contrasting Narratives: Identifying and Analyzing the Most Relevant Truths" (PhD, Utrecht University, 2018), 18.

lack of theorising makes that new methods, technological or organisational, are not grounded in broad, underlying highly conceptual frameworks. This can have severe consequences; Liaropoulos warns against relying on organisational and technological reform alone, stating *'Any effort to reform intelligence must adopt a holistic approach'*.[18] Meanwhile, with the development of new methods *'less fully considered are the appropriateness and validity of these methods as well as the underlying assumptions they enshrine'*, according to Moore.[19] With its complexity approach, this research addresses the call for a more multi- and interdisciplinary approach in intelligence studies.[20]

A more comprehensive and theorising perspective would allow for a better understanding of what drives intelligence to change and how this change can look like. Comprehensive and theorising however, does not mean 'unifying'. The goal is not to look for a single theory to explain all of intelligence (theories). The search for a fundamental, metatheoretical framework is about adopting a philosophical stance. The advantage of such a stance is that it can reflect on the structure and workings of the current fragmented theories and methods and balance against it. It can function as a background or foundation in which to see new developments or even generate new thinking. It could form a method to make some sense of the kaleidoscope of developments in intelligence. This would help to improve intelligence in many ways. *'Theorizing about the larger issues and patterns of intelligence can help to inform decisions on future intelligence systems, structures, or functions'*, according to Barger.[21]

---

[18] Andrew Liaropoulos, "A (R)Evolution in Intelligence Affairs? In Search of a New Paradigm," (Athens: Research Institute for European and American Studies, 2006), 17.

[19] David T. Moore, *Sensemaking: A Structure for an Intelligence Revolution* (Washington, DC: National Defense Intelligence College Press, 2011), 4.

[20] Stephen Coulthart, Michael Landon-Murray, and Damien Van Puyvelde, eds., *Researching National Security Intelligence: Multidisciplinary Approaches* (Georgetown University Press, 2019); Stephen Coulthart and Abebe Rorissa, "Growth, Diversification, and Disconnection: An Analysis of 70 Years of Intelligence Scholarship (1950-2020)," *Intelligence and National Security* (2023).

[21] Deborah G. Barger, "Toward a Revolution in Intelligence Affairs," (Santa Monica, CA: RAND Corporation, 2005), 107.

In its aim to improve intelligence with insights from complexity science this research contributes to addressing two more knowledge gaps. Intelligence studies is mainly concerned with intelligence on the level of the state and national intelligence services, often referred to as strategic intelligence or national security intelligence.[22] Intelligence at the level of military operations is researched far less.[23] Military intelligence is not a clearly defined intelligence off-shoot. Contrary, the term is rather ambiguous and often replaced by defence intelligence, combat intelligence or tactical intelligence. This research sees military intelligence as services and units who engage in intelligence as a 'warfighting function' – as termed in doctrine.

This military focus on intelligence is most apparent in the case study of this research. The object of analysis here is the intelligence organisation of NATO's Multinational Corps Northeast (MNC NE). The corps is the NATO tactical command for Poland, Estonia, Latvia, and Lithuania with the mission to *'train for defensive operations, in order to effectively deter any attack and if need be to defend the Alliance's northeastern territory against any aggressor'*.[24]

The data collection at MNC NE took place by means of interviews with 56 (mainly) intelligence officers from nine different corps units and commands, on how they make sense of their operational environment. In addition, numerous informal talks, participant observations, insight in documents, and desk review contributed to this collection effort. As such, next to contributing to knowledge on military intelligence, this case study also contributes to the small volume of contemporary empirically-based research within intelligence studies. And on the corps specifically, only two

[22] Robert Dover, Huw Dylan, and Michael S Goodman, "Introduction to a Research Agenda for Intelligence Studies and Government," *A Research Agenda for Intelligence Studies and Government* (2022): 5.

[23] Loch K. Johnson, "The Development of Intelligence Studies," in *Routledge Companion to Intelligence Studies* (Routledge, 2013), 13. S. Rietjens, "Intelligence in Defence Organizations: A Tour De Force," *Intelligence and National Security* 35, no. 5 (2020): 717; Sebastiaan Rietjens and Peter De Werd, "Intelligence and the Military: Introduction," (Taylor & Francis, 2023); Alessandro Scheffler and Jan-Hendrik Dietrich, "Military Intelligence: Ill-Defined and Understudied," *International Journal of Intelligence and CounterIntelligence* (2023).

[24] Website MNC NE, 'Mission', accessed 10-2-2022. https://mncne.nato.int/about-us/mission

scientific publications exist (see section 5.2.2). The military focus is also applied by using not only academic literature on intelligence but also some military doctrine and publications by military professionals.

Lastly, the case study reveals that the idea of hybrid warfare is especially problematic in making sense of the environment. This is no surprise but rather points to the external validity of the case study as it fits into a larger trend of hybridity in conflicts.

1.3 Problem statement & research questions

This research aims for a theoretical (complexity science) and an empirical (case study research) contribution to the study of intelligence, while highlighting military intelligence. From this, the following problem statement is formulated:

- ***How can complexity science advance intelligence transformation?***

The aim to improve intelligence is phrased here as intelligence transformation. To explain this it is important to distinguish it from the other terms prevalent in the debate that describe the changes (needed) in intelligence: 'reform/reorganisation' and 'revolution'. The first category, reforms/reorganisations, is a common occurrence within intelligence. The US is especially known for this, often done based on investigations into its intelligence community after failures.[25] If this results in actual improved performance is questionable. Hammond states that *'while many prescriptions for Intelligence Community ''reform'' have proved difficult to implement, IC structure seems to have been subjected to reforms and reorganizations somewhat more often, perhaps because structural problems are seen, correctly or not, as more easily solved'*.[26] Reforms and reorganisations are often just about a bureaucratic re-ordering of existing entities and structures. Agrell adds: '*Major reorganizations are in many cases cosmetic, as the staff remain intact or simply get*

[25] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 5 ed. (Washington, DC: CQ Press, 2012), 383-86; Amy B. Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11* (Princeton, N.J.: Princeton University Press, 2007), 27-34.

[26] Thomas H. Hammond, "Intelligence Organizations and the Organization of Intelligence," *The International Journal of Intelligence and Counter Intelligence* 23, no. 4 (2010): 682-83.

recycled in a new organizational chart'.[27] Pillar goes so far as to say that the calls to adjust the US Intelligence Community to the post-Cold War era have become a meaningless cliché: *'the urge to reorganize is largely background noise rather than an effective adaptation to changed circumstances'*.[28]

Reform and reorganisation, with their bureaucratic conditions, are obvious evolutions. Contrary, the second category of approaches to improve intelligence advocates not a gradual but a swift and total overhaul of the system.[29] In the literature authors that advocate a revolutionary approach are a minority.[30] However, their voices are apparently loud enough to have given birth to the term Revolution in Intelligence Affairs (RIA) to distinguish them from the larger volume of works on reform and reorganisation. Overall, the re-examination of intelligence is very fragmented. As Lahneman concludes: *'Studies varied widely in terms of focus and methodology. Since the intelligence enterprise is a very complex undertaking, most of the studies focused on only a portion of it, examining, for example, functional areas, such as […] organization, the analytic process, the policy maker-analyst relationship, open source intelligence (OSINT), covert operations, or the role of information technologies.'*[31]

Intelligence transformation in this study differs from these characterisations. It is not evolutionary reform or reorganisation because it concerns itself with more than slowly re-ordering existing entities and structures. A transformation, according to the online Cambridge Dictionary, is *'a complete change in the appearance or character of something or someone, especially so that that thing or person is improved'*.[32] A transformation is about a fundamental new approach to intelligence,

---

[27] Wilhelm Agrell, "The Next 100 Years?: Reflections on the Future of Intelligence," in *The Future of Intelligence*, ed. Isabelle Duyvesteyn, Ben De Jong, and Joop Van Reijn (London: Routledge, 2014), 139.

[28] Paul R. Pillar, "Adapting Intelligence to Changing Issues," *Handbook of intelligence studies* (2007): 157.

[29] Lahneman, *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs*, 71-72; Lowenthal, *Intelligence: From Secrets to Policy*, 327, 29, 43.

[30] Lahneman, *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs*, 71.

[31] Ibid., 14.

[32] Cambridge English Dictionary online, 'transformation', accessed 22-10-2019.

like a revolution, only it is sceptic to the violent and sudden change connotating such revolution. Unlike with revolution, time – or pace – is not inherently part of the meaning of transformation. Furthermore, this research views intelligence not as moving evenly fast in its entirety. Some aspects, like technological adaptation, develop faster than other aspects such as political oversight. Chapter 3 examines these different aspects of intelligence and their development.

While firmly embracing the novelty of transformation and revolution, this research also acknowledges that understanding of new approaches begins by explaining them with familiar language and concepts. Rejecting the reform/reorganisation approach as inadequate this research focuses on the commonality between revolution and transformation of being about complete systemic change.

Additionally, four research questions are formulated to help guide the research:

1. *What is the status of intelligence transformation?*
2. *How did intelligence evolve?*
3. *How does complexity science relate to intelligence?*
4. *How do military intelligence organisations deal with their complex operational environment?*

The next section further explains the research questions and how they relate to each other.

1.4 Research structure

To answer the central question a research structure is developed, consisting of a summary of the chapters and a research model. The structure is set up according to a cascading model. In this model the chapters build on one another: the conclusions in one chapter are pursued to the next in an incremental manner. This research builds a framework through the accumulation of the theoretical chapters, which is then used for a case study research, and is followed by concluding chapters.

After this introductory first chapter, Chapter 2 explains *What is the status of intelligence transformation?* The intelligence cycle, intelligence theory and intelligence paradigm are presented as the focal points of intelligence transformation. The third chapter will focus on the second research question *How*

did the intelligence habitus evolve? This chapter examines if the transformation issues also exist outside theoretical academic intelligence studies. This broader perspective is explained as the intelligence habitus, borrowing from French philosopher Pierre Bourdieu. To this aim a literature study is done of academic, professional and doctrinal publications to examine how intelligence developed. Hereby a comprehensive approach is needed to avoid the prevalent fragmentation and narrow scope of the transformation debate. To accomplish this, the framework of the five driving forces from *The Evolution of International Security Studies* (2009) by Barry Buzan and Lene Hansen is used; *Great Power Politics, Technology, Events, Academic Debate* and *Institutionalisation.* The framework, and what is understood by 'intelligence habitus' is explained in detail in Chapter 3. This provides a thorough overview of the evolution of the intelligence habitus.

To answer the third question *How does complexity science relate to intelligence?* Chapter 4 starts with a literature study of existing notions of complexity within intelligence literature and then connects these to complexity science. As a parallel, publications on warfare and complexity and organisational complexity theory are surveyed to help connecting complexity to intelligence. The specific research approach for the case study is discussed in Chapter 5. Chapters 6, 7 and 8 form the empirical part of the research. The corresponding research question is *How do military intelligence organisations deal with their complex operational environment?* The case study research is based on interviews with personnel from MNC NE, as well as informal talks, participant observations, insight in documents, and desk review. The last chapter answers the problem statement *How can complexity theory advance intelligence transformation?* By formulating recommendations to improve intelligence performance in complex environments. Finally, Chapter 9 reflects upon this research and recommendations for further research are formulated.

Figure 1 depicts the research model for this study. The white boxes represent the sources the research is based on, blue boxes represent chapters and are followed by the corresponding research questions.

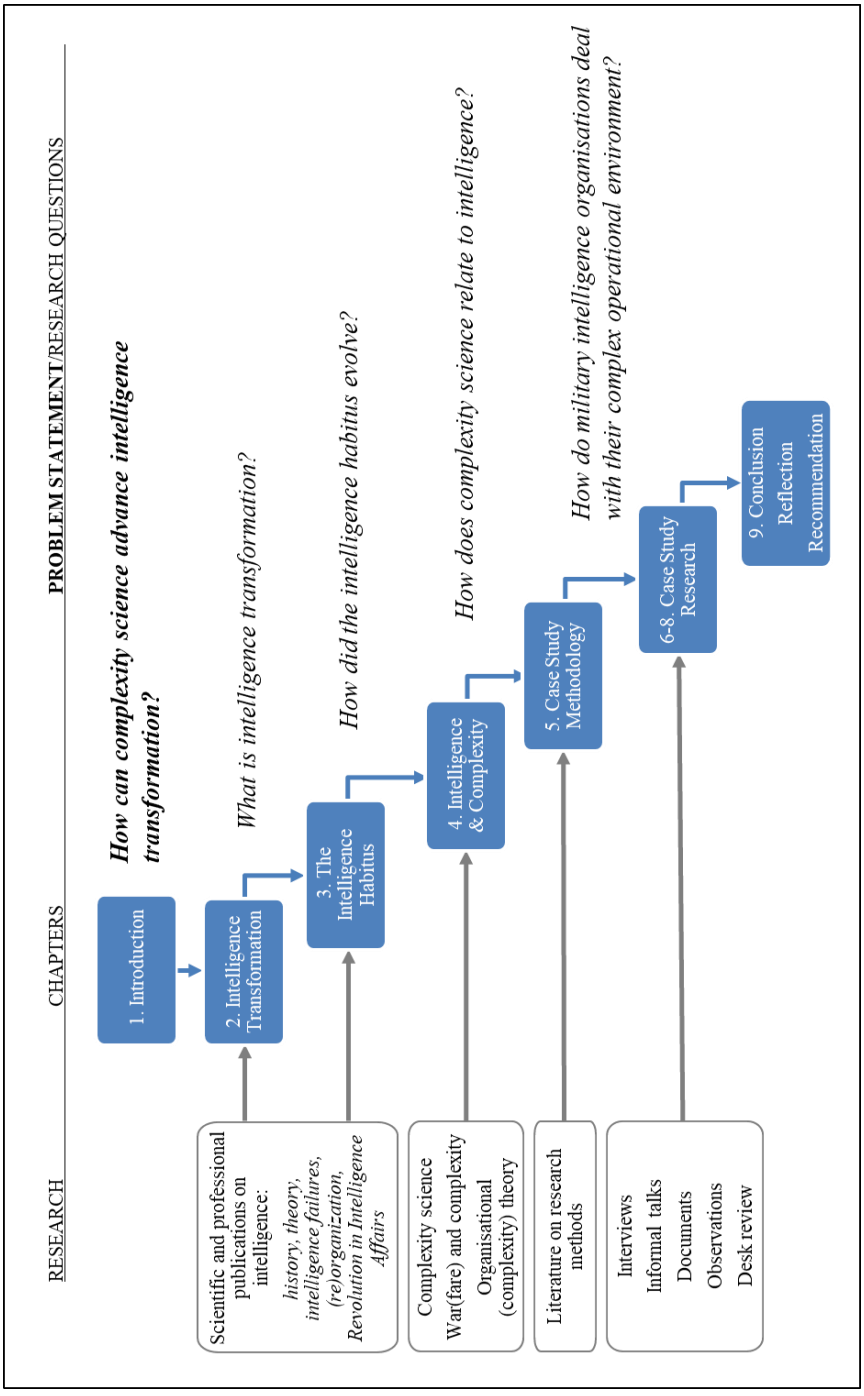


Figure 1: Research model

2. Intelligence Transformation

The first chapter briefly described the challenges for intelligence in moving from the Cold War to the present. This chapter examines the reaction of intelligence on these changes, and answers the research question *What is the status of intelligence transformation?*[33]

To establish a proper depth of research for a transformation this study identifies three fundamental shifts, in varying volume, within the study of intelligence; critique on the intelligence cycle, the development of (new) theory, and a paradigm debate. They form, what I name, a 'trinity of transformation' of issues that are not entirely separate, nor are they exactly the same. The intelligence cycle, being well established, can be regarded as the methodology of intelligence theory. It is *'part of the conceptual language used in developing theoretical approaches to intelligence'*.[34] This can have negative consequences because it *'influences and probably limits discussions'* on intelligence in general.[35] In its turn, intelligence theory relates to the epistemological and ontological assumptions of the field; it shows what is considered knowledge and how it is obtained. The paradigm debate enables to speak of intelligence transformation in a more holistic way. Intelligence theory and the intelligence cycle are key characteristics of the intelligence paradigm but are not equal to it. The idea of a paradigm includes the former two topics and builds on them. In a sense the three topics are communicating vessels where they all contribute to each other's meaning and understanding. As such these topics lie at the very heart of (the organisation of) intelligence and, furthermore, are often discussed in complexity related terminology. Together these topics have a strong potential to fundamentally transform intelligence.

This chapter consists of five sections. The first section explains what intelligence is, as a background to the trinity topics that are examined in the following three

---

[33] Parts of this chapter have been published in Bram Spoor and Maarten Rothman, "On the Critical Utility of Complexity Theory in Intelligence Studies," *Intelligence & National Security* 36, no. 4 (2021).

[34] Peter Gill, "Theories of Intelligence," in *The Oxford Handbook of National Security Intelligence*, ed. Loch K. Johnson (New York, NY: Oxford University Press, 2010), 48.

[35] Wilhelm Agrell, "Intelligence Analysis after the Cold War," in *National Intelligence Systems: Current Research and Future Prospects*, ed. Gregory F. Treverton and Wilhelm Agrell (New York, NY: Cambridge University Press, 2009), 107.

sections. The fifth, last, section concludes by presenting the status of transformation within intelligence.

2.1 Introducing intelligence

When discussing the history of intelligence many publications invoke Sun Tzu, Machiavelli, and Clausewitz. Often the same publications put this in perspective by pointing out intelligence is a fairly new term. Historical sources often speak of information on adversaries, secretly sought and kept by kings and generals. It was gained via informants or intercepting letters. Espionage as we now call it. The term intelligence is commonly used to refer to espionage having become a bureaucratic state-activity since the late 19th or early 20th century.[36] In a military sense the First World War saw reconnaissance become intelligence with large scale collection of information on enemy forces by radio intercepts, by reconnaissance airplanes, and from prisoners of war. To be effective, all this information had to be studied and sent to higher commands to aid decision making. Standards for doing so turned into intelligence doctrine being imposed on all levels and formations.[37] The further professionalisation and canonisation of intelligence also entail efforts to define it.

Intelligence is hard to define. There is an abundance of partly overlapping definitions but little agreement among them. The search for a universal definition of intelligence is a common and much problematised topic.[38] Most publications thus begin with their own version of a definition. Exemplary for the difficulty of defining intelligence, the first edition (2006) of *Intelligence in an Unsecure World* by authors Gill and Phythian has a different definition than the second and third editions (2012, 2018).

---

[36] Michael Herman, *Intelligence Power in Peace and War* (Cambridge: Cambridge University Press, 1996), 9; Michael Warner, *The Rise and Fall of Intelligence: An International Security History* (Washington: Georgetown University Press, 2014), 34-35.

[37] *The Rise and Fall of Intelligence: An International Security History*, 51.

[38] For articles solely on the issue of definition see: Alan Breakspear, "A New Definition of Intelligence," *Intelligence & National Security* 28, no. 5 (2013); Thomas F. Troy, "The "Correct" Definition of Intelligence," *International Journal of Intelligence and CounterIntelligence* 5, no. 4 (1991); Michael Warner, "Wanted: A Definition of Intelligence," *Studies in Intelligence* 46, no. 3 (2002); K. J. Wheaton and M. T. Beerbower, "Towards a New Definition of Intelligence," *Stanford law & policy review.* 17, no. 2 (2006).

This overall patchwork of intelligence definitions, all of which are partly true but not untrue, relates to postmodern ideas on relative truths and the end of metanarratives that argue that the search for a universal definition is beyond the point. While acknowledging this, for scientific clarity and as a way of being self-reflective and explicit about one's approach of a subject, a definition is provided later on in this section.

Intelligence is not unique in its problematic search for a single definition. Other phenomena such as terrorism or climate change share this faith. Still, the pluriform nature of intelligence does not help. In 1946 Kent, intelligence analysis pioneer and Yale university scholar, described intelligence as meaning both a process and the product of that process.[39] Three years later, in his seminal *Strategic intelligence for American world policy* (1949) Kent formulated intelligence as being knowledge, organisation and activity.[40] These two sets of partly overlapping observations on the forms of intelligence are widely incorporated in the definition debate. As apparent from the title of his book Kent was defining strategic intelligence and not intelligence as such. To further complicate the matter other adjectives next to strategic and military are e.g. national security (consisting of defence, foreign policy and internal/external state security), corporate, or peacekeeping. These denominations of intelligence often overlap in meaning but are not exactly the same.

There is also a degree of cultural pluriformity that confuses the issue of what intelligence is. Nations have different intelligence systems, even longstanding allies such as the United States and Great Britain. In the American context, collected information becomes intelligence only after analysis. The British call collected information (raw) intelligence. After analysis it is called (finished) intelligence.[41] The difference is that *'the United States approaches information as a specific component of intelligence, while Britain approaches intelligence as a specific type of information'*.[42]

---

[39] Sherman Kent, "Prospects for the National Intelligence Service," *The Yale review* 36 (1946).

[40] *Strategic Intelligence for American World Policy* (Princeton, N.J.: Princeton University Press, 1949).

[41] Philip H. J. Davies, "Ideas of Intelligence," *Harvard International Review* 24, no. 3 (2002): 62-64; Bob de Graaff, *Data En Dreiging: Stap in De Wereld Van Intelligence* (Amsterdam: Boom, 2019), 24.

[42] Davies, "Ideas of Intelligence," 64.

Given all these facets of intelligence many definitions tend to describe what intelligence does rather than define it.[43] Perhaps this stems from the military origins of intelligence and the duality of both doctrine, as canonised military practice, and theoretical academic attempts at a definition. Then again, the urge to describe an ambiguous term as intelligence by its demeanour rather than its nature is commonly understandable. When describing what intelligence does, instead of what it is, almost all definitions use the intelligence cycle to some degree. This model breaks intelligence down into four steps in a cycle. The first step provides the intelligence direction, or task. The second step involves collecting relevant information with the third step enriching this information into intelligence. The fourth step is disseminating the finished intelligence product to the source of the direction (see also section 2.2). Another common notion is that intelligence is to inform decision-making. It is to provide a military commander, government policymakers, or a corporate CEO with decision advantage. In striving for more definitional content the literature often focuses, and disagrees, on e.g. the role of secrecy, if to include counterintelligence and covert action, whether intelligence is for states or also for non-state actors, if intelligence is only about threats or opportunities as well, and if the separation between domestic and foreign intelligence is still valid.

Kent's terminology and the intelligence cycle generally form the building blocks of intelligence definitions. This is not surprising, regarding the fact that it is an easily understandable language to explain a very difficult process. When formulating a definition of intelligence, for purpose of clarity, this research uses the product/process duality and the intelligence cycle (direction, collection, processing, dissemination). To accommodate for the complexity approach to intelligence announced in the introduction of this chapter, a broad definition is sought. Therefore the definition has to contain many of the topics of debate. It must not be limited to states, must include threats as well as opportunities and make no distinction between domestic and foreign because this conflicts with transnational character of non-state threats. Counterintelligence is seen as inherently part of intelligence because of the need to protect sources and methods. Covert action is regarded as a consequence of intelligence and not as intelligence as such. Both terms are therefore not required in a definition. Secrecy is also not included as a pre-requisite for a definition. To some extent secrecy, like counterintelligence, is needed to protect

[43] Claudia Hillebrand and R. Gerald Hughes, "The Quest for a Theory of Intelligence," in *The Palgrave Handbook of Security, Risk and Intelligence*, ed. Robert Dover, Huw Dylan, and Michael S. Goodman (London: Palgrave Macmillan, 2017), 5.

sources and methods but it is not the main characteristic in a time wherein intelligence services, riding on the attention for terrorism and recent intelligence failures, are taking – or forced to take – a more public role as well. Secrecy is also relative because of the data explosion on the open information domain. This, among other developments such as drones, allows non-state actors, unable to organise for costly SIGINT, to employ their own intelligence activities based on open sources.[44] In line with the military focus in this study, the research begins with the NATO definition of intelligence: *'The product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers.'*[45]

The definition begins very narrow. Intelligence is mainly defined as a product. Process is only implied by naming the first three steps of the intelligence cycle. Dissemination is not mentioned, wrongly excluding the communication of intelligence from being part of intelligence itself. The definition then becomes more broad. It explicitly refers to the information-based nature of intelligence, yet there is no mention of secrecy. It does have a classic approach of assessing capabilities and intentions yet everything else is described in neutral and general terms. It is 'environment' and not 'battlefield', 'decision-makers' instead of only 'commander', and the addition of the term 'actor' makes it applicable to both state and non-state/ transnational threats. The aim is to identify both threats and opportunities. Overall, the NATO definition is quite broad, with the omission of two important features. It does not explicitly refer to intelligence as being a process as well as a product. In second instance it does not mention the dissemination step of the intelligence cycle. Therefore a slightly altered version of the NATO definition is used whereby intelligence is: *The product and process of directed collection and processing of information regarding the environment and the capabilities and intentions of actors, and resulting dissemination in order to identify threats and offer opportunities for exploitation by decision-makers.* This definition serves as the background to the trinity of transformation. These three topics are examined next.

[44] Warner, *The Rise and Fall of Intelligence: An International Security History*, 308.

[45] NATO, terminology database, 'intelligence' (record 17638), nso.nato.int/natoterm,

2.2 The intelligence cycle

The universal model of the intelligence cycle forms the structure of intelligence; how it performs its knowledge production. It is a cyclical, step-by-step, scheme of four functions of intelligence: direction, collection, processing and dissemination. Figure 2 shows the generic intelligence cycle, as used in the doctrine of NATO and many of its member states.

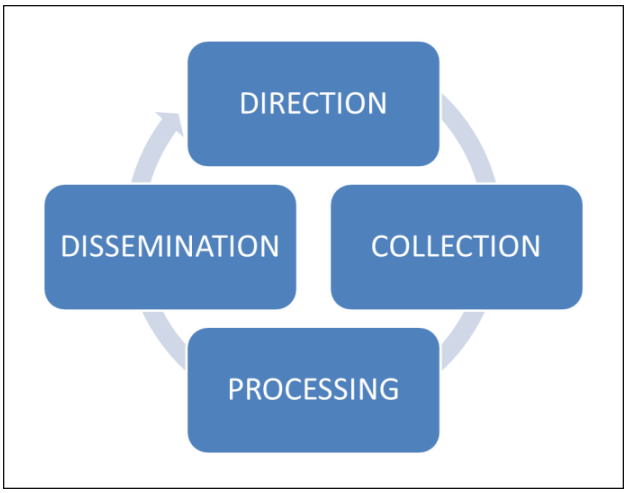


Figure 2: Generic intelligence cycle

In the first step of the cycle a decisionmaker (military commander or policy official) provides a question or problem that needs to be answered. This is translated into intelligence requirements that are pursued in the collection step. Collection is done by several disciplines:

- Retrieving intelligence from cultivated human sources (human intelligence, HUMINT).
- Interception of (non-)communication transmissions (signals intelligence, SIGINT).
- Measurement of technical data of transmissions in order to identify the source (measurement and signature intelligence, MASINT).
- Analysis of imagery from satellites, aerial platforms, or otherwise obtained (imagery intelligence, IMINT).

- Information gathering from publicly available sources (open source intelligence, OSINT).
- Intelligence derived from sound signal or emissions (acoustic intelligence, ACINT).

These collection disciplines are known as the 'INTs', named after their abbreviation and form the generic set of instruments for intelligence. The third step of the intelligence cycle processes the information to intelligence which is then disseminated (e.g. report, briefing) to the decisionmaker.

The four steps form a closed loop; a process with no apparent end since direction follows dissemination, starting a new cycle. The cycle is didactically strong. It enables a quick and simple explanation of intelligence to a complete novice. As a result, the cycle is not only central in formulating intelligence definitions but also in intelligence education, intelligence failure research and the broader study of intelligence. The intelligence process, according to the cycle, where each specialist works on a part of the whole is sometimes referred to as the intelligence factory for its resemblance with a factory with specialist assembly lines. Furthermore, the cycle forms the language of intelligence, in this research as well.

The intelligence cycle is not without its critics. Since the mid-2000s a growing body of literature points to flaws in the model.[46] In essence the critique states that the model is an oversimplification to the point that it is no longer usable. Another topic is the origin of the intelligence cycle. The (related) terms to describe the individual steps of the cycle exist since before the First World War. The graphical invocation of the cycle came into use in US intelligence teaching during the Second World War. The first textbook containing the cycle is attributed to Glass and Davidson in their book *Intelligence is for Commanders* (1948).[47] Around the same time Sherman Kent

[46] e.g. Arthur S. Hulnick, "What's Wrong with the Intelligence Cycle," *Intelligence and National Security* 21, no. 6 (2006); Mark Phythian, ed. *Understanding the Intelligence Cycle*, Studies in Intelligence (Milton Park, Abingdon, Oxon: Routledge, 2013).

[47] Robert Rigby Glass and Phillip B. Davidson, *Intelligence Is for Commanders* (Harrisburg, PA: Military Service Publishing Company, 1948); from: David Omand, "The Cycle of Intelligence," in *Routledge Companion to Intelligence Studies*, ed. Robert Dover, Michael S. Goodman, and Claudia Hillebrand (Abingdon, Oxfordshire: Routledge, 2015), 62.

and his colleagues at the newly formed CIA adopted the cycle as a teaching tool. Kent separated analysis from the processing stage to emphasise its importance. American intelligence uses this five step variant until the present day. With the establishment of NATO the intelligence cycle was embraced to create a uniform understanding for interoperability within the alliance.[48] Initially the cycle was created for intelligence for combat operations, but the increasing complexity of warfare has put pressure on the cycle.[49] Furthermore, besides combat or warfare it now covers all forms of intelligence also concerning (multi)national and complex strategic issues.[50]

Its origin from military doctrine still influences how the intelligence cycle is regarded. Doctrine can be divided into two levels: practical handbooks and manuals providing standard operating procedures for in the field, and higher doctrine to communicate more abstract frameworks and concepts on thinking about war. Davies, Gustafson, and Rigden also applied this division to the debate on the cycle and identify two main camps; proceduralists and conceptualists. Proceduralists see the cycle as prescriptive for intelligence work and the structure of organisations where this work is done. Conceptualist see the cycle as a more abstract idea on which standardised processes are based instead of it being the standard itself. Comment on the intelligence cycle comes from both camps, though conceptualist are generally less dissatisfied.[51] Several authors came up with alternative models to address the cycle's deficiencies. However, the aim here though is not to discuss in depth all the alternative models of the intelligence cycle but give primacy to focus on its overall shortcomings.

The main topic of critique is the cyclical and sequential appearance of the cycle. In reality, the order of the steps is not always as depicted by the model. For example; analysts are often involved with the translation of intelligence requirements to collection tasks to guide collectors and sensors to the most valuable or sought after pieces of information. These missing pieces stem from a process of analysing and dissecting intelligence problems and relating this to the body of knowledge on the

[48] "The Cycle of Intelligence," 61-63.

[49] Geraint Evans, "Rethinking Military Intelligence Failure – Putting the Wheels Back on the Intelligence Cycle," *Defence Studies* 9, no. 1 (2009): 22.

[50] Agrell, "Intelligence Analysis after the Cold War," 108.

[51] Philip H. J. Davies, Kristian Gustafson, and Ian Rigden, "The Intelligence Cycle Is Dead, Long Live the Intelligence Cycle: Rethinking Intelligence Fundamentals for a New Intelligence Doctrine," in *Understanding the Intelligence Cycle*, ed. Mark Phythian (Milton Park, Abingdon, Oxon: Routledge, 2013), 60-61.

subjects already present in reports and databases. This means that in practice, processing takes place first, and the order of the steps is reversed.

Another example is that sometimes not all of the steps are followed. The sub-process within the collection step, termed ISR cycle (intelligence, surveillance, reconnaissance) in doctrine, sees collected information and intelligence being disseminated before reaching the processing step. This can happen in combat situations where life-and-death decisions demand fast information. Another often heard comment is the intelligence cycle has many internal feedback loops that are not depicted. It should represent the inter-relationship between the stages instead of the linear representation of the cycle. *'In practical terms, direction, collection, processing and dissemination continuously communicated back and forth and across the "cycle" more like subroutines calling one another in computer software than the prevailing metaphor of an electromechanical feedback system.'*[52] Hulnick sees the cycle as a *'matrix of interconnections'* and Omand as an *'interactive network'*.[53]

To address this interactivity, NATO doctrine introduced Intelligence Requirement Management and Collection Management (IRM&CM). This add-on process oversees the intelligence cycle to address and guide the internal feedback loops of the cycle to improve efficiency.[54] However, the IRM&CM process is largely missing in academic literature about the intelligence cycle. Expanding on this interactivity, two alternatives to the cycle are interesting. Gill and Phythian argue the cycle is a closed system while an open system is needed because direction is not the only driving factor. They propose a web to replace the idea of a cycle because *'this better reflects the complexity that characterises intelligence, its non-linear form, the centrality of*

[52] Ibid., 64.

[53] Arthur S. Hulnick, "Controlling Intelligence Estimates," in *Controlling Intelligence*, ed. Glenn Hastedt (London: Frank Cass, 1991), 91; See also: "The Future of the Intelligence Process: The End of the Intelligence Cycle," in *The Future of Intelligence: Challenges in the 21st Century*, ed. Isabelle Duyvesteyn, Ben de Jong, and Joop van Reijn (New York, NY: Routledge, 2014); David Omand, *Securing the State* (London: C. Hurst & Co, 2010), 119.

[54] IRM&CM: *'A set of integrated processes and services to manage and satisfy the intelligence requirements by making best use of the available collection, processing, exploitation and dissemination capabilities.'* NATO, terminology database, 'IRM&CM' (record 40708), nso.nato.int/natoterm.

environmental factors in its production, and its impact on its own environment'.[55] Similarly, Clark uses complexity terms to describe his target-centric approach as alternative. He states most intelligence targets are complex systems, or networks, that evolve and are dynamic and non-linear. Instead of following the linear cycle with separate steps intelligence should form network of collector-analyst-customer around a shared target to collaborate in making sense of the problem at hand.[56]

The intelligence cycle does not accommodate for several other phenomena. Omand points to the *'cumulative value of assessed intelligence in providing situational awareness, understanding and prediction, representing more than the impact of individual intelligence reports that may well be fragmentary and incomplete as read by the customer'*.[57] The omission of counterintelligence and covert operations from the cycle are also frequently commented on. The literature mostly sees flaws, or anomalies, in the intelligence cycle as malfunction of system components (the cycle stages) or variables like unclear questions, availability of information/sensors or absence of correcting feedback loops. The reaction of adjusting and refining the intelligence cycle is trying to adapt the old model to new facts. Though this is important for professional self-reflection and historical case studies they might block the perspective that the system as a whole is becoming obsolete. [58]

In conclusion, the main point is the cycle, being a standardisation model *'assumes the process works the same way for all objectives, regardless of complexity and cognitive demands'*.[59] There is for instance a big difference between answering directed questions, even when vaguely formulated, and the activities of forecasting or horizon scanning. Hereby emerging high-impact risks and threats outside the main scope are hoped to be identified as signals among the noise, before they manifest

---

[55] Peter Gill and Mark Phythian, "From Intelligence Cycle to Web of Intelligence: Complexity and the Conceptualisation of Intelligence," in *Understanding the Intelligence Cycle* (Routledge, 2013), 24, 38.

[56] Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach*, 5 ed. (Los Angeles, CA: Sage, 2016), 30-45.

[57] Omand, "The Cycle of Intelligence," 66.

[58] Agrell, "Intelligence Analysis after the Cold War," 108.

[59] Judith Meister Johnston and Rob Johnston, "Testing the Intelligence Cycle through Systems Modeling and Simulation," in *Analytic Culture in the US Intelligence Community: An Ethnographic Study* (Washington, DC: Center for the Study of Intelligence, CIA, 2005), 50.

themselves fully.[60] This begs the question where, and if, there is a capability to adjust approaches to different problems located in the cycle. To examine this the intelligence cycle is seen as a cybernetic feedback loop: *'A feedback loop is a circular arrangement of causally connected elements, in which an initial cause propagates around the links of the loop, so that each element has an effect on the next, until the last "feeds back" the effect into the first element of the cycle. The consequence of this arrangement is that the first link ("input") is affected by the last ("output"), which results in self-regulation of the entire system, as the initial effect is modified each time it travels around the cycle.'*[61]

Herman applies this to the intelligence cycle: *'The cycle is a metaphor of a cybernetic system, in which a control unit 'senses' feedback and is programmed to make constant small adjustments of output, 'hunting' for the maximum desired feedback semi-automatically, without high-level decisions. […] In the metaphor of the conventional military cycle the users are the control unit, constantly adapting their stated needs to optimize their intelligence inputs.'*[62] Davies, Gustafson, Rigden judge this a *'very apt expression of the conceptual approach to the intelligence cycle'*.[63] So where collection and analysis are the knowledge creation in the intelligence cycle, the dissemination of intelligence to the initiating direction step starts the cybernetic feedback. This feedback adjusts the intelligence requirements of the originator, or controller, leading to new requirements and starting the process over. This is where the only adjustment takes place, with a new direction by policy and decision makers – it lies outside intelligence. While this is in line with intelligence being subjected to policy, it excludes any flexibility in the rest of the cycle. Whatever the intelligence

[60] For more on the difference between requirements and horizon scanning, see: Mark M. Lowenthal, *The Future of Intelligence* (Cambridge: Polity Press, 2018), 2-3; David Omand, "Is It Time to Move Beyond the Intelligence Cycle? A Uk Practitioner Perspective," in *Understanding the Intelligence Cycle*, ed. Mark Phythian (Milton Park, Abingdon, Oxon: Routledge, 2013), 143; Julian Richards, "Pedalling Hard: Further Questions About the Intelligence Cycle in the Contemporary Era," ibid., 53.

[61] Fritjof Capra, *The Web of Life: A New Synthesis of Mind and Matter* (London: Flamingo, 1997), 56.

[62] Herman, *Intelligence Power in Peace and War*, 293.

[63] Davies, Gustafson, and Rigden, "The Intelligence Cycle Is Dead, Long Live the Intelligence Cycle: Rethinking Intelligence Fundamentals for a New Intelligence Doctrine," 61.

problem is, from tactical combat to strategic complexities, the cycle will always be the cycle; there is no adaptation to the issue at hand.

This cybernetic focus on control through feedback is mirrored in the prevalence of the topic of producer-consumer relations in much of the intelligence literature. Cybernetics examine the system's behaviour rather than the system itself. It is about what a system does, not what it is. More so, it is not about any given, particular act of a system but about the total of possible actions.[64] In this sense, much of the critique on the intelligence cycle, such as internal feedback loops that are not depicted or malfunctions in the individual steps, still stays within the cybernetic frame. While the intelligence cycle has remained basically the same for over 70 years cybernetic ideas on control and organisation have evolved in other fields that offer a broader range of thinking about systems and their problem-solving capabilities (see section 4.2.2). For failing to accommodate the complexity of intelligence Agrell judges the intelligence cycle harshly: *'Of all the weaknesses of the Cold War intelligence paradigm, the hegemony of the intelligence-cycle model is probably the single most important factor in producing an intellectually inadequate concept of intelligence. While the "normal intelligence" supplied the communities with huge blinders, the adherence to the cycle tended to reduce intellectual creativity to information compilations, schematic interpretations, and unimaginative guesswork. With all its developed steering and guidance procedures, the cycle had the devastating consequence of blocking any development in the direction of "revolutionary intelligence" from within the system itself.'*[65]

Revolutionary developments in intelligence, unhindered by the intelligence cycle frame, should be visible in intelligence theorising. This second part of the trinity of transformation is examined in the next section.

2.3 Theories of intelligence

Where the intelligence cycle is a sort of universal methodology; a micro, practical, technical-like process, theory is about the epistemology (how knowledge is produced) and ontology (what is knowledge) of intelligence. While the structure of this research provides an examination of intelligence definitions at the beginning of

[64] W. Ross Ashby, *An Introduction to Cybernetics*, 4 ed. (London: Chapman & Hall Ltd, 1961), 1-3.

[65] Agrell, "Intelligence Analysis after the Cold War," 109.

this chapter, this separation is artificial because definition is part of theory. However, definitions are *'static representations of the more dynamic and foundational conceptual representation of intelligence that can be found in intelligence theories'*.[66] A definition is a snap shot of a vast, ongoing process of feedbacks like a computer network. The fluidity and interconnectedness of this process cannot correctly be understood from its structure.[67] That is where the critique on the intelligence cycle originates; it does not represent the actual feedbacks within the cycle. So good theory should at least capture or provide for the enormous potential of all interconnections between intelligence aspects and with their environment. Still, theorising and conceptualising about intelligence is often considered less interesting and exciting than other topics of research. However, there is already enough literature that *'does nothing but describe the real or imagined 'facts' of intelligence successes and scandals' and therefore only 'adds up to a highly coloured and distorted view of intelligence'*.[68] A more normative approach, instead of descriptive, can help to understand and advance the study of intelligence. Theory and concepts have an *'indispensable role in generating and organizing knowledge'*.[69]

Again, as with the intelligence definitions, this section on intelligence theories will not focus on individual examples in comparison, but rather describe the broad ranges of theory. Individual theories are only used as arguments to form the foundation of statements or as examples. Intelligence theorising has two main characteristics in literature. Firstly, many publications deal with the relation of intelligence studies to the field of international relations, often framing intelligence as its 'missing dimension'.[70] Because of this relation to international relations, intelligence scholars use its theories to examine intelligence. In a general sense this

---

[66] Marrin, "Evaluating Intelligence Theories: Current State of Play," 481.

[67] Johnston and Johnston, "Testing the Intelligence Cycle through Systems Modeling and Simulation," 37.

[68] Peter Gill and Mark Phythian, *Intelligence in an Insecure World*, 3 ed. (Cambridge, UK Polity Press, 2018), 27.

[69] Ibid.

[70] Christopher Andrew and David Dilks, *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century* (London: Macmillan 1984); James Der Derian, *Antidiplomacy: Spies, Terror, Speed, and War* (Cambridge, MA: Blackwell, 1992); Michael G. Fry and Miles Hochstein, "Epistemic Communities: Intelligence Studies and International Relations," *Intelligence and National Security* 8, no. 3 (1993).

is true but it can be argued that intelligence's preoccupation with the War on Terror, with much written on 9/11, the invasion of Afghanistan and Iraqi WMDs, failed to connect it to mainstream debates with international relations.[71] In any case, the relation between intelligence and international relations is very much unidirectional as intelligence is pretty absent in international relations theory.[72] Very few mainstream scholars of history or political science incorporate intelligence literature into their work.[73]

The second characteristic of intelligence theorising is the status of being under-theorised, meaning there are few attempts to theorise, or existing theory is not rich enough.[74] Compounding this is that, aside from international relations, intelligence studies remains relatively isolated from knowledge in other domains and fields.[75]

---

[71] Richard J. Aldrich, "Beyond the Vigilant State: Globalisation and Intelligence," *Review of International Studies* 35, no. 4 (2009): 890.

[72] Christopher Andrew, "Intelligence, International Relations and 'under-Theorisation'," *Intelligence and National Security* 19, no. 2 (2004); Len Scott and Peter Jackson, "The Study of Intelligence in Theory and Practice," *Intelligence & National Security* 19, no. 2 (2004): 147.

[73] Johnson, "The Development of Intelligence Studies," 8; Stephen Marrin, "Improving Intelligence Studies as an Academic Discipline," *Intelligence and National Security* 31, no. 2 (2016): 278.

[74] Barger, "Toward a Revolution in Intelligence Affairs," 107; Walter Laqueur, *World of Secrets: The Uses and Limits of Intelligence* (London: Weidenfeld and Nicolson, 1985), 8; Kira Vrist Rønn and Simon Høffding, "The Epistemic Status of Intelligence: An Epistemological Contribution to the Understanding of Intelligence," *Intelligence & National Security* 28, no. 5 (2013): 697; Jennifer Sims, "The Theory and Philosophy of Intelligence," in *Routledge Companion to Intelligence Studies*, ed. Robert Dover, Michael S. Goodman, and Claudia Hillebrand (Routledge, 2015), 42.

[75] Stephen Coulthart, Michael Landon-Murray, and Damien Van Puyvelde, "Introduction: A Pluralistic Approach to Intelligence Sholarship," in *Researching National Security Intelligence: Multidisciplinary Approaches*, ed. Stephen Coulthart, Michael Landon-Murray, and Damien Van Puyvelde (Washington, D.C.: Georgetown University Press, 2019), 3.

However, a general weak theoretical base of intelligence studies is countered by both Lillbacka and Marrin who see a growth in theorising attempts.[76]

Under-theorised or not, several authors see it as unlikely that the many aspects and varieties of intelligence can be made to fit one theory.[77] Historical, cultural and local backgrounds shape different kinds of intelligence and thus differing theories to explain them. This multitude of perspectives can in turn help to understand individual aspects of intelligence.[78] Warner points out the paradox that the idea that *'intelligence is too diverse to be categorised because it is something unique to each political system was itself a theory of intelligence by default'*.[79] Still Warner acknowledges the differences in theories and - using complexity-related terminology - deems it: *'a logical next step to explain intelligence as a reflexive activity, for intelligence systems under comparative scrutiny always interact with other systems (and with the world around them) in dynamic relationships and also in complex manners. Intelligence systems and the regimes that wield them, after all, comprise people, with their tendencies to biases, habits, and non-linear reactions to events'*.[80]

---

[76] Ralf G. V. Lillbacka, "Realism, Constructivism, and Intelligence Analysis," *International Journal of Intelligence and Counterintelligence* 26, no. 2 (2013): 304; Marrin, "Evaluating Intelligence Theories: Current State of Play," 479.

[77] Adda Bozeman, "Political Intelligence in Non-Western Societies: Suggestions for Comparative Research," in *Comparing Foreign Intelligence: The US, the USSR, the UK & the Third World*, ed. Roy Godson (Washington, DC: National Strategy Information Center, 1981), 149; Lawrence Freedman, "'Powerful Intelligence'," *Intelligence and National Security* 12, no. 2 (1997): 200-01; Peter Gill, "Theories of Intelligence Where Are We, Where Should We Go and How Might We Proceed?," in *Intelligence Theory: Key Questions and Debates*, ed. Peter Gill, Stephen Marrin, and Mark Phythian (Routledge, 2009), 212.

[78] Stephen Marrin, "Intelligence Analysis Theory: Explaining and Predicting Analytic Responsibilities," *Intelligence and National Security* 22, no. 6 (2007): 825; Lawrence T Mitelman, "Preface to a Theory of Intelligence," *Studies in Intelligence* 18, no. 3 (1974): 19.

[79] Michael Warner, "Theories of Intelligence: The State of Play," in *Routledge Companion to Intelligence Studies*, ed. Robert Dover, Michael S. Goodman, and Claudia Hillebrand (Routledge, 2015), 26.

[80] "Intelligence and Reflexivity: An Invitation to a Dialogue," *Intelligence & National Security* 27, no. 2 (2012): 169.

However, the traditional intelligence focus is on 'them', and does not include 'us'.[81] As of yet there is no *'definitive assessment of the state of intelligence theory'*.[82] What is clear though is that intelligence approaches cover a range of relations between theory and empirical observation. The two extremes at this range can be described as: *'One holds that the role of theory is to order, explain, predict, and that the validity of the theory can be assessed only against empirical data. The other believes that there are no facts independent of theories; all knowledge is socially constructed. Thus, "facts" can never be submitted to decisive empirical validation'*.[83]

This difference between facts independent of theory and facts as socially constructed values is about epistemology.[84] Phythian explains the positivist epistemology as a fact-based approach that beliefs *'theories exist to explain laws'* and *'in the social sciences these laws take the form of hypothesis derived from observation and/or measurement'*.[85] Phythian differentiates between two levels of laws: *'First, there are 'laws' themselves, based on proven and inevitable links. Second, there are 'law-like statements'. These latter are probalistic, derived from observation that demonstrates that a proposition is often and reliably proven but is still not inevitable, and therefore falls short of constituting a 'law'. Theory is then required to help us understand these observations. […] generating hypotheses ('laws') which call for theories to provide explanation and which can lead to corollaries or modifications to the hypothesis'*.[86]

The positivist approach utilises models, like the intelligence cycle, for aiding theorisation. Furthermore, the positivist approach assumes there is an objective

---

[81] Wilhelm Agrell and Gregory F. Treverton, *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy* (Oxford ; New York: Oxford University Press, 2015), 48.

[82] Marrin, "Evaluating Intelligence Theories: Current State of Play," 480.

[83] Gregory F. Treverton et al., "Toward a Theory of Intelligence: Workshop Report" (2006), 5.

[84] Stephen Marrin, "Intelligence Analysis and Decision-Making: Methodological Challenges," in *Intelligence Theory: Key Questions and Debates*, ed. Peter Gill, Stephen Marrin, and Mark Phythian (Routledge, 2009), 141.

[85] Mark Phythian, "Intelligence Theory and Theories of International Relations Shared World or Separate Worlds?," in *Intelligence Theory: Key Questions and Debates*, ed. Peter Gill, Stephen Marrin, and Mark Phythian (Routledge, 2009), 56.

[86] Ibid.

truth and a world knowable through measurement and observation, in an intelligence sense this equals 'speaking truth to power' through collection and analysis.[87]

This positivist epistemology is linked to realism, liberalism and idealism in international relations. Hereby the international system is seen as driven by states competing for power in an anarchic situation. States are rational actors that base their decisions on, ideally, complete and accurate information. In the power competition the intentions of other states are an important part of the information need to base one's own strategy on. In part these can be gauged because it is assumed states will always act rationally in self-interest. However, states also try to hide their intentions for others. This is where intelligence comes in; to glean secrets from rival states about their intentions and military capabilities. Gill and Phythian describe this realist approach to intelligence as a 'great game' between states wherein *'threats could be objectively measured, and the "truth" of what happened discovered by the accumulation of oral and written evidence'*.[88] This is based on the assumption that *'more information will lead to more intelligence and thus less ignorance'*.[89] Realist approaches, being state-centric, were applicable during the Cold War but encounter problems with the rise of transnational threats in the post-9/11 era.

In contrast to the fact-based, positivist approach to intelligence, a growing body of literature that advocates a value-based epistemology is less clearly to label.[90] It

[87] Agrell and Treverton, *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*, 159; Julie Mendosa, "Expanding Mental Models in Intelligence through Diverse Perspectives," *International Journal of Intelligence and CounterIntelligence* 35, no. 4 (2022): 623-24; Phythian, "Intelligence Theory and Theories of International Relations Shared World or Separate Worlds?," 65.

[88] Gill and Phythian, *Intelligence in an Insecure World*, 27.

[89] Omand, "The Future of Intelligence: What Are the Threats, the Challenges and the Opportunities?," 16.

[90] e.g. Claudia Aradau and Mc Cluskey, "Critical Security and Intelligence Studies," in *A Research Agenda for Intelligence Studies and Government*, ed. Robert Dover, Huw Dylan, and Michael S Goodman (Cheltenham: Edward Elgar, 2022); Hamilton Bean, Peter de Werd, and Cristina Ivan, "Critical Intelligence Studies: Introduction to the Special Issue," *Intelligence and National Security* 36, no. 4

entails a variety of approaches that all are not positivist but criticise it. These different approaches are therefore often grouped together as critical (theory). A critical approach to intelligence states that *'intelligence practitioners (and […] academics) are not insulated from the forces of history, culture and social positioning. A critical theorist investigates the consequences of these structures for multiple intelligence stakeholders – especially for those whose voices are suppressed – and intervenes in various discourse communities in order to promote reflection and change.'*[91]

Because of the interwoven web of historical, cultural and social perspectives 'facts' are not observed in isolation and therefore not free of values or labels.[92] This narrative of facts interpreted as values is constructed by the observer and differs from other observers even though they possess the same facts. Instead of describing the world as it is, intelligence analysis *'actively creates'* the world.[93] In essence this is about what constitutes knowledge. Post-positivist denominations, though different in detail, all share this problematisation of knowledge.

A good example of, and philosophical background for this problematization of knowledge is Lyotard's *The Postmodern Condition: A Report on Knowledge* (1986). In his book Lyotard postulates that the post-industrial age and postmodern culture have changed the status of knowledge. The technological developments of these times have an impact on knowledge. The growing use of computers to process data

(2021); Hager Ben Jaffel et al., "Collective Discussion: Toward Critical Approaches to Intelligence as a Social Phenomenon," *International Political Sociology* 14, no. 3 (2020); Gunilla Eriksson, Swedish Military Intelligence: Producing Knowledge, (Edinburgh: Edinburgh University Press, 2016); Nate Kreuter, "The US Intelligence Community's Mathematical Ideology of Technical Communication," *Technical Communication Quarterly* 24, no. 3 (2015); David W Kriebel, "Anthropological Theory and Intelligence," *Global Security and Intelligence Studies* 1, no. 1 (2015); Samantha Newbery and Christian Kaunert, "Critical Intelligence Studies: A New Framework for Analysis," *Intelligence and National Security* (2023). See also other references in this section.

[91] Hamilton Bean, "Intelligence Theory from the Margins: Questions Ignored and Debates Not Had," *Intelligence & National Security* 33, no. 4 (2018): 529.

[92] Gill and Phythian, *Intelligence in an Insecure World*, 28.

[93] Fry and Hochstein, "Epistemic Communities: Intelligence Studies and International Relations," 25.

and communication means that, instead of knowledge being formulated by the human self, the production of knowledge is externalised. Artificial Intelligence currently being the most vivid example of this. As a result knowledge becomes a commodity, indispensable to power. Foreshadowing the phenomena of fake news, troll factories, mass-surveillance, Big Data and cyber espionage Lyotard observed that knowledge: *'is already, and will continue to be, a major – perhaps the major – stake in the worldwide competition for power. It is conceivable that the nation-states will one day fight for control of information, just as they battled in the past for control over territory, and afterwards for control of access to and exploitation of raw materials and cheap labor. A new field is opened for industrial and commercial strategies on the one hand, and political and military strategies on the other'.*[94]

At the same time however, the proliferation of data and information, and the machines to process this mark the end of the state and science as sole authoritative providers of knowledge. This means the great narratives provided to explain society, e.g. political theories and scientific progression, are less valid as they are substituted by a multitude of smaller narratives. The legitimation of providing explanations and meaning – truth and facts – no longer applies to traditional authorities, there are only values; facts observed and deformed by local biases.

The lesson for intelligence in all of this is the post-positivist focus on *'not how to avoid making errors, but rather how to embrace a reflexive mode of inquiry in which the practitioner consciously admits to a bias, and sometimes makes errors because of it, and thus seeks to find ways to overcome that bias'*.[95] A useful approach to be reflexive is postmodern intelligence because it seeks to *'question or undermine 'modernist' rules and conventions of prediction and control and instead emphasize complexity, multiplicity, ambiguity, and uncertainty'*.[96] As presented shortly, complexity theory offers a way to apply this emphasis. Within the small body of post-positivist literature the publications on postmodern intelligence form even a smaller

[94] Jean Françoıs Lyotard, *The Postmodern Condition: A Report on Knowledge* (Manchester: Manchester University Press, 1986), 5.

[95] Mary Manjikian, "Positivism, Post-Positivism, and Intelligence Analysis," *International Journal of Intelligence and Counterintelligence* 26, no. 3 (2013): 567.

[96] Bean, "Intelligence Theory from the Margins: Questions Ignored and Debates Not Had," 534.

part.[97] However, the complexity-like characterizations it often carries – as seen in the quote above – are in line with the language of the trinity of transformation. It is therefore interesting to further explore this postmodern approach to intelligence.

Rathmell introduced postmodern intelligence by applying five postmodern themes to intelligence.[98] The first theme concerns the rejection of modernist unifying theories to explain social phenomena. Postmodernism brings about the 'end of grand narratives' and replaces them with alternative discourses leading to fragmented perspectives on the world. For intelligence, the end of the grand narrative of the Soviet Union meant a fragmentation of targets, roles, and missions. Furthermore, during the Cold War developments were apparently incremental and linear. Now intelligence has to understand a world that appears chaotic with multiple, overlapping and often contradictory narratives. Developments display the properties of non-linear, dynamic systems.

The second postmodern theme, related to the end of grand narratives is the end of objective truth. Instead, is the constructivist approach that the observer shapes reality according to his or her own biases. Rathmell, borrowing from Nye, compares Cold War intelligence problems to puzzles and present day intelligence problems to mysteries.[99] Cold War intelligence knew the problem at hand and could therefore comprehend some kind of objective reality, and envision a solution. Modern day intelligence does not even know if there is a single objective reality it can understand.

The third theme is the idea of 'absent centres and uncertain identities'. Contemporary technological, social, and economic advancements are breaking down binaries such as male/female, human/machine and local/global. The intelligence workforce also finds its traditional identity challenged. Technological advancements that outperform humans challenge the traditional human-machine relation. Whereas the Cold War provided focus for the intelligence effort, nowadays it is

---

[97] Myriam Dunn Cavelty and Victor Mauer, "Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence," *Security Dialogue* 40, no. 2 (2009); Chong Guan Kwa, "Postmodern Intelligence: Strategic Warning and Crisis Management," in *Perspectives on Military Intelligence from the First World War to Mali: Between Learning and Law*, ed. Floribert Baudet, et al. (The Hague, The Netherlands: T.M.C. Asser Press, 2017); Andrew Rathmell, "Towards Postmodern Intelligence," *Intelligence and National Security* 17, no. 3 (2002).

[98] "Towards Postmodern Intelligence."

[99] Joseph S. Nye, "Peering into the Future," *Foreign Affairs* 73, no. 4 (1994).

unclear for which department or national organisations, or corporation, intelligence is produced.

At the same time, constituting the fourth theme, these technological, social, and economic advances blur boundaries between states, regions, cultures and corporations. Hard and static boundaries are replaced by more fluid and multifaceted ones. For intelligence the clear boundaries of the Cold War are replaced by fluid boundaries of a myriad of state and non-state threats. Other boundaries that are changing is the increased importance of horizontal knowledge networks over hierarchy, and cooperation with the private sector.

The last theme is the emergence of the knowledge economy. Post-industrial societies go through a *'demassification of production'*. In essence this is a disruption of society by replacing hierarchical structures by networks and broadcast media with interactive personalised media – leading to the end of corporate loyalties and the rise of the autonomous knowledge worker. This means '*the end of the intelligence factory'* according to Rathmell. The knowledge economy, driven by technological and social change, is changing commerce, government, and armed forces – and it will also change the outdated idea of an intelligence factory. Given all these changes described by Rathmell, Richards looks at the intelligence cycle and describes it as a *'Fordist, Taylorian model' that's just 'not postmodern enough'*.[100]

Stated extremely, the positivist and post-positivist approaches are mutually exclusive. Positivism objects the relativism of stating value over facts and accuse it of rendering every approach to build knowledge, when subjected to specific context and thus disabling generalisations, as useless.[101] The post-positivist critics question positivist belief in empiricism and objectivity. They accuse it of denying the inherent uncertainty of an unknowable reality and knowledge construction that involves the biases of the constructors. When looking at this total of theories of intelligence the dominant theory is positivist, realist and objectivist.[102] Phythian states: *'in practice,*

[100] Richards, "Pedalling Hard: Further Questions About the Intelligence Cycle in the Contemporary Era," 48.

[101] Philip HJ Davies, "Theory and Intelligence Reconsidered," in *Intelligence Theory: Key Questions and Debate*, ed. Peter Gill, Stephen Marrin, and Mark Phythian (New York, NY: Routledge, 2009), 199.

[102] Hamilton Bean, "Rhetorical and Critical/Cultural Intelligence Studies," *Intelligence and National Security* 28, no. 4 (2013): 496; Peter Gill, Stephen Marrin, and Mark Phythian, eds., *Intelligence Theory: Key Questions and Debates* (London:

both intelligence customers and practitioners tend to view the world through realist/idealist dichotomy that does not easily accommodate or see the immediate policy relevance of post-structuralist or reflectivist approaches. Practitioners are unlikely to be highly receptive to approaches to IR which deny the possibility of uncovering objective truth when their task is to deliver the most objective analysis possible ('best truth'), and where failure can result from compromising this effort and, instead of telling 'truth to power', tailoring analysis to suit real or imagined customer preferences'.[103]

Gill acknowledges this search for truth in intelligence. He calls it *'praiseworthy'* and states the dominance of positivism is caused by it. Still, Gill also notes searching for truth can be *'highly misleading – the more so the greater the complexity and uncertainty of the threat being assessed'*.[104] From this positivist dominance it follows that post-positivist, or critical approaches, are underrepresented in intelligence theories.[105] In general, this means that the little novel theory that exists, is also not very outspoken and comprehensive. Specifically, next to the dominance of realist empiricism, there is not enough attention for new epistemologies, while this could offer valuable insights for the intelligence enterprise of the 21st century. Alternative theories and models *'can discern connections that were not evident'* in established ones.[106]

This imbalance between, roughly categorised, positivist and post-positivist intelligence theories can perhaps be explained by intelligence studies being a relatively new academic discipline. It has had too little time to evolve – compared to the related disciplines of International Relations or Security Studies – leading to the current new-born state of its critical variant. Marrin concludes that *'While there has been recent progress on developing different kinds of intelligence theory, intelligence*

Routledge, 2009); Manjikian, "Positivism, Post-Positivism, and Intelligence Analysis," 565.

[103] Phythian, "Intelligence Theory and Theories of International Relations Shared World or Separate Worlds?," 61.

[104] Peter Gill, "Intelligence, Threat, Risk and the Challenge of Oversight," *Intelligence & National Security* 27, no. 2 (2012): 212.

[105] Hamilton Bean, "Intelligence Theory from the Margins: Questions Ignored and Debates Not Had," ibid.33, no. 4 (2018): 528; Marrin, "Evaluating Intelligence Theories: Current State of Play," 483-84.

[106] Gill and Phythian, *Intelligence in an Insecure World*, 28.

studies has not yet effectively created schools of thought or fostered these structured debates'.[107]

From a Kuhnian perspective, in times of crisis scientists turn to *'philosophical analysis as a device for unlocking the riddles of their field'*.[108] Science normally tends to avoid philosophy because the paradigm is working and there is no need to question it. This also explains the relatively small amount of intelligence theories that reject the existing positivist paradigm. This underdevelopment and proliferation of new theories in intelligence studies is mirrored in the transformation debate, which I characterised as fragmented.

From the fragmented intelligence transformation debate and the theoretical imbalance it is logical and important to investigate these new theories of post-positivist, or critical, approaches to intelligence and explore their potential. As De Werd states: *'The implications for intelligence of critical philosophical approaches are profound, at various levels: the debate over paradigms in intelligence studies, the structuring of intelligence processes in organizations, and the analysis of intelligence problems'*.[109] This research therefore relates to a postmodern approach of intelligence. Where postmodern intelligence is often infused with terms like complexity or non-linear, like the other sides of the transformation trinity, it is interesting for one more reason. In other fields postmodern approaches have often led to the application of complexity theory.[110] This is a logical development. A postmodern view on knowledge seems to connect quite easily to complexity science, as philosopher and complexity researcher Cilliers shows: *'As far as postmodernism is concerned, the argument is simply that a number of theoretical approaches, loosely (or even incorrectly) bundled together under the term 'postmodern' (e.g. those of Derrida and Lyotard), have an implicit sensitivity for the complexity of the phenomena they deal with. Instead of trying to analyse complex phenomena in terms*

[107] Marrin, "Improving Intelligence Studies as an Academic Discipline," 270-71.

[108] Thomas S. Kuhn, *The Structure of Scientific Revolutions*, Fourth edition. ed. (Chicago: The University of Chicago Press, 2012), 88.

[109] Werd, "Critical Intelligence: Analysis by Contrasting Narratives: Identifying and Analyzing the Most Relevant Truths," 18. See also: "Critical Intelligence Studies? A Contribution," *Journal of European and American Intelligence Studies* 1, no. 1 (2018).

[110] Paul Cilliers, *Complexity and Postmodernism: Understanding Complex Systems* (London: Routledge, 1998).

of single or essential principles, these approaches acknowledge that it is not possible to tell a single and exclusive story about something that is really complex.'[111]

Cilliers very explicitly connects postmodernism to complexity. He states that Lyotard's description of the postmodern condition *'is in fact a description of the network of our society and of the manner in which it produces and reproduces knowledge. […] this network has become too complex for general or overarching descriptions'*.[112] Cilliers shows complexity theory and the postmodern society are both about open systems with many non-linear interactions that lead to novel behaviour and knowledge.[113] Complexity and postmodernism see relations as non-linear. Their product is more than the sum of its parts making reductionism irrelevant. Cause and effect cannot be discovered and precise prediction is impossible, resulting in ever present deep uncertainty. De Graaff contrasts intelligence's enduring positivism with the postmodern realisation of many social scientists that the ambition of imitating the natural sciences with its positivist laws and certainties has led to a crisis. If the social sciences are to deliver truth and indisputable certainties, there is little science left. To drive the point home, De Graaff cites American sociologist Wallerstein. In his book *The Uncertainties of Knowledge (2004)*, Wallerstein, drawing on complexity science, states the *'cultural end of certainties'* has been reached and that the only *'intractable reality'* is uncertainty.[114]

From the handful of articles on postmodern intelligence, only Dunn and Mauer have followed this relation between postmodernism and complexity theory. Rathmell mentions complexity theory as promising, but does not apply it.[115] Dunn and Mauer apply it to warning intelligence stating the combination of postmodernism and complexity theory *'might increase understanding of the limitations of knowledge and lead to the establishment of a political discourse of uncertainty'* in the context of intelligence.[116]

---

[111] Ibid., VIII.

[112] Ibid., 116.

[113] Ibid., 119-23.

[114] Bob de Graaff, "Intelligence and Intelligence Studies. Time for a Divorce?," *Romanian Intelligence Studies Review*, no. 21 (2019): 17.

[115] Rathmell, "Towards Postmodern Intelligence," 100.

[116] Dunn Cavelty and Mauer, "Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence," 125.

2.4 A paradigm shift

The literature often frames the process of moving from Cold War intelligence to a new form as a paradigm shift.[117] This term is introduced by the American philosopher of science Thomas Kuhn who used it to describe the development of science in his influential work *The Structure of Scientific Revolutions* (1962). It can be a helpful concept to study the shift towards post-Cold War intelligence, provided it is based on a proper theoretical explanation and not used too loosely – as is often the case. This section therefore examines what Kuhn meant with 'paradigm' (shift), before discussing several authors who apply it to intelligence with proper theoretical Kuhnian substance.

Kuhn states that the history of science is not a single, linear story of progress through the accumulation of facts. Science is about revolutions, not evolution. In a pre-revolution state 'normal science', as Kuhn names it, adheres to a paradigm. This is a model of laws, theory, application and instrumentation *'from which spring particular coherent traditions of scientific research'*.[118] Not only is research done according to the characteristics of the model, like the intelligence cycle, newcomers to the community – students – are educated in the model as well. A paradigm is scientifically successful because of two reasons. It has enough commonalities in its explanation of the world to attract a certain scientific community or discipline. Simultaneously, it leaves enough questions unanswered for practitioners to pursue scientific research. As mentioned above, this research is done according to the paradigm the researchers are part of. In a way the research aims at extending and defining the ruling paradigm more clearly. Kuhn therefore calls this *'mopping up operations'*.[119] Because the scientific work is done to optimise the ruling paradigm, there is little aim to produce novelties. In this perspective, adjusting and refining the intelligence cycle is a mopping up operation.

---

[117] e.g. James B. Bruce, "Dynamic Adaptation: A Twenty-First Century Intelligence Paradigm," (2004). (unpublished, unclassified, internal, relasead CIA paper); William J. Lahneman, National Intelligence Agencies and Transnational Threats: The Need for a New Intelligence Paradigm, (College Park, MD: Center for International & Security Studies, U. Maryland, 2008). See also other references in this section.

[118] Kuhn, *The Structure of Scientific Revolutions*, 11.

[119] Ibid., 24.

Such operations do not mean novelties are not found. Research can generate empirical facts (discoveries) or theories (inventions) that do not fit the paradigm of said research. Perhaps, in a Kuhnian sense, the anomalies of the cycle are pointing towards the explanatory failure of 'normal intelligence'. The newly discovered facts, in the words of Kuhn, are *'incommensurable'* with existing traditions of research. Sometimes it takes time to even become aware of these results. But when they are acknowledged as something to scientifically explain, they are at first incorporated into the existing paradigm. If this is not possible, the ruling paradigm can begin to shift. This starts with a small disenfranchised scientific community that lacks any critical mass. However, as the paradigm continues to be criticised more anomalies are found. A crisis begins to emerge that, as its ultimate outcome, can destroy the ruling paradigm in favour of a new one. Confronted with this crisis existing paradigms lose their monopoly while there is still no new paradigm to replace it. Normal science then resorts to extraordinary research, outside of the paradigm. This crisis of the old paradigm and transition towards a new paradigm has several symptoms. There is a *'proliferation of competing articulations'* that is accompanied with voiced discontent regarding the existing paradigm. This invokes a *'willingness to try anything' in research and a 'recourse to philosophy and to debate over fundamentals'*.[120] Though small in volume, this is where the proliferation of post-positivist intelligence theories comes into play.

Having examined Kuhn's paradigm concept, applications of it to intelligence transformation are reviewed next. One example is Moore, who states the failures of the intelligence to predict the attacks of 11 September 2001 and correctly ascertain the state of Saddam Hussein's programs of WMD are examples of Kuhnian systemic reframing crises. The Cold War approach of the understanding of problems does not fit new phenomena. It became painfully clear that *'the epistemology of normal intelligence is insufficient and new knowledge is needed. The recent failures highlight the necessity for change, as does the graying of the intelligence sensemaking workforce — new people faced with new and emerging issues should be comfortable with finding new ways to systematise their work. The changed contexts and data, once they confront practitioners with problems that are unintelligible in normal intelligence, will reflect the idea that a Kuhnian-style revolution in intelligence is underway.'*[121]

[120] Ibid., 91.

[121] Moore, *Sensemaking: A Structure for an Intelligence Revolution*, 47-48.

Many discussion of paradigms from intelligence literature, theoretically heavy or light, begin with the duality of state and non-state actors. This is not surprisingly because of the observation made earlier on intelligence in general regarding non-state actors as the most important driver of change. George sees problems with fitting non-state actors to the traditional intelligence paradigm: *'a paradigm which develops critical information through a national, classified system of collection and analysis. This paradigm has been effective in organizing US intelligence –as well as many other national intelligence systems in other countries – for what have been largely state-centric challenges'*.[122] To address transnational threats, the new paradigm should abandon its tradition of total secrecy, according to George. Intelligence should instead exploit the open sources of the Information Revolution and synthesise knowledge from the academic, private and government sectors. This collaboration is needed to cope with the deep uncertainty of the post-Cold War, multipolar world: *'As the 21st century is expected to be far less predictable and dynamic, the objective is to scan the horizon for emergent issues and so called weak signals that are harbingers of futures for which few governments have begun preparing. […] While the traditional paradigm would focus on specific "hard targets" for specific facts (also known as plans, intentions and capabilities), the collaborative model is scanning for interesting interconnections among issues, anomalies from what experts might normally expect to see, and other insights, which in the traditional paradigm would be considered irrelevant or too unconventional to be of use.'*[123]

The rise of non-state actors does not exclude traditional state-based threats. Lahneman correctly states a new paradigm should incorporate the old one based on state actors.[124] Still, a true new paradigm should contain more than a change of its referent object. It must form something completely different in all its aspects. To do so, Lahneman uses a puzzle analogy. In the traditional paradigm intelligence is about solving puzzles to which pieces are missing. Collecting as many and important puzzle pieces as possible forms a basis from which analysis can make assessments and estimates about the complete puzzle. Puzzle pieces fall into three categories: secrets, mysteries, and open source. Secrets are information that actors secure from other

[122] George, "Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm."

[123] Ibid.

[124] Lahneman, *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs*, 118-19.

actors but is still knowable. Mysteries are information that is unknowable. Contrary, open source information is easy to gain but comes with the risk of overload. The focus in this traditional paradigm is on solving secrets. In this process the puzzle pieces were relatively static; they were predictable and changed only slowly over time. This comes from the Cold War where the Soviet Union was a closed state, difficult to gain insight into. Missile launch sites and Soviet leaders do not move their position suddenly or often. Furthermore big puzzle pieces were more important than small pieces because they tell more of the whole than small pieces.[125]

Lahneman's paradigm to address transnational threats is called adaptive interpretations. Instead of solving incomplete puzzles with secrets, adaptive interpretations is about solving extremely complicated puzzles for which however almost all of the pieces are available. This is because most pieces are neither secrets or mysteries but are found in open source information. To process this, constant information collection and sharing instead of ad-hoc and problem based structures are needed. Next, this information must be continuously updated because the many and small pieces of adaptive interpretations are much more dynamic. Their information value and relation to other pieces changes and adapts to each other. Terrorists and their leadership change position quickly as opposed to Soviet weapons and politicians.[126] Summarising the paradigms, Lahneman provides a table:

[125] Ibid., 116-18.

[126] Ibid., 119-20.

Characteristic	Traditional paradigm (solving incomplete puzzles)	New paradigm (performing adaptive interpretations)
Nature of threat	Predominantly military.	Predominantly non-military.
Information requirements	Limited: emphasises secrets.	Enormous: most required information is not secret.
Nature of indicators (pieces to puzzles / adaptive interpretations)	Large and small pieces.	All pieces are small.
Importance of pieces	Large pieces are more important than small pieces. Values are static.	The value of each small piece can change from moment to moment.
Durability of solutions	Relatively constant: 'Picture' experiences slow, incremental changes.	Dynamic: values of pieces and, therefore, meaning of adaptive interpretations, change rapidly.
Need for updates to analysis	Periodic (to detect major changes).	Continuous.

Table 1: Difference between traditional and new intelligence paradigms.[127]

The dynamic and changing character of Lahneman's adaptive interpretations links to George's use of terms like *'emergent issues'* and *'interconnections'* and *'anomalies'* as being the object of his collaborative paradigm. This type of terms relates to the notion of complexity.

[127] Ibid., 120.

Treverton, who writes extensively on improving intelligence, shares this complexity-like approach. Though he does not always refer to paradigms, when he does, Treverton – like Lahneman – give substantially more body and theory to the idea of a paradigm shift than many other authors. Treverton describes the traditional paradigm as focused on a single foe (Soviet Union), depended on secrets to solve puzzles and with collection separated from analysis. This was done to safeguard the secret sources and methods. Also, because everything gained from the secretive Soviet state was worth analysing and told something about the whole, analysis was not always involved in formulating collection requirements. Another separation is intelligence from policy. To not become subjective to policy – intelligence is considered objective truth – intelligence was done by intelligence officials and policy done by government officials.[128] This process was centralised, or stove-piped, and differentiated between domestic and foreign threats.[129] In another work Treverton contrasts the old paradigm of the Cold War with the phenomena of terrorism. He does so with a table quite reminiscent of Lahneman's:

[128] Agrell and Treverton, *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*, 159; Sims, "The Theory and Philosophy of Intelligence," 43.

[129] Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information* (New York City, NY: Cambridge University Press, 2003), 221.

	Old: Cold War	New: Age of Terror
Target	States, primarily the Soviet Union.	Transnational actors, also some states.
'Boundedness'	Relatively bounded: Soviet Union ponderous.	Much less bounded: terrorists patient, but new groups and attack modes.
'Story' about target	Story: states are geographic, hierarchical, bureaucratic.	Not much story: non-states come in many shapes and sizes.
Information	Too little: dominated by secrets.	Too much: broader range of sources, although secrets still matter.
Interaction with target	Relatively little: Soviet Union would do what it would do.	Intense: terrorists as the ultimate asymmetric threat.

Table 2: From the Cold War to an Age of Terror.[130]

With Treverton the complexity is hinted at with the boundedness of intelligence problems. The Soviet Union could be defined according to its geographic, hierarchical and bureaucratic boundaries. The problem could be shaped and from its parts the whole could be constructed, and vice versa. Transnational actors are unbounded problems in that they change shape and size and new actors arise.

The goal here is not to strive for an exhaustive and clearly described paradigm shift, if that is even possible. The account of moving intelligence beyond the Cold War, condensed in above, is sufficient for now. If anything, it is important to realise the Cold War paradigm was *'so dominating that it was regarded not as a way to see the*

[130] Gregory F. Treverton, *Intelligence for an Age of Terror* (Cambridge: Cambridge University Press, 2009), 2. See page 22 in this publication for an extented version of the table.

world but as the world itself'.[131] This requires a thorough examination of how intelligence functions in the post-Cold War era. A pertinent feature of this era is the idea of hybrid warfare and grey zone operations. While issues of hybridity are also present in the paradigm tables from Lahneman and Treverton, it took the Russian invasion of Crimea for hybrid warfare to really take the stage.

The debate on intelligence theories and paradigms share a focal point of state-centric intelligence turning to non-state targets.[132] However, Russian operations in Ukraine and an assertive China draw attention to hybrid and grey zone. While hybrid and grey zone mostly narrow the actors back to states, it broadens ideas on strategy, methods and what is considered a weapon. Section 3.4.2 provides more details on the event of the Russian annexation of Crimea and its hybrid character. For now the focus is on the ambiguity regarding the debate on hybrid and grey zone, and its implications for intelligence.

In short, the terms hybrid and grey zone are based on vague concepts and poor definitions.[133] They mean different things. Grey zone conflict is often described as activities between peace and war.[134] Hybrid warfare in general concerns a mixed-methods approach to warfare. In part, hybrid warfare is done in the grey zone.[135] Hybrid warfare is often associated with Hoffman who used it to describe the early 21st Century convergence of regular and irregular forms of warfare, employed by state and non-state actors, with the inclusion of terrorism and criminal activities.[136] Non-violent means are only broadly incorporated in the concept later on. In this broadening of the initial hybrid concept the attention for cyber, informational and

---

[131] Agrell, "Intelligence Analysis after the Cold War," 94.

[132] Agrell, "The Next 100 Years?: Reflections on the Future of Intelligence," 133-34.

[133] Jan Almäng, "War, Vagueness and Hybrid War," *Defence Studies* 19, no. 2 (2019); Chiara Libiseller, "'Hybrid Warfare' as an Academic Fashion," *Journal of Strategic Studies* (2023).

[134] For a comparison of several Grey Zone definitions, see: Frank G Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *Prism* 7, no. 4 (2018).

[135] Donald Stoker and Craig Whiteside, "Blurred Lines: Gray-Zone Conflict and Hybrid War-Two Failures of American Strategic Thinking," *Naval War College Review* 73, no. 1 (2020): 13.

[136] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), 14.

psychological instruments seem to get the most attention. It can be stated that the concept *'mushroomed to explain everything known and unknown about events that seemed to be a mixture of novel enigmas and brute force'*.[137] As the case study research shows, this ambiguity in the meaning of both concepts is problematic when trying to understand and defend against hybrid warfare or grey zone operations.

For reasons of clarity this research will only use the term hybrid. It is considered a mix of regular and irregular forms of warfare as well as non-violent means. Part of this mix, such as cyber-attacks and influence operations, take place in the grey zone as they are not considered peace or traditional war. Hybrid and grey zone remain contested concepts but there are several aspects commonly present in all current concepts that are specifically of note to intelligence. While denial and deception have always served to support other operations, with hybrid threats denial and deception are the operation, they *'are designed to blur the distinction between peace and war, as well as complicate and fall below the target's detection and response thresholds'*.[138] Actors that employ hybridity aim to achieve strategic goals incrementally.[139] This makes it difficult for the warning function of intelligence. In the case of Crimea there are no accounts that Western intelligence agencies had any prior warning.[140]

The blurring of peace and war and mitigating a target's detection and response thresholds are overlapping concepts. The blurring of peace and war is done by secretly and sometimes illegally operating in the space in between, often referred to as the grey zone, with a variety of means (hybrid), including non-military, without escalating to open conflict or officially declaring war. Therefore grey zone operations are difficult to detect and respond to and as such constitute 'wicked problems' that

[137] Palle Ydstebø, "Russian Operations: Continuity, Novelties and Adaptation," in *Ukraine and Beyond: Russia's Strategic Security Challenge to Europe*, ed. Janne Haaland Matlary and Tormod Heier (Palgrave Macmillan, 2016), 149.

[138] Patrick Cullen, "Hybrid Threats as a New 'Wicked Problem' for Early Warning," (Helsinki: Hybrid Center of Excellence, 2018), 2.

[139] James J Wirtz, "Life in the "Gray Zone": Observations for Contemporary Strategists," *Defense & Security Analysis* 33, no. 2 (2017): 107.

[140] Mark Galeotti, "Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?," *Small Wars & Insurgencies* 27, no. 2 (2016): 285.

are complex.[141] Because of the discrete nature of grey zone operations, intelligence services with their experience in covert action are often involved in the execution.

Staying below the detection threshold is done by using proxies and strategically exploiting the ambiguity and uncertainty of who or what the adversary is. In Crimea, for example, Russian intelligence organised units comprised of local militia, Cossacks, and former agents of the dissolved Berkut special police.[142] Another, famous, example are the 'little green men' that spearheaded Russia's annexation of Crimea. Furthermore, *'although hybrid threats share the same strategic characteristics, the diversity of ways in which individual hybrid threats match multiple instruments of power against the specific weaknesses of the society targeted can result in each individual hybrid threat campaign having a unique signature'*.[143] The complexity of this multitude of intentions, capabilities and actors not only works against detection but also makes it very difficult to respond. Attribution, and with it a legal reaction, are almost impossible with the existence of even minor plausible deniability on the side of the suspected actor.

The response issues are also very much institutional. Does the detection problem ask for the creation of a new 'hybrid intelligence' or does it require more and better data fusion?[144] In countering hybrid threats, intelligence and security services are a logical first line of defence. However, with hybrid threats conducting a whole-of-society approach against their targets, the response should be accordingly. Therefore, shared situational awareness, intelligence sharing, counterintelligence efforts and cooperation, between a broad range of actors and organisations are often mentioned as both challenges and recommendations.[145] This goes for national level

---

[141] Cullen, "Hybrid Threats as a New 'Wicked Problem' for Early Warning."; Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges."

[142] Gregory F. Treverton et al., "Addressing Hybrid Threats," (Swedish Defence University, 2018), 20.

[143] Cullen, "Hybrid Threats as a New 'Wicked Problem' for Early Warning," 4.

[144] Gregory F. Treverton, "The Intelligence Challenges of Hybrid Threats: Focus on Cyber and Virtual Realm," (Swedish Defence University, 2018), 13.

[145] E. H. F. Donkersloot, "Hybrid Threats from the East ; the Gerasimov Doctrine and Intelligence Challenges for NATO," *Militaire spectator: tijdschrift voor het Nederlandsche leger* 186, no. 9 (2017); Björn Fägersten, "Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence," *Forward Resilience: Protecting Society in an Interconnected World* (2017): 8-9; Sergiu

as well as NATO and EU. The problems for intelligence in making sense of, and responding to, hybrid threats are broadly reflected in the case study. Any theoretical progress in understanding hybrid is not reflected there, as many respondents turn out to be confused on the issue.

2.5 Conclusion: What is the status of intelligence transformation?

Having problematised intelligence along the frame of the trinity of transformation, this section provides an answer to the first research question in describing the status of fundamental changes in intelligence. Liaropoulos summarises the state of intelligence aptly: *'In the dawn of the twenty-first century, the international environment has been transformed and is more complex compared to the one that shaped the intelligence services during the second half of the twentieth century. In particular, whereas the Cold War provided a reasonably predictable and linear framework for the intelligence community, that cannot be argued for the security environment at the beginning of the twenty-first century. Requirements for providing intelligence support have changed greatly. There is greater complexity and variety of enemies and threats. The linear understanding that characterized most of the intelligence issues during the Cold War is long gone. In the post 9/11 security environment there is a great need to re-examine the way intelligence is collected and translated into policy.'*[146]

The debate on this re-examination of intelligence is characterised as fragmented debate. To this, Boelens adds the omission of intelligence for war fighters in the RIA debate, underlining the research focus of this project. He states that RIA *'focuses mainly on the strategic level of intelligence and the restructuring of national intelligence services. By contrast, there seems to be only a limited academic debate and analysis concerning the intelligence process at the operational and tactical levels in which military forces are actually confronted with this changed context.'*[147] In

---

Medar, "Intelligence in Hybrid Warfare," in *Countering Hybrid Threats: Lessons Learned from Ukraine*, ed. Niculae Iancu, et al., NATO Science for Peace and Security Series (Amsterdam: IOS Press, 2016), 52; Treverton et al., "Addressing Hybrid Threats," 80.

[146] Liaropoulos, "A (R)Evolution in Intelligence Affairs? In Search of a New Paradigm," 6.

[147] Boelens, "The Revolution in Intelligence Affairs: Problem Solved?," 121.

short, there is more disagreement than insight in what exactly constitutes intelligence, both as a whole and in the war fighting sense.

With the devaluation of the intelligence cycle, conflicting theories and a paradigm debate, aggravated by hybrid warfare, intelligence clearly shows symptoms of a proper Kuhnian paradigm shift or crisis. The old paradigm cannot incorporate emerging anomalies. It has lost its monopoly while a new paradigm has yet to form. Though it must be said that novelties of fact (discoveries) dominate the anomalies. Novel post-positivist theories (inventions) are but a small group that lacks the mass of, for example, the factual flaws of the intelligence cycle. This Kuhnian crisis means the narrative on intelligence has become one of plethora, openness and disorder. This current state of complexity, fragmentation and ambiguity is aptly framed by Lyotard in his description of postmodernism: *'Simplifying to the extreme, I define postmodern as incredulity toward metanarratives. […] The narrative function is losing its functors, its great hero, its great dangers, its great voyages, its great goal. It is being dispersed in clouds of narrative language elements —narrative, but also denotative, prescriptive, descriptive, and so on. Conveyed within each cloud are pragmatic valencies specific to its kind. Each of us lives at the inter section of many of these. However, we do not necessarily establish stable language combinations, and the properties of the ones we do establish are not necessarily communicable.'*[148]

In this light it is only logical that the debate on improving intelligence is fragmented. With the old metanarrative of Cold War intelligence diminishing, new perspectives on intelligence that are unbounded by the old emerge. The transformation debate is held, paraphrasing Lyotard, at the intersections of differing notions of intelligence. While recognising and placing much of the topics of the preceding sections in Lyotard's description, the implicit notions of complexity as seen in the trinity of transformation are a remarkably similar.

The trinity of transformation in intelligence in this chapter is mainly theoretical, based on academic and professional publications. These studies are influenced by practice of course, but are narrow in their focus on theoretical debate rather than real world developments. Fundamental changes in intelligence should also be reflected in the real world. That is the subject of the next chapter.

[148] Lyotard, *The Postmodern Condition: A Report on Knowledge*, xxiv. Original: La condition postmoderne: rapport sur le savoir (Paris, Minuit, 1979).

3. The Intelligence Habitus

Where the previous chapter examined only topics from the debate in intelligence studies, this chapter aims for a more comprehensive view in answering the second research question: *How did the intelligence habitus evolve?* Next to theory, knowledge from the environment of intelligence practice must also be examined to get a clear understanding of how intelligence evolves. This more holistic view of intelligence is needed because it is false to assume knowledge over intelligence is only produced within academia. Furthermore, it is interesting to see if the three topics of transformation (intelligence cycle, proliferation of theory, paradigm debate) are reflected in this holistic perspective. This chapter consists of seven sections. The first section presents the structure of this chapter, sections 3.2-3.6 form the actual analysis, followed by a conclusion.

3.1 Structure of the chapter

This section first explains the concept of 'habitus' that is used to integrate theory and practice to gain a holistic view of intelligence. Second, the framework to analyse the habitus is presented. Lastly, some reflections on the framework are made.

3.1.1 What is the intelligence habitus?

This chapter aims to look beyond, but not dismiss, the theoretical approach so far and also include the practical environment of intelligence. To explain this stance the concept of 'habitus' is used. As presented below, habitus is in line with the postmodern approach of this research. The concept enables a multidisciplinary broadening in the study of intelligence, while also incorporating the practice of the intelligence environment with, among others, new technologies and world events.

Habitus is introduced by French sociologist, anthropologist and philosopher Pierre Bourdieu who concerned himself with the *'absurd opposition between individual and society'*.[149] Bourdieu engages with the culture-versus-naturalness dichotomy that is prevalent in many concepts of social science and philosophy. This also entails, for example, the opposition of subjectivism and objectivism – as seen in intelligence theories.[150] The opposition is about what is the 'true' governing factor of life. Is it a

[149] Pierre Bourdieu, *In Other Words: Essays Towards a Reflexive Sociology* (Cambridge: Polity, 1990), 31.

[150] Richard Jenkins, *Pierre Bourdieu* (London: Routledge, 1992), 40.

structuralist belief in universal rules of social life (objective) or a postmodern individual outlook (subjective)?

Bourdieu meant habitus to overcome this opposition between, using another related dichotomy, agency and structure. It fuses the opposite factors by focussing on the interplay between them. For Bourdieu, life is not about objective facts of society (theory), nor about how we discern these facts in our own subjective way (practice). It is about the interplay between theory and practice; a theory of practice — explained in his equally titled book.[151] This focus on interplay relates well to complexity. The world can be seen as a collection of Fields, as Bourdieu calls them. These are social realities with their own unique rules, in their turn partly shaped by practice. Habitus is how an individual organises itself to maximise its gain in interaction with a field. In its turn, the Field is partly shaped according to earlier practice. The Habitus is about disposition – not opposition – regarding the event-specific relations between practice and theory. The Habitus is a combination of agent-specific traits, regularities derived from experience and common knowledge regarding a field, and the behaviour in matching these against the specific situation.[152] Stated differently, it is a continuum of improvisation and regulation. In the words of Bourdieu: *'The habitus, the durably installed generative principle of regulated improvisations, produces practices which tend to reproduce the regularities immanent in the objective conditions of the production of their generative principle, while adjusting to the demands inscribed as objective potentialities in the situation, as defined by the cognitive and motivating structures making up the habitus.'*[153]

Habitus in the context of this research is thus the combination of intelligence practice and theory. It is about how intelligence is constituted by, and influences, several fields. This holistic view serves to place the dominance of academic theory in the transformation approach in context. In its aim to examine the evolution of the intelligence habitus in a further comprehensive manner, a framework is adopted to

---

[151] Pierre Bourdieu, *Esquisse D'une Théorie De La Pratique, Précédé De Trois Études D'ethnologie Kabyle* (Genève: Librairie Droz, 1972). English translation: Outline of a theory of practice.

[152] Jenkins, *Pierre Bourdieu*, chapter 4. Jen Webb, Tony Schirato, and Geoff Danaher, *Understanding Bourdieu* (London SAGE Publications, 2002), chapter 2 & 3.

[153] Pierre Bourdieu, *Outline of a Theory of Practice* (Cambridge: Cambridge University Press, 1977), 78.

cover multiple fields of intelligence change. The next part explains the framework of this chapter and reflects on it. The succeeding sections apply the framework to the development of the intelligence habitus.

3.1.2 Framework

The development of the intelligence habitus is viewed through the framework from Buzan and Hansen's *The Evolution of International Security Studies* (2009). The self-explanatory title sets a clear aim for the book. The 'evolution' of Buzan and Hansen is structured according to five driving forces: great power politics, technology, events, academic debate, and institutionalisation. Security studies, like intelligence studies, is a subfield of international relations. This makes the driving forces well suited to adopt as framework for the broad approach of this chapter.

Buzan and Hansen see these drivers of international security studies in two different notions. They shape what subjects and issues are defined as the security problems, and they shape how people produce knowledge about these.[154] In this research the framework allows for an analysis of how the intelligence habitus is influenced by, and influences, the fields of great power politics, technology, events, debate and institutionalisation. By adopting the same framework to analyse the intelligence habitus it is possible to add knowledge to intelligence from the fluid constitution of strategic, war and conflict studies and peace research, and of course real world developments. It will also be interesting to see if the notions of complexity from the previous chapter, persist in this chapter and the framework. The next section describes the general framework. The driving forces are expanded upon in the introduction to their own sections.

The five forces are generated from literature as they *'most adequately account for the major conceptual movements, for continuities as well as transformation'*. Buzan and Hansen also look at *'key themes and explanatory factors'* in international relations and international security studies in combination with a more general perspective from sociology of science literature. From this perspective is concluded that any social structure is shaped by the disposition of five forces, see Table 3.[155]

[154] Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (Cambridge: Cambridge University Press, 2016), 39-40.

[155] Ibid., 40-41.

Driving force	Description
Great power politics	Material power.
Technology	Knowledge.
Events	History and the shadows it throws into the future.
Academic debate	Social constructions.
Institutionalisation	Wealth and organisational dynamics.

Table 3: The five driving forces.[156]

Power, technology and events are external factors in the evolution of international security studies and related fields. Academic debate and institutionalisation are internal factors. These five factors are not static but are always in motion. At the same time the factors are not easily separable nor mutually exclusive, they interact. Temporarily and locally some of these factors may be more significant than others. This makes a framework of a *'heuristic explanatory quality'* that is structured yet historically and empirically sensitive in its analysis; The framework is not meant to seek causal explanations and weigh the impact of a factor against that of the others, it is meant to provide overview and depth.[157]

Buzan and Hansen explicitly take a Kuhnian perspective in their sociology of science. From this, they rightfully point out that old and new paradigms are so fundamentally different that they are incommensurable. They cannot be really compared as the entire framing of the research topic, the object of study and how to interpret the results are involved. This is an important point that is often missing in intelligence literature, as seen in Chapter 2. Buzan and Hansen state this is somewhat problematic with a sociology of science perspective. It makes it difficult to conclude when incommensurability manifests itself.[158] Stated differently, the tipping point when the ruling paradigm loses (a part of) its truth value, and a new paradigm emerges is difficult – if not impossible – to discern. The exact moment when new

[156] Compiled by author.

[157] Buzan and Hansen, *The Evolution of International Security Studies*, 41.

[158] Ibid., 43.

empirical evidence and novel theories gain a sufficient coherence to be called a paradigm is elusive, just as even defining a paradigm scientifically is.

Building on their Kuhnian stance, Buzan and Hansen, state that the progress of knowledge is not solely caused by scientific evidence. One must also consider *'other forces that play into the evolution of any field of study'*. Given that Kuhn stressed that a paradigm can only really be judged by its own scientific standards, can other non-scientific factors perhaps contribute to existing paradigms and add new perspectives? And what are these other factors? This absence of a theoretical standard and how to overcome it, how to see and measure the world, is a key characteristic of academic debates as a driving force. Next to debates, the other driving forces of the framework are found to represent the *'variety of material and ideational ways in which [international security studies] has interacted with the wider world'*. These internal and external forces in the framework form an interplay that is key to understanding fundamental change.[159]

The five driving forces of great power politics, technology, events, academic debate, and institutionalisation accommodate a pluriform perspective, emphasising the interconnectedness of scientific, sociological and technological factors. In an intelligence sense, it can place e.g. 9/11 or the war in Afghanistan, as specific events, in the context of broader developments such as technological innovation and power politics.

The framework is thus a theory in the European sense. It is *'something that organises a field systematically, structures questions and establishes a coherent and rigorous set of inter-related concepts and categories, but not in the American positivist sense of the term (which requires cause-effect propositions)'*.[160] Though incommensurable paradigms are just that, a pluriform and interconnected approach can still draw insights from a single paradigm. To sharpen the framework, the next section makes some reflections on, and additions to, the framework.

3.1.3 Reflections on the framework

Because the framework of the five driving forces will form the structure of this chapter, it is worth to reflect upon. The above mentioned characteristics that make the framework a sufficient model to adopt are, after all, brought up by the creators of the framework. A less subjective perspective might provide new insights. The

[159] Ibid., 43-47.

[160] Ibid., 47.

journal *Security Dialogue* volume 41, issue 6 (2010) contains a special section with articles that react on *The Evolution of International Security Studies,* and Buzan and Hansen's reaction on these. Two of these are discussed below because of their relevance to the adoption of the driving forces in this chapter specifically, or this research in general.

Miller's critique is on the depiction of traditionalist security studies in *The Evolution of International Security Studies*. The book sees traditionalists as dominant and *'preoccupied with bipolarity, obsessed with nuclear weapons, state-centric, policy-driven, force-oriented, and content to live within these narrow and unquestioned boundaries'*. Miller argues that Buzan and Hansen represent the challengers of the traditionalists and thus present an different depiction of traditionalists than they would present themselves. According to Miller, traditionalist security studies never was unified or homogenous but divided by political, ideological, disciplinary, methodological, and theoretical perspectives. [161] Buzan and Hansen, in their turn, state that Miller's claim that they are challengers to the traditionalists is a construction of the book, not the view of its authors.[162] To take from this is the importance of explicitly stating one's research approach and philosophical stance. This research, based on postmodern ideas and complexity theory, has the danger of simplifying the traditionalist perspective in intelligence, i.e. the positivist approach. The examination of the simplicity of Cold War intelligence in the next section aims to provide a more nuanced image to balance too rigid framing on the postmodern side.

The second insightful reaction on *The Evolution of International Security Studies*, for the purposes of this research, is by Williams who states the relationship between the public and the private has an important role in conceptions, politics and practices of security. He suggests adding it to the four structuring questions. This would open the framework to include several public/private topics of which one is of particular interest for this research: the rise of private actors. The role of these actors in the security domain has grown rapidly in the last few decades. It consists of private military companies and commercial security firms that are involved in various

[161] Steven E. Miller, "The Hegemonic Illusion? Traditional Strategic Studies in Context," *Security Dialogue* 41, no. 6 (2010): 639-40.

[162] Barry Buzan and Lene Hansen, "Beyond the Evolution of International Security Studies?," ibid.: 660.

operations such as combat, logistics, guarding and risk analysis.[163] Buzan and Hansen find the idea of the public/private topic *'intriguing'* but question *'whether the inclusion of the public/private as a fifth question will change our story or just retell it with a richer, deeper content'*.[164] The growth of the number of private security actors is reflected in intelligence. An often cited figure in this is the 2007 revelation that 70% of the US intelligence budget is outsourced.[165] Therefore this research will also pay attention to private intelligence and outsourcing under the driver of institutionalisation in section 3.6..

After these reflections and additions the framework needs a time frame. This is drawn from Chapter 2 that showed the challenges of intelligence lie in moving from the Cold War to the present day. To investigate how intelligence evolved from the Cold War to the present the framework will start with 1947 and end with 2020. 1947 is chosen as starting point after the world war because it saw a concentration of defining moments: the Truman Doctrine, the American National Security Act and Kennan's Mr. X article. This, of course, does not mean there is a sharp divide between the first and second half of the 1940s. The Japanese attack on Pearl Harbor constituted a major intelligence failure. Preventing a second surprise like Pearl Harbor was the *'guiding purpose'* of the intelligence architecture established after WW2.[166] Also, to name another example of continuity, the successful SIGINT cooperation between the US and Britain to defeat the Nazi's would be reinstated in the face of the new Soviet threat.

Next to omitting all of the pre-Cold War intelligence developments, the timeline does not aim for an exhaustive history of intelligence. Providing a detailed historical overview requires a research project of its own and is not the purpose here. There

[163] Michael C. Williams, "The Public, the Private and the Evolution of Security Studies," ibid.: 624, 28.

[164] Barry Buzan and Lene Hansen, "Beyond the Evolution of International Security Studies?," ibid.: 664.

[165] S. Chesterman, "'We Can't Spy... If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions'," *European Journal of International Law* 19, no. 5 (2008): 1056.

[166] Lowenthal, *Intelligence: From Secrets to Policy*, 19.

are better works that provide excellent overviews or historical case-studies.[167] For this research, only major developments that helped to form intelligence as it is now are reviewed. These major developments will be presented in a table at the end of this chapter.

Summarised, the theoretical topics of intelligence transformation from Chapter 2 exist mostly within the academic field of intelligence studies and are too narrow and one-dimensional to draw any conclusions about the evolution of intelligence as a whole. A more comprehensive approach is needed. Therefore, intelligence as a whole is seen as the convergence of theory and practice exemplified by the concept of habitus. The intelligence habitus is examined by adopting the framework of Buzan & Hansen. This approach will answer the second research question on the evolution of intelligence. Specifically, it will show if the notion of complexity from the transformation debate resonates with broader developments within intelligence. The next section will start the process of adding data to the framework and analysing it. This is done according to the five drivers of the framework in subsequent sections 3.2-3.6.

3.2 Great power politics

The first driving force of the framework to examine the intelligence habitus is great power politics. This compromises: 1.) The distribution of power among leading states. 2.) The patterns of amity and enmity among them. 3.) Their degree of interventionism in the international system. 4.) Their particular disposition towards security.[168] This makes great power politics a logical driver, it is the genesis of strategic studies. This connects very strongly with intelligence and its policy-support role to maintain or expand state power – and to protect against other states. This section consists of four time periods: Cold War, peace dividend, War on Terror and the return of great power politics.

3.2.1 Cold War

Security analysis during the Cold War was largely about studying US-Soviet superpower rivalry in a bipolar system with global, overt and covert influence.

[167] e.g. Christopher Andrew, *The Secret World: A History of Intelligence* (Yale: Yale University Press, 2018); John Keegan, *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda* (Random House, 2004).

[168] Buzan and Hansen, *The Evolution of International Security Studies*, 52.

Though the frame of the Cold War remained stable it fluctuated with periods of détente and periods of increased animosity. It was dominant enough however to treat other topics and events as structured according to the frame, or see them as consequences of the frame.[169]

During the Cold War intelligence was mainly geared towards Soviet military capabilities and political developments, and is therefore regarded as relatively static and simple, as seen with the debate on paradigms. This is not entirely unfair given its unifying characteristic of having the Soviet Union, as the only other world power, as an opponent for over four decades. This section however aims to nuance this monolithic image of Cold War intelligence and examine it further in two ways. First a historical overview of intelligence developments in this period will be given, as part of the pillar of Great Power Politics. The major developments will question the static image of Cold War intelligence. Second, the simplicity of Cold War intelligence will be examined further.

From World War to Cold War

After the Truman Doctrine in 1947, and based on Kennan's Mr. X article in the Foreign Affairs issue of July that year, the US adopted a policy of containment towards the Soviet Union. Kennan stated the Soviet Union was an inherently expansionist state. If it could be contained within its borders it would eventually have to deal with the flaws of the communist system and be forced to change or cease to exist. For Kennan the competition between the superpowers was mainly political and economic. Other policy officials and the Korean War later on steered containment towards a more military approach. Containment for a long period provided a focus for intelligence. It was very clear what the policy was that had to be supported. Possible areas of political, military and economic Soviet expansion and their capabilities to do so were collected upon and analysed.[170]

The year 1947 also saw the creation of the American National Security Act. The act established the National Security Council and the Central Intelligence Agency (CIA), the first US peacetime, civilian intelligence organisation. In 1961 the service branch intelligence organisations became their own organisation; the Defense Intelligence

[169] Ibid., 50, 53.

[170] Lowenthal, *Intelligence: From Secrets to Policy*, 252-53.

Agency (DIA). The formation of the DIA fits in the centralisation trend of US intelligence.[171] This was a reaction to the poor American strategic intelligence of the Second World War in general and the Japanese surprise attack on Pearl Harbor specifically. An attack was not anticipated due to a lack of information sharing between intelligence and operations personnel and between services. To address this, the CIA, as apparent from its name, would fuse all available and own intelligence to inform the president. This centralisation became a defining feature of American intelligence.[172]

Directly after the Second World War British intelligence was mainly concerned with (former) colonies and mandates such as India and Palestine. By 1948 the Soviet Union had become the top priority of British intelligence.[173] The Soviet Union not only focused Western intelligence effort it also drove intelligence cooperation. Already in 1946, the same year the British SIGINT agency Government Communication Headquarters was established, the United States and Britain made the UKUSA Agreement to share everything regarding SIGINT. This agreement came to include the British commonwealth nations of Canada, Australia and New Zealand – giving birth to the term Five Eyes community. In a second instance of major long lasting strategic cooperation, the US provided the North Atlantic Treaty Organization (NATO), established in 1949, with intelligence on Soviet military capabilities to base its defence policy on.[174]

By 1950 Soviet and American intelligence were at a stalemate. Both superpowers possessed atomic weapons but had no understanding of each other's capabilities and intentions.[175] A new impulse was given by the North Korean invasion of South Korea on 25 June, undetected by Western intelligence. As remedy against future surprise attacks the United States started a worldwide warning system exploiting its regional military commands around the world established in the Second World War. Each command created a watch centre with around the clock monitoring of its geographical territory. These centres were connected to similar ones within the

---

[171] Michael Warner, "The Rise of the US Intelligence System, 1917–1977," in *The Oxford Handbook of National Security Intelligence*, ed. Loch K. Johnson (New York, NY: Oxford University Press, 2010), 114.

[172] Treverton, *Reshaping National Intelligence for an Age of Information*, 72-73.

[173] Warner, *The Rise and Fall of Intelligence: An International Security History*, 137.

[174] Lowenthal, *Intelligence: From Secrets to Policy*, 253.

[175] Warner, *The Rise and Fall of Intelligence: An International Security History*, 145.

intelligence services on American soil. Near real-time communications allow the centres to exchange information about possible crises. Fearing a Soviet first strike without a declaration of war a methodology was created to prevent surprise attack. Preparations for war could not remain undetected. If key targets could be monitored indications for war would be discovered. If a certain threshold was reached it would constitute a warning. The watch centres were transformed to Indications and Warning Centers and Indications and Warning (I&W) intelligence became a major component of US intelligence.[176] Based on scenario's, trigger events and their consequences are formulated. These are matched against incoming information and intelligence to determine what scenario is most relevant and if there are any possible deviations.

The improvements in technical espionage and reconnaissance provided a picture of Soviet capabilities that was clear enough to gain the confidence of policymakers to promote arms control and détente by the 1970s.[177] This period also marked the stagnation of improvement as Warner notes: *'Although any choice of dates for monitoring institutional change has to be somewhat arbitrary, it seems fair to say that the "Intelligence Community" in the United States had by 1977 developed beyond its infancy and troubled adolescence into a configuration in many ways quite similar to its current (2009) form.'*[178] Despite, or perhaps because of, collecting intelligence on the Soviet sole enemy for so long the collapse of the Soviet Union blindsided the CIA and US intelligence. Though it must be stated that the CIA was pointing towards stagnating Soviet economy, and its effects, for years.[179]

[176] Arthur S. Hulnick, "Indications and Warning for Homeland Security: Seeking a New Paradigm," *International Journal of Intelligence and CounterIntelligence* 18, no. 4 (2005): 594-95.

[177] Thomas Graham, Jr. and Keith A. Hansen, *Spy Satellites: And Other Intelligence Technologies That Changed History* (Seattle: University of Washington Press, 2007), 118-19.

[178] Warner, "The Rise of the US Intelligence System, 1917–1977," 107.

[179] Michael J. Sulick, "Intelligence in the Cold War," in *Guide to the Study of Intelligence*, ed. Peter C. Olseson (Falls Church, VA: Association of Former Intelligence Officers, 2016), 135.

Observations on the 'simplicity' of Cold War intelligence

The overview above shows several developments that help understand Cold War intelligence beyond the common, static notion. There was a dynamic of change and improvement. What is constant however, is the familiar context of the Soviet Union as single and capable opponent. At least in the American case it was the 'predominant national security issue'.[180] While many issues in the Middle East and post-colonial conflicts demanded attention as well, these *'did not shape the process and profession in the way that the 'Soviet target' did'*.[181] The scope of US intelligence interest in the SU was broad and far reaching.[182] Intelligence was geared towards the *'acquisition of 'tangible' technical military, scientific and economic indicators through clandestine and specialized collection mechanisms'*.[183] This is in line with the positivist approach of accumulating measurement to ascertain reality or truth.

The Soviet Union as single dominant opponent and the straightforward intelligence organisation created to confront it is however where the simplicity ends. Ascertaining the Soviet threat specifically proved difficult. To do so, in line with the hunt for tangible and technical indicators, David Singer's quintessential and, in his own words, 'quasi-mathematical' formula of *threat perception = estimated capability x estimated intent* was adopted.[184] To date, Singer's formula is widely used to ascertain the threat of intelligence targets, reflecting ideas of a positivist approach. The difficulty in Singer's formula lies in estimating intentions. Where military capabilities are physically observable, intentions are elusive. Because of this practical fact the focus was often on military capabilities, not intentions.[185] Herman describes the workings of Western threat perception of the Soviet Union: *'Western intelligence maximized the threats of Soviet military force. […] Initially Western attitudes were formed by assumptions about worldwide communist objectives and*

[180] Lowenthal, *Intelligence: From Secrets to Policy*, 13.

[181] Rathmell, "Towards Postmodern Intelligence," 91.

[182] Lowenthal, *Intelligence: From Secrets to Policy*, 252.

[183] Rathmell, "Towards Postmodern Intelligence," 91.

[184] J. David Singer, "Threat-Perception and the Armament-Tension Dilemma," *The Journal of Conflict Resolution (pre-1986)* 2, no. 1 (1958): 94.

[185] Floribert Baudet et al., "Military Intelligence: From Telling Truth to Power to Bewilderment?," in *Perspectives on Military Intelligence from the First World War to Mali: Between Learning and Law*, ed. Floribert Baudet, et al. (The Hague: T.M.C. Asser Press, 2017), 8.

by the way Soviet behaviour seemed to bear them out; nevertheless it was Soviet military capabilities and potential that appeared to transform this picture of hostility into a massive threat. As the Cold War progressed the Soviet strategic arsenal and conventional military superiority took a growing place in the Western world-view, particularly as world communism and Soviet support for decolonization came to be of less weight. Military targets were intelligence's highest priority and provided much of the hard information available about the USSR.'[186]

The focus on military capabilities often outweighed considerations of what these capabilities were meant to achieve. Sometimes intentions were inferred from capabilities. The British Defence White Paper of 1955 spoke of Soviet military superiority which was understood by NATO member states as indication for its political objectives.[187] Soviet capabilities were easier to collect than intentions but these also had its difficulties. Examples of this are the bomber and missile gaps of the late 1950s or the differences between UK and US estimates on Soviet missiles.[188] The CIA and military estimates on Soviet military capabilities differed continuously.[189] During the Cold War the United States sometimes overstated and sometimes understated the Soviet threat.[190] All in all, even with the difficulties of threat perception diminishing the simplicity of Cold War intelligence, Western intelligence proved successful: *'In many ways Western intelligence was a success. On observable, actual aspects of Soviet military capabilities it moved from great uncertainty in the 1940s and 1950s to a reasonably good picture from the 1960s onwards, much of it derived from satellite reconnaissance. The official Soviet baseline figures handed over for the SALT, START and CFE arms control agreements of the 1970s and 1980s contained few surprises. The transparency provided by Western intelligence gave reassurance during periods of tension, and played a significant part*

[186] Herman, *Intelligence Power in Peace and War*, 246.

[187] Ibid., 241.

[188] Len Scott, "British Strategic Intelligence and the Cold War," in *The Oxford Handbook of National Security Intelligence*, ed. Loch K. johnson (New York, NY: Oxford University Press, 2010), 150.

[189] Sulick, "Intelligence in the Cold War," 134.

[190] James H. Lebovic, "Perception and Politics in Intelligence Assessment: U.S. Estimates of the Soviet and "Rogue-State" Nuclear Threats," *International Studies Perspectives* 10, no. 4 (2009): 395.

in arms control and the eventual winding down of the conflict. Considering Soviet secrecy, these were no small achievements.'[191]

To conclude, Cold War intelligence was not always simple, but it was positivist. Still, it was not exactly static and unchanging, given major developments within intelligence. The constant Soviet target would best fit the static characterisation. A better characterisation of Cold War intelligence is as a linear story of progress, as the citation above shows.

3.2.2 Peace dividend

With the Cold War ended thoughts of peace dividend and Fukuyama's concept of the end of history began to take hold. With the existential threat of a nuclear armed Soviet Union gone there was no longer a clear focus and priorities in foreign policy, defence and intelligence. Budget cuts were a logical political consequence and posed a real danger to intelligence services. The CIA as well as the German Federal Intelligence Service (Bundesnachrichtendienst, BND) were nominated for abolishment by some politicians.[192] The Dutch foreign intelligence service (Inlichtingendienst Buitenland, IDB) was actually abolished in 1994. By the end of the decade its tasks were taken over by the military intelligence service and the civilian domestic intelligence service.[193]

Budget cuts led to downsizing meaning that a shrinking workforce that was specialised in all things Soviet had to make sense of a post-Cold War world that was to be determined by diverse and more complex policy issues than before.[194] These difficulties were experienced throughout Western intelligence. Budget cuts for defence made US military cut down on tactical intelligence and pass this task to

---

[191] Herman, *Intelligence Power in Peace and War*, 242-43.

[192] Wolfgang Krieger, "The German Bundesnachrichtendienst (Bnd): Evolution and Current Policy Issues," in *The Oxford Handbook of National Security Intelligence*, ed. Loch K. johnson (New York, NY: Oxford University Press, 2010), 797; Rhodri Jeffreys-Jones, "The Rise and Fall of the CIA," ibid., ed. Loch K. Johnson, 133.

[193] Dick Engelen, "Mars Door De Tijd Van Een Institutie: Beknopte Geschiedenis Van De AIVD," in *Inlichtingen-En Veiligheidsdiensten*, ed. B.A. de Graaf, E.R. Muller, and J.A. Reijn (Alphen aan den Rijn: Kluwer, 2010), 68; Bob de Graaff and Cees Wiebes, *Villa Maarheeze: De Geschiedenis Van De Inlichtingendienst Buitenland* (Den Haag: Sdu Uitgevers, 1999), 403.

[194] Lowenthal, *Intelligence: From Secrets to Policy*, 272-73.

national intelligence services. The military's request for intelligence gave the intelligence community a new purpose but there were concerns over seconding national security to military operations. Still president Clinton, via presidential decision in 1995, made intelligence support to military operations official priority.[195] This was basically a return to the primary function of intelligence. As long as there has been war, intelligence was meant to support it. The goal of national security is a relatively new one.[196]

A vivid metaphor to describe this post-Cold War uncertainty, and therefore often quoted, is from R. James Woolsey confirmation hearing as nominee for director of Central Intelligence in 1993. Refusing to endorse any immediate budget cuts Woolsey stated that *'We have slain a large dragon. But we live now in a jungle filled with a bewildering variety of poisonous snakes. And in many ways, the dragon was easier to keep track of*'.[197] Many snakes indeed manifested themselves in the 1990s. The Gulf War, the civil war in Rwanda and the Bosnian war are but well known examples of a long list of conflicts that dominated international politics up until the 11th of September 2001.

3.2.3 War on Terror

Though terrorism was no new phenomena by any means, the attacks by Al Qaeda on US soil and the subsequent wars in Afghanistan and Iraq led to Islamic terrorism becoming the focus of the US and other Western nations. The pressure from policy and from society for protection against terrorism made intelligence part of the war on terror(ism), as coined by US president Bush. This provided a frame for intelligence to work in, like containment did, though the war on terror was less defined. For instance, many issues in the post-Cold War period are related. Terrorism, climate change and failed states form interdependencies that are difficult to prioritise. Terrorism also lacks easy to identify structures such as bases or command structures like the large political-military structure of the Soviet Union. During much of the Cold War Soviet capabilities were largely known, but not its intentions. With terrorists it was mostly the other way around.[198] The focus on capabilities, also referred to as bean-counting, is impossible with de-territorialised and networked threats as they

[195] Warner, *The Rise and Fall of Intelligence: An International Security History*, 261.

[196] Treverton, *Reshaping National Intelligence for an Age of Information*, 70.

[197] Douglas Jehl, "C.I.A. Nominee Wary of Budget Cuts," *New York Times*, 3 February 1993.

[198] Lowenthal, *Intelligence: From Secrets to Policy*, 273, 79.

are only identified through their actions.[199] As a result, the practice of intelligence in the context of counterterrorism and counterinsurgency became more complex than it was during the Cold War.

The war on terror eroded several classic divides within intelligence. The transnational feature of Islamic terrorism eroded the organisational separation between foreign and domestic intelligence. It also blurred the divide between investigative services and intelligence services. This is not an easy combination as investigations rely on facts for proof that will hold up in court and intelligence deals in possibilities and probabilities. This brought intelligence into conflict with civil rights and legislative barriers and gave rise to the idea of mass-surveillance by Western democratic states on their own citizens.[200]

The wars in Afghanistan and post-invasion Iraq proved to be difficult for the Western militaries that were geared towards large scale combat operations with a peer rival. The fighting in Afghanistan and Iraq was low-intensity, asymmetric and the enemies – an amorph assembly of insurgents, criminals and terrorists – hid among the population. This led to renewed attention for counterinsurgency and the lessons of colonial conflict. Rupert Smith even advocated a paradigm shift in modern warfare; 'interstate industrial war' had become 'war amongst the people'. This forced military intelligence to make sense of non-military issues such as societal and ethnic factors in a conflict, blurring yet another traditional division.

For military intelligence the invasion of Afghanistan and the occupation of Iraq changed its traditional enemy-centric nature. The unknown cultures for the West that Islamic terrorism hides within were to be navigated with 'population-centric intelligence', 'intelligence-led operations' and 'winning hearts and minds'. [201] These ideas were codified with the new US counterinsurgency field manual (FM 3-24).[202] One of the measures stemming from this doctrine document was the establishment of the US Human Terrain System (HTS). This was a programme by the US Army to

---

[199] Baudet et al., "Military Intelligence: From Telling Truth to Power to Bewilderment?," 9.

[200] Ibid., 11-12. Omand, "The Future of Intelligence: What Are the Threats, the Challenges and the Opportunities?," 19.

[201] Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York, NY: Vintage, 2008).

[202] "Field Manual 3-24: Counterinsurgency," ed. Headquarters Department of the Army and Headquarters Department of the Navy (Washington, DC 2006).

embed anthropologists and social scientists with units in Iraq and Afghanistan *'to support field commanders by filling their cultural knowledge gap in the current operating environment and providing cultural interpretations of events occurring within their area of operations'*.[203] The concept of human terrain was an approach to understand the complex interplay of culture, tribal politics and local realities.[204] While the system has been abandoned in the US, the Dutch Army still employs human terrain analysts.

All this adaptation was not easy, as exemplified by the report 'Fixing intel: a blueprint for making intelligence relevant in Afghanistan' (Center for a New American Security, 2010). It is a review of the US intelligence effort in Afghanistan, written four years after the introduction of FM 3-24 and three years after HTS started. Co-authored by then director of ISAF intelligence Michael Flynn, it states that *'because the United States has focused the overwhelming majority of collection efforts and analytical brainpower on insurgent groups, our intelligence apparatus still finds itself unable to answer fundamental questions about the environment in which we operate and the people we are trying to protect and persuade'*.[205]

Despite the focus on terrorism in the wake of 9/11, state actors were never completely out of sight. However, with the 'axis of evil' label from the Bush administration they were still viewed through the prism of the war on terror. The focus of intelligence on terrorism, with its non-state character, had to be adjusted again with China and Russia asserting themselves in the international system.

3.2.4 Return to great power politics

The year 2007 marks a turning point in Russian post-Soviet foreign policy. Prior, Russia was seeking ties with the United States and Europe. With the expansion of

---

[203] Nathan Finney and "AR", "Human Terrain Team Handbook," (Fort Leavenworth, KS.: Human Terrain System program, 2008), 2.

[204] Dorough-Lewis James, "Investing in Uncertainty: Applying Social Science to Military Operations," in *Social Science Goes to War: The Human Terrain System in Iraq and Afghanistan* (Oxford University Press, 2015); Louise Wiuff Moe and Markus-Michael Müller, eds., *Reconfiguring Intervention: Complexity, Resilience and the 'Local Turn' in Counterinsurgent Warfare* (London: Palgrave Macmillan, 2017).

[205] Michael T. Flynn, Matt Pottinger, and Paul Batchelor, "Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan," Working paper (Washington, DC: Center for a New American Security, 2010), 4.

NATO and the EU Russia retreated into Eurasianism; focussing on former Soviet republics along its Southern borders.[206] However, Western encroachment upon former Soviet states continued, highlighted by the interference with the Ukrainian elections in 2004.[207] Putin reacted in his speech at the 2007 Munich Security Conference. He rejected American unilateralism stating the *US 'overstepped its national borders in every way. This is visible in the economic, political, cultural and educational policies it imposes on other nations'*.[208] After Munich, Russia adopted an aggressive foreign policy with military interventions in Georgia, Ukraine and Syria. It considered itself threatened by NATO enlargement and made this a central feature of policy. This in turn led to Western politicians and militaries constituting a renewed Russian threat to democracy. Though this has a fair degree of truth to it, some nuance is in place: *'Western pundits are pessimistic about the West's ability to resist what they view as a resurgent Russia. The reality today is otherwise: Putin is on the defensive […] Democratization has already doubled the number of democratic states over the past four decades and […] there is no indication that it will stop altogether. The West's strategic position has improved enormously since the end of the Cold War, while Russia is struggling to hold on in Syria and parts of Ukraine.'*[209]

Still, Russian intelligence, building on the legacy of Soviet 'active measures', is actively trying to disrupt Western democracies. The interference with the 2016 US presidential election, the assassination attempt on Sergei Skripal – a Russian intelligence officer turned British agent – and the attempted hacking of the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Netherlands are well known examples. This makes Russia (again) a top priority for Western intelligence.

---

[206] Anuradha M. Chenoy and Rajan Kumar, *Re-Emerging Russia: Structures, Institutions and Processes* (Singapore: Palgrave Macmillan, 2017), 217.

[207] Andrew Wilson, "Ukraine's Orange Revolution, Ngos and the Role of the West*," *Cambridge Review of International Affairs* 19, no. 1 (2006).

[208] Vladimir Putin, 'Speech and the Following Discussion at the Munich Conference on Security Policy' (2007), Kremlin website, accessed 12-7-2020. http://en.kremlin.ru/events/president/transcripts/24034

[209] Maarten Rothman, "On the Instrumentality of Soft Power; or Putin against Democracy Promotion," *Winning without killing: the strategic and operational utility of non-kinetic capabilities in crises* (2017): 52.

Contrary to Russian foreign policy, China – at least seemingly – tries to avoid creating international tensions. Its staggering rise as a world power in the last few decades is based on the concept of 'Peaceful Development' that seeks to foster mutually beneficial relations with other powers to maintain economic growth. Peaceful Development guides foreign policy in such a way that it is seen as China's grand strategy.[210] Despite this intention China is becoming more assertive, also militarily, to leverage power in the international arena. Visible actions are growing pressure on Taiwan, the re-kindling of the border dispute with India, territorial claims in the South China Sea, and a growing presence in Africa.

However, independent of its international conduct, the sheer economic growth in combination with military investment is too threatening for its neighbours and established political (super)powers.[211] This alone justifies China as an intelligence target. However, China also seeks acquisition of foreign science and technology to accelerate its economic and military modernisation.[212] Chinese collection is large in its scope and scale. It collects on traditional governmental and military targets but also on universities and companies. Collection via Chinese students studying abroad and cyber espionage are often invoked examples.[213]

A re-emergent Russia and a more assertive China do not fit the frame of the war on terror or the axis of evil. The main focus of intelligence shifted back from non-state actors and 'rogue' states to power rivalry between major states. Their influence on global politics forces Western intelligence to analyse them in their own right. At the same time the struggle against terrorism continues. This underlines the observation

---

[210] Lukas K. Danner, *China's Grand Strategy: Contradictory Foreign Policy?* (Cham, Switzerland: Palgrave MacMillan, 2018).

[211] Edward Luttwak, *The Rise of China Vs. The Logic of Strategy* (Cambridge, MA: Belknap Press of Harvard University Press, 2012).

[212] Nicholas Eftimiades, "On the Question of Chinese Espionage," *Brown J. World Aff.* 26 (2019); David Snetselaar, "Dreams Lab: Assembling Knowledge Security in Sino-Dutch Research Collaborations," *European Security* 32, no. 2 (2023).

[213] William C. Hannas, James C. Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (London: Routledge, 2013). Peter Mattis, "A Guide to Chinese Intelligence Operations," (18-8-2015) Warontherocks.com; Peter Mattis and Matthew Brazil, *Chinese Communist Espionage: An Intelligence Primer* (Naval Institute Press, 2019).

of Lahneman, mentioned in the first chapter, that a new post-Cold War intelligence paradigm should incorporate both state and non-state actors.

3.3 Technology

The second driver of the framework of this chapter concerns the role of technology. Military and civilian technologies are not separate entities. There is a high degree of interplay and dual use. Technology therefore impacts economic, political, military and cultural developments.[214] As such, it is also inherently part of intelligence with collection, from Cold War multi-platform IMINT to current cyber espionage, almost equating technology. This is emphasised by the primacy of collection over direction and analysis. Driven by the idea that more information reduces uncertainty, technical collection often leads to an overload that exceeds the focus of the questions and the capacity of analysis. Another aspect of this primacy is when direction is based on previous collection. Technical collection systems therefore drive and consume by far the largest part of intelligence budgets.[215] Technology also has an impact on the external intelligence environment. It gives an adversary new capabilities, the focal point for intelligence to determine its threat. All this makes technology a strong driving force for intelligence.[216] This section is divided in two parts: from machines to computers, and the information revolution.

3.3.1 From machines to computers

In the Cold War the Soviet Union was a 'closed target' which forced intelligence to rely on remote technical collection systems.[217] Ships and planes were fitted with IMINT and SIGINT sensors to spy on the Soviet Union. Perhaps the most famous example is the U2 spy plane of the late 1950's with its characteristic look and its legacy of disproving the bomber gap. It was not only the US that performed aerial reconnaissance into the Soviet Union. The U2 mission that disproved the bomber gap was flown by a British pilot on a British mission. Sweden, France and Germany

---

[214] Buzan and Hansen, *The Evolution of International Security Studies*, 53-54.

[215] Agrell and Treverton, *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*, 39-43. Lowenthal, *Intelligence: From Secrets to Policy*, 63-64.

[216] See also: Agrell, "The Next 100 Years?: Reflections on the Future of Intelligence," 138-39; Thomas Quiggin, *Seeing the Invisible: National Security Intelligence in an Uncertain Age* (World Scientific, 2007), 36-41.

[217] Graham and Hansen, *Spy Satellites: And Other Intelligence Technologies That Changed History*, 4.

also performed aerial reconnaissance missions. The launch of the Russian Sputnik satellite in 1957 heralded the next decade that would be characterised by satellite espionage from space. In a famous example satellite IMINT, corroborated by ELINT and HUMINT, uncovered the perceived missile gap of Soviet ICBM. By the 1980s satellites outperformed aerial IMINT.[218] All in all, overhead reconnaissance was the *'most important technological development'* of Cold War intelligence.[219] The development of unmanned aerial vehicles (UAV) in the twenty-first century, that are cheaper and faster on target than satellites, balance the dominance of space-based IMINT and SIGINT.[220]

The Vietnam War brought the realisation that computerised systems of surveillance, targeting, and command and control will greatly increase combat power.[221] However, long turnaround times for national IMINT and SIGINT systems made them unsuited to provide actionable intelligence for battlefield commanders until near the end of the Cold War.[222] The introduction of precision guided ammunition forced intelligence to deliver targets faster and better. By the late 1970s the US military realised its command and control system was unsuited to make effective use of new precision weapons. The original term of 'command and control' (C2) was complemented with 'communications', abbreviated as C3. In the 1990s, against the background of the Revolution in Military Affairs (RMA), it became C4 with the addition of 'computers'. Later on 'intelligence, surveillance and reconnaissance' were added as well, making the abbreviation C4ISR. This laid the basis for the armed forces to revolutionise the old idea of command and control by seeing it as an integrated web of rapid, coordinated information flows. This became known as Network-Centric Warfare (NCW), which was heavily influenced by complexity (see Chapter 4). Modern information and communication systems, and better sensors improve military decision making. They enable distribution of information on the environment and enemy more widely and faster than before. This means that sensor-to-shooter timings are shortened, opponents can be outmanoeuvred and hit with precision munition. Vivid examples are the operations Desert Storm and Iraqi Freedom. The new precision weapons also changes intelligence at the strategic level.

---

[218] John Hughes-Wilson, *On Intelligence* (London: Constable, 2017), 178-84.

[219] Sulick, "Intelligence in the Cold War," 131.

[220] Hughes-Wilson, *On Intelligence*, 197.

[221] Warner, *The Rise and Fall of Intelligence: An International Security History*, 196.

[222] Treverton, *Reshaping National Intelligence for an Age of Information*, 13; Warner, "The Rise of the US Intelligence System, 1917–1977," 114.

A wide range of targets opened up for the improved weapons, forcing intelligence to prioritise targets.[223]

The role of intelligence in all this is not without critique either. Regarding intelligence as reliable, transparent, and on-call means the boundary with target acquisition becomes blurred. Intelligence is less concerned with uncertainty and the time-consuming process of understanding the operational environment but instead focuses only on finding targets regardless of context.[224] The concepts of C4ISR and network centric warfare are very much positivist: *'The assumption is that intelligence will be an engine fit for a fine-tuned, high-performance, machine – reliable, understood, useful, usable and on-call. One can learn exactly what one wants to know when one needs to do so, and verify its accuracy with certainty and speed. The truth and only the truth can be known. It is further assumed that intelligence will show what should be done and what will happen if one does. According to this line of thought, action taken on knowledge will have precisely the effect one intends, nothing more or less.'*[225]

Notwithstanding battlefield successes, another implication for intelligence became clear in the post-invasion insurgency after Iraqi Freedom and in the war in Afghanistan. The overreliance on technical collection led to an apparent lack of human intelligence sources. Furthermore, war is a social phenomenon and the complexity of culture, language, and religion of the people of Iraq and Afghanistan cannot be understood through technical collection alone.[226] This was the real problem the human terrain system from section 3.2.3 was to address.

---

[223] Lahneman, *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs*, 64-66; Warner, *The Rise and Fall of Intelligence: An International Security History*, 240.

[224] John Ferris, "Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?," *Intelligence and National Security* 19, no. 2 (2004): 204.

[225] Ibid., 201.

[226] Kjeld Galster, *The Face of the Foe: Pitfalls and Perspectives of Military Intelligence* (Kingston, ON: Legacy Book Press, 2015), 176-85.

3.3.2 The Information Revolution

Next to fundamentally altering traditional command and control, and envisioning concepts of armed forces as information networks with faster and better decision making and targeting, the Information Revolution has other major implications. The exponential growth of data and information and better technologies to harvest them has all the danger of overload for intelligence.[227] US general Vincent Stewart, former director of the DIA formulated the problem clearly: *'We are collecting more data today than we can effectively consume. There is simply so much information that we struggle to make sense of it. What we are able to collect, we can't process. And what we can process, we can't effectively disseminate'.*[228]

Internet and mobile communication confronted intelligence with social media, the open source domain and cyberspace. This provided an unprecedented opportunity to follow individuals online and to improve and enlarge the role of open source intelligence. A vivid example is the US program Total Information Awareness that aimed to correlate vast amounts of information to look for dangerous individuals and terrorist plots. All this readily available data and (social) media blur the collector/analyst and the producer/consumer distinctions.[229] Traditional intelligence consumers, from politicians to commanders, themselves can retrieve information and engage through the internet to try to understand the complex world. The increasing volume and value of data and information created a new domain, cyberspace, in addition to the traditional warfighting domains of land, sea and air. For intelligence this created new opportunities for espionage and covert action. Engaging human sources online led to the new terms cyber HUMINT, and cyberattacks – being difficult to attribute – became a new method of covert action.

---

[227] Tess Horlings, Roy Lindelauf, and Sebastiaan Rietjens, "Battling Information Overload in Military Intelligence & Security Organisations," in *Towards a Data-Driven Military. A Multidisciplinary Perspective.*, ed. Peter B.M.J. Pijpers, Mark Voskuijl, and Robert M. Beeres, Netherlands Annual Review of Military Science (Leiden: Leiden University Press, 2022).

[228] Kathleen M. Vogel, "The Impact of Technology on Intelligence Analysis," in *A Research Agenda for Intelligence Studies and Government*, ed. Robert Dover, Huw Dylan, and Michael S Goodman (Cheltenham: Edward Elgar, 2022), 114.

[229] Agrell and Treverton, *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*, 135.

However, while cyber presents new ways of intelligence collection and operations, all the opportunities and dangers of cyberspace are not yet clearly understood.[230]

The exponential growth of data, be it bulk or big, provides a problem for the human intelligence analyst, but the application of algorithms might help to harvest its benefits for intelligence analysis. However, as of yet, much detail on what current intelligence applications are – as well as studies of it – are lacking.[231] What is clear is that incorporation of algorithms creates new challenges as well. What will be the role of the human analyst? How to change recruitment and training?[232] The information revolution is challenging intelligence organisations beyond data overload and problems of analysis. Zegart distinguishes three major challenges[233]: 1.) Technology provides new methods, not bounded by geography, for threat actors. In this it also empowers small non-state actors. 2.) While intelligence agencies struggle with data overload, the democratisation of data leads to new intelligence producers from individual citizens to companies. Intelligence now has competitors in the sense-making business it once had monopoly over. 3.) The need for technological innovation forces intelligence organisations to engage with the outside world and leave traditional secrecy behind. The growth of publicly available information also pulls intelligence away from relying only on traditional secret intelligence. The full potential of big data and artificial intelligence in a military context remains to be seen.[234] Still, artificial intelligence is already used by different US intelligence agencies to optimise the processing of information with, for example,

[230] e.g. Maarten Rothman and Th B. F. M. Brinkel, "Of Snoops and Pirates: Competing Discourses of Cyber Security," *Cyber warfare: critical perspectives* (2012).

[231] Tess Horlings, "Dealing with Data: Coming to Grips with the Information Age in Intelligence Studies Journals," *Intelligence and National Security* 38, no. 3 (2023).

[232] Vogel, "The Impact of Technology on Intelligence Analysis."

[233] Amy B Zegart, "Spies, Lies, and Algorithms," in *Spies, Lies, and Algorithms* (Princeton: Princeton University Press, 2022), 3-10.

[234] André J Hoogstrate, "The Effect of Big Data and Ai on Forecasting in Defence and Military Applications," in *Towards a Data-Driven Military. A Multidisciplinary Perspective.*, ed. Peter B.M.J. Pijpers, Mark Voskuijl, and Robert M. Beeres, Netherlands Annual Review of Military Science (Leiden: Leiden University Press, 2022), 145-46.

automatic translation or dissemination of reporting on threats.[235] In another example, the US has established the Algorithmic Warfare Cross Functional Team, also known as Project Maven, to integrate big data and machine learning into the military. Its first mission, in 2017, was to process the sheer amount of surveillance data in the campaign against the Islamic State into actionable intelligence.[236]

Twenty-first century communication and digital technological developments are obvious drivers for change, as technology is in general. There is however, arguably, a growing impact of technological factors in today's global world. There is a general sense that some kind of threshold is surpassed in technological importance and prominence. Yet, Rathmell tempers the technological enthusiasm of advocates of an Information Age: *'It is not yet clear whether telematics and digital technologies are 'merely' transformative technologies that will change social, economic and political structures, as did the car, telephone and television earlier this century, or whether they truly represent an information revolution along the lines of the adoption of the Roman alphabet or the introduction of moveable type. Advocates of the concept of an 'Information Age' would have us believe the latter. They argue that, as with previous information revolutions, the widespread adoption of cyber and digital technologies will revolutionize our societies in ways we cannot yet conceive.'*[237]

The cultural implication of this is profound. If knowledge is increasing as a factor of production compared to capital and labour, knowledge workers become empowered. Here is a direct link with intelligence transformation. However, Rathmell observes that *'although it represents the epitome of a knowledge industry, the intelligence community is only gradually coming to grips with the implications of this profound cultural and structural transformation'*.[238]

---

[235] Patrick Tucker, "Spies Like AI: The Future of Artificial Intelligence for the US Intelligence Community" (27-1-2020), Defenseone.com.

[236] Cheryl Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End" (21-7-2017), US Department of Defense website, www.defense.gov; Marcus Weisgerber, "The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt Isis" (14-5-2017), Defenseone.com.

[237] Rathmell, "Towards Postmodern Intelligence," 98.

[238] Ibid., 99.

3.4 Events

The third category of the framework, events, are the most obvious intelligence drivers. To put it more strongly, they are the *raison d'être* of intelligence. Intelligence must inform decision-makers on threatening events and support policy to address these threats. As such, events are often framed as intelligence failure or success. The reflex is then often to focus research on e.g. organisational, analytic or legislative reform to address these events. This implies the assumption that events are a causal force that claims much influence over intelligence. It disregards other driving factors. Buzan and Hansen therefore see events in a 'constructivist manner' and point to the *'interplay between events and the other driving forces'*.[239] Events can be single, one time occurrences like a terrorist attack, or events can unfold over time in the way that environmental concerns have moved from the background to the foreground in public and policy debate.

The events examined in this section will not form a complete overview of intelligence failures or successes. Only a small selection will be regarded for their impact on intelligence. Taking from Warner, as mentioned previously, that intelligence development stagnated in de mid-1970s, the wars in Korea and Vietnam together with the Cuban Missile Crisis will serve to cover the formative Cold War period of intelligence. The 21st century transition to the post-Cold War period will be exemplified by the terrorist attacks on 9/11, Iraq's alleged Weapons of Mass Destruction and the Russian intervention in Ukraine in 2014.

3.4.1 Formative Cold War events: Korea and Vietnam Wars, and the Cuban Missile Crisis

The invasion of South Korea by North Korea was not the only intelligence failure of the Korean War. Both US and British intelligence also missed clues about Chinese intervention.[240] Despite explicit Chinese warnings not to cross the 38th parallel or risk Chinese intervention, the capture of Chinese soldiers, and combat with Chinese troops inside North-Korea the US Far East Command in early November 1950 only assessed Chinese intervention as *'distinctly possible'*.[241] Meanwhile around 300.000 Chinese troops had crossed into North-Korea and by the end of December had driven

[239] Buzan and Hansen, *The Evolution of International Security Studies*, 55.

[240] Percy Cradock, *Know Your Enemy: How the Joint Intelligence Committee Saw the World* (London: John Murray, 2002), 100-01.

[241] Harvey A. DeWeerd, "Strategic Surprise in the Korean War," (Santa Monica, CA: Rand Corporation, 1962), 20-25.

out US and UN troops. What did not help was that McArthur kept the newly created CIA out of theatre intelligence.[242] This lack of connection was exemplary for the overall lack of intelligence cooperation or coordination during the Korea War.[243] There was some change in april 1951 when general MacArthur was relieved of command and his successor general Ridgway brought in the CIA.[244] Still, only in 1952 did intelligence become all-source.[245] Both intelligence failures of the war, the North Korean invasion and Chinese intervention, would have a lasting impact on US intelligence leading to the establishment of a global warning system and warning intelligence as a discipline, as described in section 3.2.1.

The Vietnam War saw better intelligence connection, though this had its own intelligence problems. The CIA disagreed with the military assessments of North Vietnamese troop strength.[246] Furthermore, providing intelligence to the president as well as battlefield commanders proved difficult and enemy intentions were still difficult to ascertain, leading to many operational and tactical surprises despite good tactical SIGINT.[247] The most famous surprise is the Tet offensive, though a military defeat for North-Vietnam it was an intelligence failure for the US.[248] Overall, the intelligence apparatus was too big, too slow and too compartmentalised.[249] The war was a technological turning point as it was the first time computer technologies were integrated into almost all aspects of the military.[250] A good example of the technological sophistication is the Hamlet Evaluation System (HES) designed to provide an estimate of Vietcong and/or allied control over the South-Vietnamese

---

[242] Bruce O. Riedel, *JFK's Forgotten Crisis: Tibet, the CIA, and Sino-Indian War* (Washington, D.C.: Brookings Institution Press, 2015), 14.

[243] Matthew Aid, "US Humint and Comint in the Korean War: From the Approach of War to the Chinese Intervention," *Intelligence and National Security* 14, no. 4 (1999): 18.

[244] Riedel, *JFK's Forgotten Crisis: Tibet, the CIA, and Sino-Indian War*, 16.

[245] Warner, *The Rise and Fall of Intelligence: An International Security History*, 147.

[246] Sulick, "Intelligence in the Cold War," 134.

[247] Warner, "The Rise of the US Intelligence System, 1917–1977," 116.

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

[249] Hughes-Wilson, *On Intelligence*, 203.

[250] Oliver Belcher, "Sensing, Territory, Population: Computation, Embodied Sensors, and Hamlet Control in the Vietnam War," *Security Dialogue* 50, no. 5 (2019): 417.

population at the level of its smallest population units, the village and the hamlet, based on 140 indicators.[251] Though there is a great deal of criticism on HES, several recent authors state it did capture the complexity of population dynamics.[252] Though the understanding of social phenomena would soon be forgotten after Vietnam, it would come back to haunt intelligence in the next century.

The hot wars in Korea and Vietnam and the Cold War with the Soviet Union were difficult to manage at the same time. Though intelligence cooperation increased, the joint intelligence successes from the Second World War were not repeated.[253] The growing costs of intelligence (technology) related poorly to its functioning in e.g. Vietnam. President Nixon ordered a commission, led by James Schlesinger, to investigate options for reform. The report, titled 'A Review of the Intelligence Community' is often referred to as the 'Schlesinger report'. It states that the cost of intelligence has *'almost doubled' from 1960 to 1970 and that collection saw 'spectacular increases'*. This *'greatly improved knowledge about the military capabilities of potential enemies', however it did not bring 'a similar reduction in […] uncertainty about the intentions, doctrines and political processes of foreign powers'*.[254] The solution would be to centralise budgeting and programming, this centralising feature would become the dominant mode of intelligence reform for years to come.[255]

Contrary to the intelligence failures in the Korea and Vietnam War, the Cuban Missile Crisis of October 1962 is commonly seen as an intelligence success with the discovery of Soviet ballistic missiles on Cuba by an U2 spy plane. However, the success narrative only holds when the period prior to the discovery is not reviewed too critical. The pre-crisis record of intelligence, with intelligence estimates repeatedly

---

[251] Stathis N. Kalyvas and Matthew Adam Kocher, "The Dynamics of Violence in Vietnam: An Analysis of the Hamlet Evaluation System (Hes)," *Journal of Peace Research* 46, no. 3 (2009): 340.

[252] Belcher, "Sensing, Territory, Population: Computation, Embodied Sensors, and Hamlet Control in the Vietnam War," 419; Kalyvas and Kocher, "The Dynamics of Violence in Vietnam: An Analysis of the Hamlet Evaluation System (Hes)," 341.

[253] Warner, "The Rise of the US Intelligence System, 1917–1977," 114.

[254] James R. Schlesinger, "A Review of the Intelligence Community," ed. Office of Management and Budget (1971), 1.

[255] Warner, "The Rise of the US Intelligence System, 1917–1977," 117.

dismissing the possibility of Soviet military build-up on Cuba, can be seen as a warning failure.[256] The reason for this was the fragmented intelligence effort with many institutional boundaries preventing the accumulation of found signals. Zegart, notes this is not unique to the Cuban Missile Crisis as a parallel can be drawn with pre-9/11 intelligence.[257] What was unique to the crisis was the comprehensive and intensive Russian deception.[258] The eventual discovery of the Soviet missiles was done by IMINT, however it operated in the context of SIGINT (increased Russian shipments in combination with unusual communication patterns) and HUMINT (reports on planned missile placements by intelligence colonel Penkovsky, the Soviet source who also debunked the missile gap).[259] This established the lesson that good intelligence requires multiple sources from multiple intelligence disciplines.[260]

3.4.2 Transition to the 21st Century: 9/11, Iraq WMD, and the Russian annexation of Crimea

The impact of the terrorist attacks on 11 September 2001 was of such a scale that it quickly leads to comparison with Pearl Harbor, the constitutive event of US intelligence.[261] Like Pearl Harbor, 9/11 had a profound impact on intelligence and led to structural reforms. Furthermore, Al-Qaeda and the attacks can be seen as complex phenomena that emerged from an increasingly complex world.[262] The attacks have

---

[256] Amy B. Zegart, "The Cuban Missile Crisis as Intelligence Failure," *Policy Review*, no. 175 (2012).

[257] Ibid., 30-34.

[258] James H Hansen, "Soviet Deception in the Cuban Missile Crisis," *Studies in Intelligence* 46, no. 1 (2002).

[259] Sulick, "Intelligence in the Cold War," 130.

[260] Joseph Caddell, "Discovering Soviet Missiles in Cuba: How Intelligence Collection Relates to Analysis and Policy" (19-10-2017), Warontherocks.com.

[261] For example, see: Fred L. Borch, "Comparing Pearl Harbor and "9/11": Intelligence Failure? American Unpreparedness? Military Responsibility?," *The Journal of Military History* 67, no. 3 (2003); James J. Wirtz, "DéJà Vu?: Comparing Pearl Harbor and September 11," *Harvard International Review* 24, no. 3 (2002).

[262] Antoine J. Bousquet, "Complexity Theory and the War on Terror: Understanding the Self-Organising Dynamics of Leaderless Jihad," *Journal of international relations and development* (2012); Karin Knorr Cetina, "Complex Global Microstructures: The New Terrorist Societies," *Theory, Culture & Society* 22, no. 5 (2005); John Urry, "The Global Complexities of September 11th," *Theory, Culture and Society* 19, no. 4 (2002).

been widely investigated by two official commissions and many practitioners, scholars and journalists. This multitude of sources are impossible to briefly discuss here. Dahl, however, provides an apt summarising description stating that all these investigations follow the *'conventional wisdom about how intelligence fails'*: *'There had been warning signals about the threat from bin Laden and al-Qaeda, but these warnings were misunderstood or ignored in an intelligence failure unmatched by any in American history since Pearl Harbor. The reasons behind this failure - the reasons why the warnings were ignored - have been hotly debated. But the standard argument, expressed in the report of the 9/11 Commission, is that intelligence and national security officials lacked the imagination to ''connect the dots'' and make sense of the information that was available.'*[263]

It is good to distinguish between strategic and tactical warning intelligence here. Most research concludes the real problem was not with strategic warning; the more abstract and longer term indications of al-Qaeda's intentions. Where the system failed was with tactical warning intelligence; clear and distinct signals of an impending attack. Still, *'in the mission to provide usable warning, performance before September 11 failed in all phases of the intelligence cycle'*.[264] The failure was caused by several interconnected organisational obstacles such as poor information sharing, decentralisation and lacking coordination.[265]

The 9/11 commission concluded that intelligence tried to solve the Al Qaeda problem with Cold War capabilities. These capabilities were insufficient and not much improvement had taken place. The intelligence failure of 9/11 is part of *'the government's broader inability to adapt how it manages problems to the new challenges of the twenty-first century'*, especially transnational ones.[266] Hughes-Wilson describes the problem that *'After all the money, all the lessons of the past and all the work […] American intelligence was still, sixty years after Pearl Harbor, in*

[263] Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), 128.

[264] Richard K. Betts, "Two Faces of Intelligence Failure: September 11 and Iraq's Missing WMD," *Political Science Quarterly* 122, no. 4 (2008): 587.

[265] Ibid., 591; Thomas E. Copeland, *Fool Me Twice: Intelligence Failure and Mass Casualty Terrorism* (Leiden ;: Martinus Nijhoff, 2007), 214.

[266] National commission on terrorist attacks upon the United States, "The 9/11 Commission Report," (2004), 350-53.

an uncoordinated mess'.[267] Though not untrue, this is a rather orthodox view of the problem being a fault in the system and not the system itself. This is in stark contrast with the literature on paradigm shift that advocates a new system for intelligence. As such, the RIA debate was accelerated by 9/11.[268]

The reforms of 2004 fit the centralisation trend of US intelligence. A Director of National Intelligence (DNI) was created to oversee all the intelligence agencies, as recommended by the 9/11 commission. Previously, the CIA director held a dual role as Director of Central Intelligence (DCI) to oversee the intelligence agencies but this was deemed too much for one person given the coordination problems surrounding 9/11. The second reform was the establishment of a National Counterterrorism Center.

While 9/11 was caused by a failure to connect the dots, the intelligence failure regarding Iraq's weapons of mass destruction was caused by connecting too many dots.[269] In other words, intelligence jumped to conclusions by lack of rigour. It was not a purely American intelligence failure as *'all intelligence services in all countries and most private analysts came to roughly the same conclusions'* that WMDs were present and/or developed.[270] This false conclusion was mainly based on *'Iraqi behavior and the motives assumed to be consistent with that behavior'*.[271] Iraq often did not cooperate and obstructed UN weapon inspections and therefore was suspected of hiding something. As the US commission tasked with investigating the matter observed: *'When someone acts like he is hiding something, it is hard to entertain the conclusion that he really has nothing to hide.'*[272] Furthermore, Iraq had previously surprised the world with its invasion of Kuwait and its strategic weapons program then. The misjudgement on Iraqi WMDs *'was especially striking because it*

---

[267] Hughes-Wilson, *On Intelligence*, 402.

[268] Boelens, "The Revolution in Intelligence Affairs: Problem Solved?," 120.

[269] Betts, "Two Faces of Intelligence Failure: September 11 and Iraq's Missing WMD," 596; Lowenthal, *Intelligence: From Secrets to Policy*, 343.

[270] Robert Jervis, "Reports, Politics, and Intelligence Failures: The Case of Iraq," *Journal of Strategic Studies* 29, no. 1 (2006): 18.

[271] Betts, "Two Faces of Intelligence Failure: September 11 and Iraq's Missing WMD," 599.

[272] WMD Commission, "Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction," *Washington, DC: US Government Printing Office* (2005): 155.

dealt with capabilities rather than intentions, and these are supposed to be less difficult to discern'.[273]

Many involved nations performed investigations into their own road to war, the US even two. All these are very different in scope and topics, making it difficult to generalise the reasons for the intelligence failure. Also, the different national intelligence cultures confuse the matter.[274] Furthermore, with Iraq WMDs as a *casus belli* that proved to be false, inquiries were *'steeped in high politics, and played for high stakes'*.[275] For instance, the 'overall commission finding' of the US WMD commission, as it is popularly known, concludes that not only were the intelligence assessments wrong, how they were made and communicated to policy officials is also seriously flawed.[276] The report is very much focussed on the performance of the intelligence community and thus seems to absolve policymakers.[277] The Dutch inquiry (also called Commission Davids) however also criticises the use of intelligence by policy makers stating the intelligence services *'were more reserved in their assessments of the threat posed by Iraq's WMD programme than government ministers were in their communications with the Lower House'*.[278] The British investigation, dubbed the 'Butler Review', looks at the evidence chain from its beginning up to the Joint Intelligence Committee (JIC). Because the JIC consists of both intelligence producers and consumers the British system sees assessment as a government function instead of only an intelligence function. It therefore covers both intelligence and policy issues and suffers to a lesser extent of assessment problems like the American system does. The Butler Review sees flaws in the

---

[273] Robert Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War* (Ithaca, NY: Cornell University Press, 2010), 123.

[274] e.g. Lawrence J. Lamanna, "Documenting the Differences between American and British Intelligence Reports," *International Journal of Intelligence and CounterIntelligence* 20, no. 4 (2007).

[275] Alex Danchev, "The Reckoning: Official Inquiries and the Iraq War," *Intelligence & National Security* 19, no. 3 (2004): 437.

[276] Commission, "Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction," 557.

[277] Mark Phythian, "The Perfect Intelligence Failure? U.S. Pre-War Intelligence on Iraqi Weapons of Mass Destruction," *Politics & Policy* 34, no. 2 (2006): 401.

[278] English summary in: Commissie van Onderzoek Besluitvorming Irak, "Rapport Commissie Van Onderzoek Besluitvorming Irak," (Amsterdam: Boom, 2010), 531.

intelligence on Iraq specifically and not as endemic failure of the system and provides no explicit recommendations.[279]

The recommendations of the US WMD Commission followed the centralising line and, almost resembling post-9/11 reforms, proposed to grant the DNI more authority and to establish a National Counter Proliferation Center. In the Dutch case the investigative commission observed that the Dutch civilian and military intelligence services did not possess much intelligence from own collection, only from partners. In the case of Iraq the intelligence from partners, mainly US, and therefore suffered from the same problems regarding validity. This led to the realisation that Dutch intelligence should perform collection of their own at least to better be able to relate and asses partner intelligence.[280] An idea that has in it the possibility of far reaching consequences in budget and organisation for a small-power nation as The Netherlands.

Despite the difficulties of generalising from all these investigations, Jervis makes an interesting observation about the intelligence on Iraq and the many investigations. They both *'neglected social science methods, settled for more intuitive but less adequate ways of thinking, and jumped to plausible but misleading conclusions'*.[281] This neglect of social science is observed in that both the intelligence and the investigations *'fail to use the comparative method, ignore the power of asking what evidence should be seen if alternative accounts of the reality being described are correct, neglect the importance of negative evidence, and do not probe the psychology that lay behind many of the inferences, both correct and incorrect'*.[282]

The attacks by al-Qaeda on 9/11 and Iraq's missing WMD are relatively bounded problems, at least *ex post facto*. This is not to simplify the events but non-state terrorism and a state actor's strategic weapons programme can be described with

[279] Philip Davies, "A Critical Look at Britain's Spy Machinery'," *Studies in Intelligence* 49, no. 4 (2005); Lamanna, "Documenting the Differences between American and British Intelligence Reports," 620-21.

[280] Irak, "Rapport Commissie Van Onderzoek Besluitvorming Irak," 336-37; Evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2002, "Evaluatie Wet Op De Inlichtingen-En Veiligheidsdiensten 2002: Naar Een Nieuwe Balans Tussen Bevoegdheden En Waarborgen," (2013), 9.

[281] Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*, 123.

[282] Ibid., 154-55.

terminology and concepts that were familiar at the time of the events. The Russian invasion of Crimea and the Donbass 2014 is more difficult to label because the Russians used military means but stopped short of conventional, large scale war. Instead they also employed non-military means and non-state proxies in order to blur the lines between peace and war and create general ambiguity regarding the identity, Russian or separatist militias, of units in action.[283] Diplomatic, legal and media campaigns, the mobilisation of local political support among civilian groups, and economic pressures were used to redraw borders while playing at plausible deniability to disable international response and bolster domestic Russian support.[284] In Western perception this constituted a new way of warfare employed by Russia seeking to re-establish itself as a world power. This happened in hindsight as the invasion and annexation of Crimea came as a surprise, and as an intelligence failure. In this context the term Gerasimov Doctrine was introduced by Mark Galeotti in his discussion, and published translation, of an article by Russian Chief of the General Staff Valery Gerasimov. Gerasimov, writing before the Ukrainian events, observes: *'The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures - applied in coordination with the protest potential of the population. All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special-operations forces.'*[285]

With hindsight this resembles the Russian intervention in Ukraine. However, it is important to note that Gerasimov makes observations on the development of

[283] Geir Hågen Karlsen, "Tools of Russian Influence: Information and Propaganda," in *Ukraine and Beyond: Russia's Strategic Security Challenge to Europe*, ed. Janne Haaland Matlary and Tormod Heier (Palgrave Macmillan, 2016), 202; Andrew Mumford and Pascal Carlucci, "Hybrid Warfare: The Continuation of Ambiguity by Other Means," *European Journal of International Security* 8, no. 2 (2023).

[284] Roy Allison, "Russian 'Deniable' Intervention in Ukraine: How and Why Russia Broke the Rules," *International Affairs* 90, no. 6 (2014): 1258.

[285] Valery Gerasimov, "The Value of Science in Prediction," *Military-Industrial Courier* 476, no. 8 (2013). From: Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War" (6-7-2014), inmoscowsshadows.wordpress.com.

current conflicts in general and does not prescribe a new Russian doctrine.[286] The annexation of Crimea and military activities in the Donbass became synonymous with hybrid warfare and the events drove the debate on it.[287] For a large part this was caused by NATO's adoption of the term during the Wales Summit of 2014 in reaction to Russian aggression against Ukraine.[288]

The 2022 full-scale, Russian invasion of Ukraine happened during this research. The first impressions are that several significant intelligence developments took place with regards to disclosure, success, and failure – as seen in the introduction of this research. However, it is too early to tell if they represent a mere acceleration of the drivers in the framework of this research, or if they need their own category. What can be stated is that where the annexation of Crimea caused a focus on hybrid, the 2022 invasion emphasises that large scale conflict – major combat operations against a peer adversary – are still relevant. This challenges NATO and its intelligence organisation to organise for hybrid as well as conventional warfare, something that is reflected in the case study.

3.5 Debate

The fourth field of the analysis framework is about debates. This also marks the transfer from external drivers to internal ones. Buzan and Hansen state that in a positivist model, international security studies evolves progressively, responding to the external drivers only. In this model empirical data would be matched against hypothesis and theories would be confirmed, adjusted or abandoned. The actual progress of international security studies is more conflictual because there are more approaches than a positivist one and the question is if they come to be incommensurable or keep sharing constants between them.[289] In this context Buzan

[286] Mark Galeotti, "The Mythical 'Gerasimov Doctrine' and the Language of Threat," *Critical Studies on Security* 7, no. 2 (2019); "I'm Sorry for Creating the 'Gerasimov Doctrine'," *Foreign Policy* 5 (2018).

[287] Matej Kandrik, "Rethinking Russian Hybrid Warfare," *Perspectives*, no. 7 (2023): 1; Mumford and Carlucci, "Hybrid Warfare: The Continuation of Ambiguity by Other Means," 195; Tobias Sæther, "War of Broken Fraternity: Competing Explanations for the Outbreak of War in Ukraine in 2014," *The Journal of Slavic Military Studies* 36, no. 1 (2023): 34-35.

[288] Libiseller, "'Hybrid Warfare' as an Academic Fashion."

[289] Buzan and Hansen, *The Evolution of International Security Studies*, 57-60.

and Hansen talk about widening and deepening to show the different theoretical perspectives in international security studies. Widening means looking beyond the military sector as the sole domain of security. Deepening means including other referent objects than the state, such as collectives or individuals.[290]

The paradigm shift debate and the emergence of new post-positivist theories from the former chapter are about new perspectives on intelligence in an ontological and epistemological sense. While this is definitely the start of a process of widening and deepening in intelligence, it is as of yet too early to formulate any definitive answer.[291] It remains to be seen if post-positivist approaches will gain traction within intelligence and how dominant positivist intelligence approaches will react to this. The body of literature on this, examined in Chapter 2, is too small to draw any conclusions on coherence for theory or establish schools of thought. Therefore this research aims to contribute to the growing volume of post-positivist approaches to intelligence (see section 2.3).

This current chapter covers many other debate topics, e.g. Cold War intelligence, the influence of technology, and intelligence failure. Many more debates and topics exist but this particular section examines two: the debate around Sherman Kent versus Willmoore Kendall, and intelligence as art or science. Both debates are fundamental and relevant. Kent in some way is the personification of the traditional intelligence system and Kendall provides it with enduring and valid critique. The relation of intelligence to science and/or art is essential to understanding how knowledge is created. As such, both debates provide substance that parallels, or compliments, the debate on paradigms.

Lastly, the adjective 'academic' before debate is left out in this research. This broadens the term 'debate' to include academic as well as professional debate. This better suits the fact that many intelligence academics are former practitioners, including Kent and Kendall.

3.5.1 Kent and Kendall

The first debate is between Sherman Kent and Willmoore Kendall, who are the first intelligence theorists with Kent being regarded as the founding father of intelligence analysis. Both men represent different approaches to intelligence during its

[290] Ibid., 188.

[291] Newbery and Kaunert, "Critical Intelligence Studies: A New Framework for Analysis."

formative period of the mid-1940s. It is a constituted debate, created because Kent and Kendall are opposites on several intelligence issues, most notably the relation between intelligence and policy – and this opposition forms a natural range along which to examine intelligence. It is a debate only in hindsight. Despite working in the same surroundings or organisations at several instances there is not much evidence of interaction.[292] Furthermore, there are other authors that have written on the same topics as Kent, and thus also Kendall.[293] Perhaps, Kent as the founding father of intelligence analysis and Kendall having reviewed his seminal *Strategic Intelligence for American Foreign Policy* (1949) is the only reason the debate largely ignores the other names. Still, even for a constituted debate, Kent and Kendall's opposite views can be helpful to understand the intelligence habitus. Kent heavily influenced intelligence, and still does, as performed by the US and its allies as well.[294] His positivist epistemology and emphasis on applying the scientific method of the natural sciences to social science is still the dominant feature of intelligence.[295] Kendall seems to have some important lessons for how intelligence might be able to change.[296]

---

[292] Jack Davis, "The Kent-Kendall Debate of 1949," *Studies in Intelligence* 35, no. 2 (1992): 96.

[293] Marrin, "Improving Intelligence Studies as an Academic Discipline," 271, 73.; Roger Hilsman, "Intelligence and Policy-Making in Foreign Affairs," *World Politics* 5, no. 1 (1952); Thomas L. Hughes, "The Fate of Facts in the World of Men" (paper presented at the Proceedings of the American Society of International Law at its annual meeting, 1969); Klaus Eugen Knorr, "Foreign Intelligence and the Social Sciences," (Center of International Studies, Princeton University, 1964); Washington Platt, *Strategic Intelligence Production: Basic Principles* (Praeger, 1957).

[294] Agrell and Treverton, *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*, 48.

[295] Graaff, "Intelligence and Intelligence Studies. Time for a Divorce?," 11-12; Marrin, "Analytic Objectivity and Science: Evaluating the US Intelligence Community's Approach to Applied Epistemology," *Intelligence and National Security* 35, no. 3 (2020): 352.

[296] Anthony Olcott, "Revisiting the Legacy: Sherman Kent, Willmoore Kendall, and George Pettee–Strategic Intelligence in the Digital Age," *Studies in intelligence* 53, no. 2 (2009): 21.

A short biography of the two men can shed more light on their different views of intelligence. Kent was an assistant professor of History at Yale University. When war broke out he joined the Research and Analysis Branch of what soon would become the Office of Strategic Services. After the war he took a position at the National War College during which he wrote his famous book on strategic intelligence before joining the CIA in 1950. Before the war Kendall, too, was an assistant professor. His field was political science at the University of Richmond. He joined the war effort taking various positions which were more operational than intelligence. After the war he joined what would become the CIA. In 1947 he became an associate professor of political science at Yale, the same year Kent became a full professor at the History Department. The opposite nature of the Kent Kendall debate is reflected in their backgrounds: history and intelligence (analysis) versus political science and operations.

Kendall reviewed Kent's *Strategic Intelligence for American Foreign Policy* (1949).[297] He criticised Kent's recommendations for improving intelligence as well as his underlaying general theory of intelligence.[298] Kendall dubbed Kent's work not as the book of a reformer. His critique was that it is dominated by a wartime conception of intelligence. Kendall saw Kent's intelligence as too fixated on (potential) enemies to support policy. In doing so it neglected *'the big job – the carving out of United States destiny in the world'*.[299] *'Although Kendall obviously had views about what that destiny should be, he did not take the triumph of those views as a self-evident scientific "fact," as did Kent. Rather he defined that destiny as a belief system'*, according to Olcott.[300]

Kendall also stated the work was based on a *'crassly empirical conception of the research process in the social sciences'*. Because intelligence tends to divide the world into regional analytic responsibilities and staffs it with social scientists a high number of historians will end up in intelligence analysis. Their historic reflex will be to process all incoming information to test hypothesis. The information overload will make analysis a matter of not trying to drown in the sea of information. Instead, Kendall wants analysis to be properly based on the social sciences in that it

[297] Willmoore Kendall, "The Function of Intelligence," *World Politics* 1, no. 4 (1949).

[298] Davis, "The Kent-Kendall Debate of 1949," 95.

[299] Kendall, "The Function of Intelligence," 544, 48.

[300] Olcott, "Revisiting the Legacy: Sherman Kent, Willmoore Kendall, and George Pettee–Strategic Intelligence in the Digital Age," 26.

formulates theory. Then, analysts will be given real-time data from the field and not written reports that are always behind on the unfolding events.[301]

Intelligence's fixation on prediction to prevent surprise stopped short of Kendall's idea of intelligence. He observes that with Kent *'the course of events is conceived not as something you try to influence but as a tape all printed up inside a machine'* and intelligence only reads the tape to policymakers.[302] In his view intelligence should influence in the sense that it helps policy to understand the operative factors on which it can have an impact.[303]

To summarise the differences between Kent and Kendall they are characterised by Olcott as a puzzle and a mystery solver respectively. Kent with his positivist belief in facts and truths sees intelligence problems as missing facts, or puzzle pieces. This is very much the traditional intelligence paradigm, which is no wonder regarding Kent's influence on the profession of intelligence. Contrary, Kendall is more postmodern and sees intelligence problems as mysteries because they exist in a belief system that are *'arbitrary constructions that — importantly — can never be proven to be true or false'*.[304] Another characterisation concerns the proximity of intelligence to policy. For Kent intelligence should be independent and objective and refrain from advise. The desired independence and objectivity intelligence led to the famous motto of 'speaking truth to power'. *'Objectivity is part of the search for truth with its value being absolute […] – the separation of intelligence analysts from policymakers – ensures that the search for truth can continue unimpeded'*, explains Marrin.[305] For Kendall intelligence should actively work together with policy. In the literature this is often captured as the traditionalist and activist models of intelligence.[306]

---

[301] Kendall, "The Function of Intelligence," 550-51.

[302] Ibid., 549.

[303] Davis, "The Kent-Kendall Debate of 1949," 95.

[304] Olcott, "Revisiting the Legacy: Sherman Kent, Willmoore Kendall, and George Pettee–Strategic Intelligence in the Digital Age," 27.

[305] Marrin, "Analytic Objectivity and Science: Evaluating the US Intelligence Community's Approach to Applied Epistemology," 352-53.

[306] Uri Bar-Joseph, "Intelligence Intervention in the Politics of Democratic States: The United States," *Israel, and Britain (University Park: Pennsylvania State Press, 1995)* (1995): 23; Arthur S Hulnick, "The Intelligence Producer–Policy Consumer Linkage: A Theoretical Approach," *Intelligence and National Security* 1, no. 2

Against the background of positivist dominance in intelligence and the emergence of post-positivist theories Kendall still seems relevant. Agrell and Treverton state that a bigger role for Kendall might have *'explicitly acknowledged that "us" and our actions cannot be excluded from the analysis'*, established more interaction between policy and intelligence, and might have given more theory or thought to its own business.[307] The insights of Kendall betray a more complex view of intelligence with attention to interaction with operations and policy, and the reflexive idea that there is no objective perspective because the observer influences the perception.

The Kent-Kendall debate is about ontology, epistemology and methodology. It is also about how much influence social sciences should have. The debate was in part formed around policy issues and hereby was concerned with the boundary between the scholar and policy advisor roles, or traditionalist and activist models of intelligence. While Kent and Kendall form perhaps more of a distinction than a true debate, they represent two established positions along which to examine intelligence. All this makes both men highly influential in the debate on intelligence. The relation between intelligence and science, that Kent and Kendall wrote about, is the topic of the next section.

3.5.2 Intelligence as art or science

The question if a discipline or profession is an art or science is fundamental to its pursuit. If it is art, practical and subjective knowledge arrived at by intuition, then learning and improving the discipline is extremely difficult. If a discipline is science, then objective knowledge is created through measurement with structured methods and more easy to learn.[308] The art-or-science approach is therefore a helpful contradiction to investigate intelligence.[309] Still, the science perspective seems to

(1986): 214; Loch K Johnson and James J Wirtz, *Intelligence: The Secret World of Spies: An Anthology*, 3 ed. (Oxford University Press, 2011), 165-66.

[307] Agrell and Treverton, *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*, 54.

[308] Robert D Folker, *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods* (Washington, D.C: Joint Military Intelligence College, 2000), 6.

[309] Josh Kerbel, "Lost for Words: The Intelligence Community's Struggle to Find Its Voice," *Parameters* 38, no. 2 (2008): 103-05; Stephen Marrin, *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice* (Milton Park, Abingdon, Oxon: Routledge, 2012); Julian Richards, *The Art and*

have the upper hand. Within intelligence, natural sciences play a major part in technical processes and collection disciplines. These, however, have little to offer to understand intelligence as a whole. As a form of knowledge production intelligence lacks an artificial, closed system for controlled experiments. Social science, carried out in open systems where change is constant, seems more suitable for studying intelligence and, stated more specifically, intelligence analysis.[310]

Wirtz states the US, and other countries such as the UK and Israel, developed an 'intelligence paradigm' that is *'an effort to apply analytic methodologies and insights drawn from the social sciences'*.[311] Marrin shows that the literature mainly sees intelligence as a (social) science, not as art. Starting with Kent's *Strategic Intelligence for American Foreign Policy* (1949) much foundational literature is an approximation of the scientific method where data is collected, hypotheses are formed and tested, and conclusions based on the foregoing are drawn.[312] With this, the scientific ethos of objectivity, along with independence, has also been incorporated in intelligence analysis. The most exemplary form of intelligence (analysis) as social science is the use of Structured Analytic Techniques (SATs). These are techniques, adopted from social science to structure thinking and to reduce biases.[313] In a way they are meant to guarantee the objectivity in intelligence.

Science of Intelligence Analysis (Oxford ;: Oxford University Press, 2010); Itai Shapira, "Strategic Intelligence as an Art and a Science: Creating and Using Conceptual Frameworks," *Intelligence and National Security* 35, no. 2 (2020).

[310] Treverton et al., "Toward a Theory of Intelligence: Workshop Report," 6.

[311] James J. Wirtz, "The American Approach to Intelligence Studies," in *Handbook of Intelligence Studies*, ed. Loch K. Johnson (Routledge, 2009), 31.

[312] Stephen Marrin, "Is Intelligence Analysis an Art or a Science?," *International Journal of Intelligence and CounterIntelligence* 25, no. 3 (2012): 530. Marrin bases his article for a large part on an lenghty e-mail exchange between member of the International Association for Intelligence Education (IAFIE). For reasons of clarity Marrin's article is referenced and not the primary (e-mail) sources; See also: "Modeling Intelligence Analysis on the Social Sciences," in *Handbook of Intelligence Studies*, ed. loch K. Johnson (Routledge, 2009).

[313] Richards J. Heuer and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, Second edition. ed. (Washington, DC: CQ Press, 2015); Morgan D Jones, *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving* (Crown Business, 1998); "Quick Wins for Busy Analysts," ed.

There are however several reservations to be made when intelligence is equated with (social) science. Intelligence analysis is not repeatable like scientific experiments are. Chances are, different analysts working with the same data and following the same methodology will end up with different outcomes. Furthermore, with intelligence problems the effects of variables, or even the variables themselves, are unpredictable. Still, to some extent this reflects the limitations of social science in general.[314] Intelligence however, differs in several specific issues from science. It is meant to be relevant, timely and actionable from the perspective of a specific consumer. Intelligence is not a scientific search for some ground truth but the production of practical wisdom.[315] Furthermore, with intelligence the subject of study often takes measures to avoid being analysed correctly by adapting its behaviour and/or spreading false information, known as denial and deception.

Next to these caveats, intelligence as, or borrowing from, social science is met with critique. Several publications question the science of SATs.[316] Agrell labels intelligence a protoscience because it lacks a comprehensive set of theories, a scientific discourse, and self-reflection. It needs to become an *'applied science with an open culture in which competing interpretations are the norm, not the (barely tolerated) exception'*.[317] Cooper states that *'analysis falls far short of being a "scientific method" […] this view of science itself is "scientism," which fails to*

Defence Intelligence (London: United Kingdom Ministry of Defence, 2013); "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," ed. Center for the Study of Intelligence (Washington, D.C.: Central Intelligence Agency, 2009).

[314] Marrin, "Is Intelligence Analysis an Art or a Science?," 532.

[315] Werd, "Critical Intelligence: Analysis by Contrasting Narratives: Identifying and Analyzing the Most Relevant Truths," 16.

[316] e.g. Stephen J. Artner, Richard. Girven, and James B. Bruce, "Assessing the Value of Structured Analytic Techniques in the US Intelligence Community," (Rand Corporation, 2016); Stephen J. Coulthart, "An Evidence-Based Evaluation of 12 Core Structured Analytic Techniques," *The International Journal of Intelligence and Counter Intelligence* 30, no. 2 (2017); Mandeep K. Dhami, Ian K. Belton, and David R. Mandel, "The "Analysis of Competing Hypotheses" in Intelligence Analysis," *Applied Cognitive Psychology* 33, no. 6 (2019).

[317] Agrell, "Intelligence Analysis after the Cold War," 94, 113.

recognize the important role of less "rational" and less "scientific" elements, such as imagination and intuition.'[318]

Another critique, by Bang, is that intelligence as social science is mainly about qualitative methods with quantitative methods seen as unsuited.[319] According to Bang this is based on doubts of scientific reliability and validity. There are concerns regarding data quality, data scarcity, supposedly unquantifiable data or quantitative methods not being suited for intelligence, a negative trade-off with much needed qualitative methods, or the assumption war is too complex to quantify because there are too many factors involved.[320] This debate also exists in most fields of social science, not least within political science, especially security studies.[321] However, the explosion of data and technological developments both force and enable quantitative methods that go beyond the statistics of present day social network analysis that is broadly used in intelligence. If any, quantitative methods are very well suited for studying complex phenomena such as war (see section 4.3.1).

Because of the mentioned reservations and critique on intelligence as science it is also seen as an art, though the literature on this is limited.[322] Instead of proving or falsifying hypothesis, intelligence as an art is about instinct, education and experience. It is the creative and imaginative thinking that manipulates information to reveal new information and perspectives.[323] There are methods and techniques to this approach but they do not constitute a scientific process, rather, this is what is referred to as tradecraft. Describing the relation between science and art, in the context of intelligence, as a dichotomy denies the overlap. If intelligence as art takes up the space where intelligence is not science then it is more logical to regard intelligence as a combination of the two. Based on this reasoning a comparison

[318] Jeffrey R. Cooper, "Curing Analytic Pathologies," (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2005), 26-27.

[319] Martin Bang, "Pitfalls in Military Quantitative Intelligence Analysis: Incident Reporting in a Low Intensity Conflict," *Intelligence & National Security* 31, no. 1 (2016): 49.

[320] Ibid., 55-57.

[321] Ibid., 56.

[322] Marrin, "Is Intelligence Analysis an Art or a Science?," 540.

[323] Ibid., 533.

between intelligence and medicine, and vice versa, is sometimes mentioned.[324] Several publications compare intelligence to a diverse set of disciplines such as behavioural and social science, history and public policy analysis.[325]

Agrell and Treverton go even further by stating that there is a convergence between intelligence and science as such. They state intelligence *'is becoming more "scientific", not necessarily in the traditional academic disciplinary sense, but resembling more the emerging complex, cross-boundary, and target-oriented research efforts.'* At the same time *'trans- and interdisciplinary research in science is becoming more like intelligence in focusing on risk assessments, probabilities, and warning, and in communicating not only results but also uncertainty'*.[326] Stated differently, increased complexity of targets and public and policy demand for better assessments of a wider range of threats, forces intelligence to transform from a proto-discipline to inter- and trans-intelligence approach.[327]

The main point of this section is that while intelligence may still be protoscience, it could also be viewed as making inter and transdisciplinary approaches to understand the increased complexity of the environment. In a true postmodern sense, instead of following a linear progress and becoming a discernible discipline first, intelligence already changes its shape. On the question if intelligence studies is a proper

---

[324] Amy K. Blake, "From Intelligence Analysis to Medical Education: Using Structured Tools to Manage Bias," *Medical Education* 52, no. 3 (2018); Stephen Marrin and Jonathan D. Clemente, "Modeling an Intelligence Analysis Profession on Medicine," *International Journal of Intelligence and CounterIntelligence* 19, no. 4 (2006); Stephen Marrin and Efren Torres, "Improving How to Think in Intelligence Analysis and Medicine," *Intelligence and National Security* 32, no. 5 (2017).

[325] "A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis."; Stephen Marrin, "Understanding and Improving Intelligence Analysis by Learning from Other Disciplines," *Intelligence and National Security* 32, no. 5 (2017). This issue of INS is dedicated to comparing intelligence to other disciplines.

[326] Agrell and Treverton, *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*, 8; See also: Agrell, "Intelligence Analysis after the Cold War," 112-13.

[327] Agrell and Treverton, *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*, 7.

discipline Gill and Phythian state that it *'is a coherent subject area, but its project is most effective when it draws on other disciplines and reaps the benefits of interdisciplinarity'*.[328] Richards also emphasises the interdisciplinarity of intelligence studies.[329] This sharply contradicts the observations from several scholars and authors in section 2.3 that portrays intelligence as a field that exists in isolation from other fields of knowledge and academic disciplines.

3.6 Institutionalisation

The last field from the framework to examine is institutionalisation. Referencing Foucault, Buzan and Hansen, notice *'that academic fields and disciplines are not objective representations of reality, but rather particular ways of looking at, and generating knowledge about, the world'.* In the same way, the particular Kentian model is the standard for generating knowledge in the intelligence habitus. Buzan and Hansen state being a field of study requires self-identification. Academic debates do not exist in a vacuum. For an academic discipline or field to exist there have to be supporting institutional structures and identities that shape it. Institutionalisation involves allocation of resources, processes of reproduction and the bureaucratic dynamics of organisations. Because of this, institutionalisation creates a type of inertia or momentum that carries the past into the future. It also creates a conservative attitude when encountering novelties such as widening/deepening approaches.[330] Buzan and Hansen are writing on international security studies but the parallels with the intelligence habitus are obvious. Supporting structures such as government bureaucracy, national and military decision-making and a closed, professional culture that permeate intelligence also make it troublesome to adapt.

To examine the Institutionalisation of international security studies, Buzan and Hansen see it as compromising four overlapping elements: organisational structures, funding, the dissemination of knowledge, and research networks. However, this is in the context of the study of an academic field while this research examines the intelligence habitus. Therefore the original subcategories of institutionalisation are

[328] P. Gill and M. Phythian, "What Is Intelligence Studies?," *The International Journal of Intelligence, Security, and Public Affairs* 18, no. 1 (2016): 7-8.

[329] Julian Richards, "Intelligence Studies, Academia and Professionalization," ibid.

[330] Buzan and Hansen, *The Evolution of International Security Studies*, 60-61.

replaced, or rather subsumed, by Landscape (what entities make up the habitus) and Adaptation (how intelligence adjusts to new phenomena).

3.6.1 Landscape

The number of actors that inhibit the modern intelligence landscape has grown since the late 19th or early 20th century when it was in essence a bureaucratic state-activity. Within governments, the consumers of intelligence have grown beyond heads of state and military commanders to a government-wide consumer base. Though intelligence has seen outsourcing to private contractors since its very beginnings, present day outsourcing dwarfs all historic examples. Another, relatively new, actor is the academic field of intelligence studies.

These three groups (government, private sector, academic intelligence studies) are the major, most interconnected, inhabitants of the intelligence landscape and as such exercise the most influence on the habitus. These three actors are examined in this section. However, there are more intelligence actors. Closely aligned with the government as an intelligence actor – at least in many democratic countries – are parliamentary oversight bodies, legal accountability bodies, and media. While these are important actors, they are peripheral in that they do not do intelligence, nor develop it actively. As such, they fall outside the scope of this research.

The proliferation of technology and knowledge of intelligence procedures and methods has given rise to a multitude of very different actors. These range from activist and research networks, the surveillance technology industry or companies that specialise in corporate, or business, intelligence.[331] Though there can be an overlap between these smaller groups and the larger contractor group, the small groups are essentially more independent from government or any traditional, national intelligence system. For their smaller influence on the intelligence habitus these 'smaller' private entities are excluded from this research.

Government is the first category to examine what entities and their activities make up the intelligence landscape. Herman offers a useful way to generalise about government intelligence. Though references to an intelligence community remain an English speaking speciality there is, at least in the West, a realisation that intelligence forms a national system to be managed as a national resource. Drawing from the US and the British intelligence structure, Herman presents a schematic applicable to other Western systems. In this schematic there is an intelligence community at the

[331] Warner, *The Rise and Fall of Intelligence: An International Security History*, 308.

national level consisting of departments and agencies. From this level there are *'downward extensions of central intelligence'*, as Herman calls them. These extensions are armed forces intelligence and security intelligence. They form vertical intelligence communities, extending from the national and strategic level of agencies down to the operational and tactical level of military units and law enforcement. Next to the dedicated intelligence organisations above, there are also temporary and part-time intelligence resources. Defence attachés and also platforms such as ships and aircraft perform intelligence collection on a temporary base or simultaneously with their normal missions. [332] These downward extensions of national level intelligence are usually not included when the intelligence community is invoked.

Contrary, in describing the organisation of national intelligence the term 'stovepiped' is commonly used. This means national intelligence is structured according to specialist intelligence collection disciplines.[333] This stovepipe structure means that SIGINT, for instance, is the domain of the National Security Agency (NSA) in America and of the Government Communications Headquarters (GCHQ) in Britain, while other agencies focus on e.g. HUMINT. Each agency is specialised in a part of the intelligence process for reasons of efficiency. The entire process therefore resembles Henry Ford's application of the conveyer belt in his car factories. The downside of this specialisation with intelligence is the compartmentalisation of gained intelligence. It is not natural to freely share intelligence scoups and risk sources and methods. Hammond takes an another, interesting, approach and states that the structure of an intelligence organisation is mainly driven by two logics: Should the organisation be centralised to optimise command and control or should it be decentralised to allow for flexibility? And, should an organisation be structured according to geographic region or by function?[334] Whatever the structure, organising intelligence, to run its daily business, results in much hierarchy and bureaucracy. Rathmell characterises this Cold War legacy of intelligence organisation as follows: *'This intelligence community shared the characteristics of other modern state and capitalist institutions. For instance, the concept of the intelligence 'factory' captured the similarity of intelligence to Fordist modes of production. The hierarchical and*

[332] Herman, *Intelligence Power in Peace and War*, 16-33.

[333] Ibid., 23; Treverton, *Reshaping National Intelligence for an Age of Information*, 7-8.

[334] Hammond, "Intelligence Organizations and the Organization of Intelligence," 696-703.

bureaucratized organisational structures of most intelligence institutions came close to the Weberian bureaucratic ideal.'[335]

The second category of actors in the intelligence landscape covers intelligence produced by private companies. Outsourcing forms a big part of intelligence. Because intelligence budget specifications are usually secret, an often invoked example is a briefing by a senior procurement executive from the US Office of the Director of National Intelligence from a 2007 conference. The briefing, titled 'Procuring the Future' revealed that 70% of the 2005 US intelligence budget of 60 billion USD was spent on outsourcing.[336] A more recent example is given by Van Puyvelde who names the US annual report on Security Clearance Determinations 2015. It shows that around 1 million intelligence contractors were provided a security clearance, making up 25% of the total of security clearances.[337] After 2015 the annual report no longer specified the personnel categories that received clearances. These two examples also show the problems of examining intelligence outsourcing: many budgets and contracts are secret and the data that is available is often of US origin due to its transparent political culture and its system of intelligence accountability. In this sense examining intelligence outsourcing suffers the same problems regarding secrecy and US prominence as intelligence studies in general.

Outsourcing can lead to new problems as well, in another example from the US, Google employees successfully protested the company's involvement in project Maven. Information on the increased use of contractors in other countries is scarcely available. The little information that exists however points towards similar developments as in the US.[338] Overall, outsourcing is a underrepresented subject in

[335] Rathmell, "Towards Postmodern Intelligence," 91.

[336] Chesterman, "'We Can't Spy... If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions'," 1055-56.

[337] Damien Van Puyvelde, Outsourcing US Intelligence: Contractors and Government Accountability, (Edinburgh: Edinburgh University Press, 2019), 1.

[338] Hamilton Bean, "Privatizing Intelligence," in *Routledge Handbook of Private Security Studies* (Routledge, 2015), 86; Van Puyvelde, *Outsourcing US Intelligence: Contractors and Government Accountability*, 8.

intelligence literature.[339] *'Academic explanation and understanding of the drivers, forms, and outcomes of private intelligence is lacking'*, according to Bean.[340]

In the literature there is consensus that outsourcing has always been part of intelligence but that 9/11 is a turning point after which contractors' involvement increased strongly. From the nineties on there was a build-up of a privatisation movement, budget and personnel cuts and the IT revolution. When intelligence needed to adapt to the War on Terror outsourcing was viewed as a more quick and flexible way to surge personnel numbers and seek expertise and knowledge that was lost or simply not available in-house.[341] Not only the number of contractors grew, the relationship between intelligence and contractor also deepened and diversified.[342] Next to logistical services, technology support and administrative tasks contractors are also involved in a variety of intelligence functions regarding collection and analysis. Contractors are working in functions that are considered very sensitive and are at the very core of intelligence such as HUMINT and briefing high level officials and commanders.[343]

The US Office of the Director of National Intelligence (ODNI) distinguishes between three types of intelligence contractors. Commercial services contractors that supply straight forward demands such as catering or guard services, commodity contractors that supply intelligence specific technology regarding satellites or computers and

---

[339] Morten Hansen, "Intelligence Contracting: On the Motivations, Interests, and Capabilities of Core Personnel Contractors in the US Intelligence Community," *Intelligence & National Security* 29, no. 1 (2014): 58; Van Puyvelde, *Outsourcing US Intelligence: Contractors and Government Accountability*, 2.

[340] Bean, "Privatizing Intelligence," 79.

[341] Hansen, "Intelligence Contracting: On the Motivations, Interests, and Capabilities of Core Personnel Contractors in the US Intelligence Community," 60; Patrick R. Keefe, "Privatized Spying: The Emerging Intelligence Industry," in *The Oxford Handbook of National Security Intelligence*, ed. Loch K. johnson (New York, NY: Oxford University Press, 2010), 298-300; Glenn J. Voelz, "Contractors and Intelligence: The Private Sector in the Intelligence Community," *International Journal of Intelligence and CounterIntelligence* 22, no. 4 (2009): 586.

[342] Van Puyvelde, *Outsourcing US Intelligence: Contractors and Government Accountability*, 76.

[343] Voelz, "Contractors and Intelligence: The Private Sector in the Intelligence Community."

contractors that augment intelligence staffs.[344] These contractors range from well-established defence industry giants such as Boeing, BAE Systems and Booz Allen Hamilton to smaller and more specialised corporations like Jane's, Stratfor and Control Risk to start-ups.[345] Intelligence outsourcing is situated against a background of broader security outsourcing and can be seen as part of the debatable military-industrial complex.[346] Critics of outsourcing view intelligence as an inherently government affair and raise questions about oversight, accountability, costs and a brain drain on government personnel.[347]

The third actor in the intelligence, intelligence studies, is young compared to other social sciences.[348] In the early years of the Cold War it emerged as a distinctly American phenomena. The culture of openness on the functioning of intelligence within a democracy in the United States helped gain its initial momentum. In contrast, the study of intelligence to learn lessons on its functioning in Britain in the same period was only done in government circles.[349] Another uniquely American characteristic is what Richards calls the 'CIA school'. This refers to the former practitioners-turned-academics, most known being Sherman Kent and Richards J. Heuer Jr., that laid the academic foundations of American intelligence.[350] During the 1980s intelligence became an academic subject in the US, UK and Canada. In the Netherlands the study of intelligence began in the 1990s with intelligence being taught as facultative module in university courses at Utrecht University and the

---

[344] Hansen, "Intelligence Contracting: On the Motivations, Interests, and Capabilities of Core Personnel Contractors in the US Intelligence Community," 60.

[345] Bean, "Privatizing Intelligence," 80-81; Van Puyvelde, *Outsourcing US Intelligence: Contractors and Government Accountability*, 95.

[346] Bean, "Privatizing Intelligence," 80. Van Puyvelde, *Outsourcing US Intelligence: Contractors and Government Accountability*, 59.

[347] Chesterman, "'We Can't Spy... If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions'," 1065-73; Hansen, "Intelligence Contracting: On the Motivations, Interests, and Capabilities of Core Personnel Contractors in the US Intelligence Community," 63.

[348] Peter Gill, "Knowing the Self, Knowing the Other," in *Handbook of Intelligence Studies*, ed. Loch K. johnson (Routledge, 2009), 82.

[349] Scott, "British Strategic Intelligence and the Cold War," 139-40; Wirtz, "The American Approach to Intelligence Studies," 29-31.

[350] Richards, "Intelligence Studies, Academia and Professionalization," 30.

University of Amsterdam, and the establishment of the Netherlands Intelligence Studies Association to promote intelligence research. In France intelligence studies also emerged in the 1990s while elsewhere on the European continent academic attention for intelligence remained low.[351] After the attacks of 9/11 interest grew resulting in literature of increased sophistication and abstraction with much emphasis on key intelligence concepts and theories.[352] Richards summarises it as follows: *'Indeed, the subject of intelligence studies itself gained significant momentum after the events of 9/11, which moved the subject beyond the simple and traditional question of how government machineries fail to spot strategic shocks before they come, and into the world of terrorism, counter-terrorism, and the changing character of conflict after the end of the Cold War. These are matters of strategy and psychology, to name but two parallel areas of study. In many ways, the postmodernity argument is as compelling for intelligence studies, as it is for any number of other disciplines.'*[353]

The number of countries outside the Anglosphere that saw intelligence studies come up in academia also increased, e.g. Romania, France, Japan, Spain, and Latin American countries.[354] Countries that already had some presence of intelligence studies prior to 9/11 matured. In the Netherlands currently both the Netherlands Defence Academy Faculty of Military Sciences and Leiden University offer a minor and master courses in intelligence.

Overall, the 'academisation of intelligence' took place during the last decades of the 20th century.[355] In this period the main journals *Intelligence and National Security* and *International Journal of Intelligence and Counter Intelligence* were founded. It also saw the establishment of organisations that promote the study in intelligence such as an Intelligence Studies Section as part of the International Studies Association. This is reflected in the growing number of articles on intelligence since 1986, as analysed in an article by Coulthart and Rorissa. They also find that the period 1950-

[351] Johnson, "The Development of Intelligence Studies," 4-7.

[352] Marrin, "Improving Intelligence Studies as an Academic Discipline," 279.

[353] Richards, "Intelligence Studies, Academia and Professionalization," 23.

[354] P. Gill and M. Phythian, "What Is Intelligence Studies?," ibid.: 13; Julian Richards, "Intelligence Studies, Academia and Professionalization," ibid.: 21.

[355] Kobi Michael and Aaron Kornbluth, "The Academization of Intelligence: A Comparative Overview of Intelligence Studies in the West," *Cyber, Intelligence, and Security* 3 (2019).

1985 only saw about a dozen articles each year, mostly from practitioner outlets such as the CIA's *Studies in Intelligence*. The period 1986-2001 saw a strong growth to a little over 100 articles in 2001. The period 2002-2020 saw an exponential growth with 4410 articles on a total of 6000 articles from 1950-2020 that the authors analysed.[356]

Intelligence studies consists of two 'dimensions' according to Gill and Phythian. At first there is the study of intelligence history, stimulated by the release of information on the role of intelligence in the Second World War and later on the Cold War. Second, the study of intelligence as a 'social science project' that draws on insights from other disciplines such as sociology, international relations and psychology *'which pose key questions about how we think about and understand intelligence—what it is, how it is conducted, by whom, with what effect, and with what degree of effective control'*.[357] This translates to four main areas of academic interest: research/historical, definitional/methodological, organisational/functional, and governance/policy.[358] The evolution of intelligence studies, its transition from the Cold War to the 21st century, is summarised by Gill and Phythian in the following table:

[356] Coulthart and Rorissa, "Growth, Diversification, and Disconnection: An Analysis of 70 Years of Intelligence Scholarship (1950-2020)."

[357] Gill and Phythian, "What Is Intelligence Studies?," 6.

[358] Ibid., 8-11.

	Early	Contemporary
Definition	Aspiring discipline.	Naturally interdisciplinary.
Focus	Narrow: strategic national intelligence.	Broad: security intelligence, including 'human'.
Conceptual concerns	How to improve analysis? The analyst-policymaker relationship. How to avoid intelligence failure?	Relationship between intelligence, state and individual. Oversight and accountability. Causes of intelligence failure.
Area focus	US/UK intelligence.	International/comparative intelligence.
Level of analysis	National.	Multi-level: organisational, national, regional, international.
Primary audience	National security practitioners, especially US.	Practitioners, policymakers, researchers, scholars, students, concerned citizens.

Table 4: The evolution of the study of intelligence.[359]

This evolution led the study of intelligence *'that now converges at a number of points with established academic disciplines'*. This convergence is seen in the former section on intelligence and science. Likewise, the growing amount of actors, and the increasing volume of articles on intelligence in the intelligence landscape is in line with the nascent widening/deepening observations from the former section.

3.6.2 Adaptation

Intelligence changes though reforms and reorganisations (see section 1.3), often following intelligence failures. As a result, there is no shortage of publications on intelligence failures since Wohlstetter's pioneering book *Pearl Harbor: Warning and Decision* (1962) on the warning failure of the Japanese attack on Pearl Harbor. Intelligence failures, and subsequent reforms of organisational structure, is the most

[359] Ibid., 15.

advanced topic within the study of intelligence.[360] However, few publications cover intelligence failures over a longer period of time with most intelligence scholars focusing on single intelligence failures and the subsequent investigations and reports.[361] The studies that do look at multiple intelligence failures usually synthesise general principles.[362] There is hardly any aggregation towards a more theorising approach on adaptation, even when article titles contain the word adaptation.[363] Compounding this is that the question how intelligence adjusts to changing circumstances is an often neglected, if not non-existent, topic within the study of public administration, political science and organisational science.[364] In its turn intelligence studies rarely draws on public administration and organisation theory scholarship.[365]

A notable exception to all this is Zegart's *Spying Blind: the CIA, the FBI, and the Origins of 9/11 (2007)*. Instead of investigating the post-mortems of 9/11, Zegart examines the 'adaptation failure' of US intelligence prior to 9/11. She regards adaptation as more than reform or change efforts. Adaptation is about change, the

---

[360] Woodrow J Kuhns, "Intelligence Failures: Forecasting and the Lessons of Epistemology," in *Paradoxes of Strategic Intelligence*, ed. Richard K. Betts and Thomas Mahnken (London: Routledge, 2003), 81.

[361] Uri Bar-Joseph and Rose McDermott, *Intelligence Success and Failure: The Human Factor* (New York, NY: Oxford University Press, 2017).

[362] e.g. Copeland, "Intelligence Failure Theory."; Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond*; Jervis, *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War*.

[363] e.g. Adam Cobb, "Intelligence Adaptation," *The RUSI Journal* 156, no. 4 (2011); John A Gentry, "Intelligence Learning and Adaptation: Lessons from Counterinsurgency Wars," *Intelligence and National Security* 25, no. 1 (2010).

[364] Lars D. Nicander, "Understanding Intelligence Community Innovation in the Post-9/11 World," *International Journal of Intelligence and Counter Intelligence* 24, no. 3 (2011): 535; Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11*, 43.

[365] Rick Caceres-Rodriguez and Michael Landon-Murray, "Charting a Research Agenda for Intelligence Studies Using Public Administration and Organization Theory Scholarship," in *Researching National Security Intelligence: Multidisciplinary Approaches*, ed. Stephen Coulthart, Michael Landon-Murray, and Damien Van Puyvelde (Washington, D.C.: Georgetown University Press, 2019), 143.

magnitude of that change and an improved relation between an organisation and its external environment. Mere change without context is meaningless because *'adaptation must be judged relatively to environmental demands'*.[366] For Zegart then, changes need to be major and have a positive effect on an organisations' dealing with its environment to constitute adaptation.

To investigate adaptation failure Zegart uses the data of 12 examinations of the US Intelligence Community between the fall of the Soviet Union in 1991 and the terrorist attacks of September 11, 2001. She found that, of 340 recommendations on improving intelligence in total, 268 (79%) resulted in no action at all. Those that saw implementation were partial or minor in nature, urged for more study instead of adopting a solution or were implemented to an unknown extent. While many issues were covered there was great consensus on four topics. Of all the recommendations 84% dealt with (1) the lack of coherence/coordination within and between intelligence agencies, and between intelligence and other government entities, (2) the lack of defining intelligence priority by senior intelligence officials and policymakers, (3) the need to strengthen HUMINT capabilities and sources and (4) the need to increase the sharing of personnel and information between agencies to increase knowledge.

The adaptation failure of US intelligence to shift from the Cold War to the increased threat of terrorism is apparent from the fact that both the 9/11 commission and Congressional Joint Inquiry came to the same four points as all the pre-9/11 investigations.[367] Rovner and Long also found some striking similarities between 9/11 investigations and earlier failures. They compared reports on the attack on Pearl Harbour, the Yom Kippur war, the fall of the shah of Iran, India's first nuclear test and the partial meltdown of nuclear power plant Three Mile Island. Rovner and Long concluded that: '*Almost all blame human error to a significant degree. Each commission found that a mindset of some sort was to blame for catastrophic failure. Each also recommended either increased centralization in response to a perceived lack of coordination in activity, or increased decentralization in response to the lack of alternative analysis of problems'.*[368]

---

[366] Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11*, 16-17, 20-21.

[367] Ibid., 27-41.

[368] Joshua Rovner and Austin Long, "The Perils of Shallow Theory: Intelligence Reform and the 9/11 Commission," *International Journal of Intelligence and Counterintelligence* 18, no. 4 (2005): 626, 27.

The data clearly points towards adaptation failure being a consistent feature in multiple events over a long period. In explaining this consistency Zegart distinguishes three sources of bureaucratic reform: *'internal reforms made by the agency itself, whether in memos, speeches, revised guidelines, or sanctions of undesired behavior; executive branch action, for example, executive orders, presidential directives, or efforts by executive branch officials outside the agency in question such as the National Security Council; and statutory reforms that require the involvement of both Congress and the executive branch. These paths suggest that impediments to adaptation are likely to emerge from both inside and outside the agency'*.[369]

Building on this, Zegart explains adaptation failure is caused by 3 factors: (1) the conservative and compartmentalised nature of intelligence organisations with standardised procedures making internal reform difficult, (2) the rational self-interest of president, legislators and government bureaucrats, which works against executive reforms because change is risky and without guaranteed rewards and (3) the fragmented structures of federal government which erects high barriers to legislative reforms.[370]

Rovner and Long provide a more theoretical explanation for adaptation failure. They refer to *Normal Accidents: Living with High-Risk Technologies* (1984) by Charles Perrow. In the book Perrow explains systems can be characterised according to the level of interrelationship between its components (coupling) and the level of interaction among these components (complexity). Tightly coupled systems, as opposed to loosely coupled, are very time-sensitive and have no delay or slack in them. A high amount of interacting components, often unobservable and/or unexpected, distinguishes complex systems from linear ones. According to Perrow, tightly coupled, complex systems are most prone to (catastrophic) failure. Measures to safeguard against failure only add to the complexity. Accidents are normal in the sense that they are unavoidable in these systems.[371] Tactical warning intelligence, according to Rovner and Long, is a tightly coupled complex system. Coming back to the observation that many post-failure reforms call for centralisation and/or decentralisation, Rovner and Long state: *'The problem with complex, tightly coupled*

[369] Zegart, *Spying Blind: The CIA, the FBI, and the Origins of 9/11*, 50.

[370] Ibid., 50-59.

[371] Charles Perrow, *Normal Accidents: Living with High-Risk Technologies*, Princeton Paperbacks (Princeton, N.J.: Princeton University Press, 1999), 62-100.

systems is that they require simultaneous centralization and decentralization. In order to deal with complexity and the unforeseen, the system should be decentralized to give operators or analysts latitude in thinking and problem-solving. At the same time, the tight coupling requires centralization to ensure prompt and coordinated response. These demands are incompatible, so no optimal organizational solution exists.'[372]

However, the optimal solution is still sought, without attention for a more contextual view that draws attention to adapting to changing circumstances. Baudet et al therefore see adaptation as central to understanding intelligence: *'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.'*[373]

With all reform efforts after each intelligence failure Zegart, Rovner and Long and Baudet et al offer compelling arguments, that are also mirrored in the case study of this research, as to why these never seem to lead to successful adaptation.

3.7 Conclusion: How did the intelligence habitus evolve?

This conclusion consists of an overall analysis for the drivers. Accompanying this text is table 3.3 with all driving forces along a timeline. The topics of the driving forces form the data for the figure.

After the Cold War ended the driver of great power politics shows an increase in international actors that compete and cooperate in an increasingly interconnected global network, maximising the effects of international (mis)conduct and broadening the forms of conflict with hybrid strategies. The driver of technology partly enables and forms power politics, but it also offers a way to understand and act in this environment. Technology is also used to increase the processing of information to speed up targeting and try to discern patterns in the growing data availability. The driver of events can be seen as the symptoms of the shifting power politics. The

[372] Rovner and Long, "The Perils of Shallow Theory: Intelligence Reform and the 9/11 Commission," 627.

[373] Baudet et al., "Military Intelligence: From Telling Truth to Power to Bewilderment?," 14.

events cause large effects in the international system and, in their turn, shape it. For intelligence this basically constitutes a series of intelligence failures that speak against any improvement, or speaks for the inevitability of failures, due to the complex and fundamentally uncertain nature of intelligence.

Making sense of these changes and uncertainty in the practice dimensions of intelligence falls to the more theoretical dimensions of the habitus. Here the question of method comes up. The question is how do social science and intelligence relate? However, this debate is lagging behind the changes and offers no approach to new problems. Specifically, the volume of critical, or postmodern, approaches to make sense of the changing habitus and the volume of transformational approaches to fundamentally alter and improve intelligence is growing, but still small too balance out the traditional approaches of realism, positivism and superficial reform efforts. The driver of institutionalisation, by nature, is the most resistant to change. This creates an imbalance among the drivers where a response to a changing world is small and lagging behind.

In conclusion, the intelligence habitus sees a growing interconnection between all external driving forces of the framework. This is not to say they never influenced each other before, or before the beginning of the time scope of this research. What has changed is the intensity and volume of interconnections. This growing interconnectedness is not sufficiently addressed by the internal drivers of intelligence. This does not mean there is no reaction to a changing environment, but it too dispersed and small in volume to call it an organisation, or system wide, adaptation. In other words, the habitus is crooked because the theory of practice does not fit the environment.

Decade	(Great) power politics	Technology	Events	Debate	Institutionalisation
1940-1950	Cold War US National Security Act Indication & Warning system Focus on Soviet military capabilities and political developments.	Machines Remote technical collection		Kent-Kendall Traditionalist-activist intelligence Positivist or a complex view on intelligence? Puzzles or mysteries?	Government (landscape) Study of intelligence reforms, reorganisation Introduction intelligence cycle
1950-1960	intentions x capabilities x activities Linear improvement of intelligence on Soviet Union.		Korean War Lack of coordination, cooperation. Much single source intelligence.		
1960-1970		Computers	Vietnam War Hamlet Evaluation System Cuban Missile Crisis Importance of all-source intelligence.		Dawn of intelligence studies
1970-1980				Intelligence as art or science?	
1980-1990			End of Cold War		
1990-2000	Peace dividend Loss of focus. Budget cuts Snakes instead of a dragon.	Revolution in Military Affairs Network Centric Warfare From C2 to C4(ISR) Less seperation between intelligence and target aquisition.			Increase in governmental intelligence customers and users.
2000-2010	War on Terror Rise of non-state actors. Interdependence of threats (failed states, terrorism, international organised crime). Less seperation between foreign and domestic intelligence. Population-centric intelligence, Human Terrain System.	Information revolution Information overload Growth of open source information environment/OSINT. Cyberspace Total Information Awareness	9/11 Still lack of coordination, cooperation. Centralisation reforms Iraq WMDs Focus on capabilities. Neglected social science intelligence.	Structured Analytic Techniques, accusations of 'scientism'. Critique on the intelligence cycle. Widening and deepening of intelligence, emergence of postmodern and critical intelligence studies. Paradigm debate	Private contractors (landscape) Growth of intelligence studies Intelligence adaptation
2010-2020	Return to great power politics Re-emergence of Russia, rise of China.	Algorithms, Project Maven Big data	Russian intervention in Ukraine Focus on hybrid warfare.	Convergence intelligence and science, proto-science with multi- and interdisciplinary approaches.	

Table 5: Overview of driving forces of the intelligence habitus.[374]

[374] Compiled by author.

4. Intelligence & Complexity

This chapter examines complexity science along the research question *How does complexity science relate to intelligence*?[375] It grounds the complexity terminology from the previous chapters and will provide an understanding of complexity to perform the case study research of the subsequent chapters. The first section starts with a review of existing intelligence literature on complexity to see how much attention is given to it, how it is combined with intelligence and what opportunities for improvement there are. This concerns publications that adopt more of complexity thinking than just terminology but cover topics that are not observed in the previous two chapters. The second section introduces complexity science in relatively general terms before the third section will explore in depth several characteristics that are an integral part of complexity science. The fourth section applies complexity science and presents three design properties to better align organisations with their complex environment. The fifth section is the conclusion.

In examining complexity, several instances of its usage in the study of war and warfare will be explored. This serves to balance against a too theoretical and abstract treatment of complexity and give an example on how complexity is used in related fields and topics.

4.1 Complexity in intelligence literature

As seen with the trinity of transformation the nexus of complexity and intelligence is not entirely new. Next to this, there are more applications of complexity present in the study of intelligence. Often this is only reflected in the terminology used in publications but several explicit theoretical approaches with more analytic depth exist as well. However, the volume of these works remains small, as described in the first chapter

To gain more insight in the nexus of complexity and intelligence already present in the existing literature, an explorative – but by no means exhaustive – search was conducted. This is based on two main sources; the WorldCat Discovery database of scientific publications and Google Scholar. This provides access to the major outlet of intelligence publications. The search queries were several combinations of the terms complex(ity), non-linear/nonlinear, intelligence (analysis). These terms have

[375] Parts of this chapter have been published in Spoor and de Werd, "Complexity in Military Intelligence."

to relate to the title of the publications and/or the key words assigned to it. In varying depth, between 100 and 300 query results per combination were scanned for anything substantive on intelligence and complexity. This was cross checked against a direct search in the databases of the following journals:

- International Journal of Intelligence and Counter Intelligence (IJIC)
- Intelligence and National Security (INS)
- The International Journal of Intelligence, Security, and Public Affairs (IJISP)
- Journal of European and American Intelligence Studies (JEAIS)
- Journal of Intelligence History (JIH)

Only 48 publications were found to match the criteria with only a few having complexity as the main topic and most treating it as a partial topic or background of the changing intelligence environment. Out of this total only 13 were articles in academic, peer-reviewed intelligence journals and 10 were academic books or book sections on intelligence. The remaining publications were spread among non-intelligence and/or non-academic journals and books, conference papers, websites, reports and theses. Although this database search is not exhaustive, it provides a good impression that the amount of publications on intelligence and complexity is quite small. This underlines the earlier observation by Beebe and Beebe.

Section 2.4 on intelligence paradigms already found that when complexity terminology is used to describe threats it often lacks theoretical and analytical depth. Rather than studying the external complexity (threats) the literature review found that the 48 selected publications focus more internally on the organisation of intelligence and changes to analysis. A complete review is not the aim here, rather a synthesis is presented to identify main themes and publications. This will be done according to three categories; organising intelligence, intelligence analysis, and the last category will present several ideas from intelligence on uncertainty that are useful for this research.

4.1.1 Organising intelligence

Two prominent perspectives on organising intelligence for complex problems are those of Treverton and Moore. Each author takes a more holistic approach and differentiate between problem types before linking this to considerations for organising intelligence. Treverton builds on Nye's puzzles and mysteries categories

(see section 2.3) and classifies intelligence problems as puzzles, mysteries and complexities, see Table 6 below.[376]

Type of issue	Description	Intelligence product
Puzzle	Answer exists but may not be known.	*The* solution.
Mystery	Answer contingent, cannot be known, but key variables can, along with sense for how they combine.	Best forecast, perhaps with scenarios or excursions.
Complexity	Many actors responding to changing circumstances, not repeating any established pattern.	'Sensemaking'? Perhaps done orally, intense interaction of intelligence and policy.

Table 6: Puzzles, mysteries, and complexities[377]

A puzzle is fairly straightforward; the question is clear and there is a finite answer but it is yet unknown. For instance, the number of North Korean nuclear weapons. Mysteries are less clear as they are about the future and therefore contingent. For instance whether North Korea will dismantle its nuclear arsenal. Mysteries have no definitive answer as they depend on multiple future variables, there are only possibilities. Still, mysteries have some shape, they are 'bounded'; it is known what variables are important for an outcome and there may be some historical evidence or theory about how they interact. Forecasts or scenarios can be created that form the space in which key variables lead to a small range of outcomes. Complexities are unbounded, they have no shape. Because there are no comparable cases or theory

[376] Gregory F. Treverton, "Addressing "Complexities" in Homeland Security," in *The Oxford Handbook of National Security Intelligence*, ed. Loch K. Johnson (New York, NY: Oxford University Press, 2010), 343-45; See also: Agrell and Treverton, *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*, 32-35.

[377] Treverton, "Addressing "Complexities" in Homeland Security," 344. Emphasis in original.

it is unclear what to look for. The key variables are also unknown. Therefore it is impossible to deliver a definitive assessment of a complex threat or even frame it in probabilities. The way to engage with complexities is through the concept of sensemaking.[378] Sensemaking will be explained in depth in section 4.4.2, but for now it is enough to define it as a collective and reflexive process to make sense of the world by creating frameworks to interpret information from, and observation of, the developing environment.

While Treverton compares his complexities to wicked problems after Rittel and Webber's 'Dilemma's in a General Theory of Planning', Moore categorises intelligence problems directly into tame and wicked problems.[379] With a tame problem there is general agreement on who or what the adversary is. A tame problem is clearly defined and its solution is obvious even though it might be difficult to achieve. Methods to solving the problem come from a small set of alternatives that can be tested against the knowledge of the systems. Wicked problems are ill-defined, there are multiple and new adversaries, defying a single solution. Any perceived solution only changes the problem as they evolve and adapt to interference making them exhibit emergent complexity. Moore therefore states complexity is a viable method to look at wicked problems. Moore places wicked problems in the same category as Treverton's mysteries.[380] Moore does not mention 'complexities' but like Treverton, Moore sees sensemaking as a method to deal with 21st century intelligence problems – it is the title and premiss of his entire book.

The differentiation of intelligence issues by Treverton and Moore goes beyond adopting mere complexity terminology. It presents a broader and descriptive framework of the topology and characterisation of intelligence problems that draws on several complexity approaches from organisational sciences or ideas that are related or have influenced complexity thinking. For instance, next to Rittel and Webber's wicked problems both authors also refer to Snowden, from who's article

[378] Ibid., 343-45.

[379] Moore, *Sensemaking: A Structure for an Intelligence Revolution*, 17-29; Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences* 4, no. 2 (1973); Treverton, "Addressing "Complexities" in Homeland Security," 345-46.

[380] Moore, *Sensemaking: A Structure for an Intelligence Revolution*, 18.

Treverton's complexities category is derived, and to Weick who introduced the idea of sensemaking in complex environments.[381]

In the search for new organisational models to adapt to the changing environment several more publications argue complexity science is useful.[382] A notable article that is firmly grounded in complexity is 'The Complexity of Peacekeeping Intelligence' by Gans.[383] Using the United Nations mission in Mali (MINUSMA) as a case study and applying complexity it shows that stabilisation operations can be seen as complex adaptive systems. Information sharing is crucial in dealing with internal and external complexity and uncertainty. However, Gans argues, the UN mission in Mali is seen and operated as a linear organisation with a formalised structure based on hierarchy and centralised decision-making. This impacts the processing of information and intelligence, and as a result the mission as a whole.

Another noteworthy publication, that also uses the UN mission in Mali, is 'Learning in complex public systems: the case of MINUSMA's intelligence organization' by De Waard et al.[384] As the title states, the article examines the learning ability of a large multi-stakeholder organisational constellation. The article finds that the combination of centralised and distributed agency substantially complicates organisational learning in MINUSMA.[385] This directly connects back to Rovner and Long's conclusion on intelligence as a complex, tightly coupled system from section 3.6.2.[386]

Andrus argues that an intelligence organisation should continuously learn and adapt to the environment. By applying concepts from complexity science, e.g. self-

[381] David Snowden, "Complex Acts of Knowing: Paradox and Descriptive Self-Awareness," *The journal of knowledge management* 6, no. 2 (2002); Karl E. Weick, *Sensemaking in Organizations* (Thousand Oaks, CA: Sage Publications, 1995).

[382] See also: "A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis," 90-92, 117-22.

[383] Ben Gans, "The Complexity of Peacekeeping Intelligence," *Journal of European and American Intelligence Studies* 1, no. 1 (2018).

[384] Erik J de Waard et al., "Learning in Complex Public Systems: The Case of Minusma's Intelligence Organization," *Public Management Review* (2021).

[385] Ibid.

[386] Rovner and Long, "The Perils of Shallow Theory: Intelligence Reform and the 9/11 Commission," 627.

organisation, emergence, and feedback, he suggests how to transform intelligence organisation.[387] Barger propagates the need for a revolution in intelligence. Current intelligence organisations are based on an industrial-age stove piped and hierarchical model. An organisational model from the information age is needed to enable flexibility and adaptability of design. Barger deems complexity can deliver this.[388] Cooper goes so far as to state US intelligence is already a complex adaptive system because it *'resembles a living ecology with a complex web of many interacting entities, dynamic relationships, non-linear feedback loops (often only partially recognized), and specific functional niches'*.[389]

4.1.2 Intelligence analysis

This second category describes publications that deal with the actual analysis of complex intelligence problems. These publications have in common that their analysis is sensitive to complexity because it emphasises the interactions between problem components where most analysis is focused on components themselves. In this regard the article 'Understanding the Non-Linear Event: A Framework for Complex Systems Analysis' by Beebe and Beebe, as already mentioned, is exceptionally rich in complexity theory.[390] To accommodate for complexity in intelligence analysis it introduces a framework to cope with non-linearity. Second to analysis of a system – breaking up the whole into its constituent parts – a diagram of all the parts and their interactions is to be visualised. This is basically a variation on the Causal Loop Diagram; a technique to visualise the interrelated agents (both actors and factors) in a system. According to Beebe and Beebe their systemic approach counters the extrapolation, or linear projection, of singular causes and effects.

Coulthart points to the importance of defining the problem, called problem structuring, like Treverton and Moore. Unlike Treverton and Moore, Coulthart,

[387] D. Calvin Andrus, "The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community," (Washington DC: Central Intelligence Agency, 2005).

[388] Barger, "Toward a Revolution in Intelligence Affairs."

[389] Cooper, "Curing Analytic Pathologies," 9.

[390] Beebe and Beebe, "Understanding the Non-Linear Event: A Framework for Complex Systems Analysis."

drawing from policy analysis, offers several analytic methods for complex problems to help analysts structure the problem.[391]

The Intelligence Preparation of the Battlefield/Environment process (IPB/IPE) – perhaps the most vivid example of *military* intelligence – is the subject of several publications. This process, also known as intelligence preparation of the operational environment (IPOE), is part of NATO intelligence doctrine and also national doctrine of many member states. It is a process and product to assess the influence of the actors and factors from the operational environment on the planning and execution of military operations. The original term 'battlefield' referred to an enemy-centric analysis in the context of major combat operations. The population-centric approach that came with the counterinsurgencies in Iraq and Afghanistan is reflected by the label 'environment' that enables a broader view of relevant conflict actors.

Carter characterises the IPB as too enemy centric with little regard for root causes of conflict, relations between actors and the human domain in general. It fails to capture the complexity of the operating environment. Therefore the operational environment should be considered as a complex adaptive system and intelligence analysis should incorporate more systems theory and systemic approaches into IPB, according to Carter.[392] Brown employs a more practice-oriented approach and applies several concepts from complexity science to the IPE process.[393] These serve as system components to examine in addition to the already existing systems. In later publications Brown, together with Pike, apply complexity to IPB in a technological way.[394] They shift the original IPB focus on threat to a population centric approach

[391] Stephen Coulthart, "What's the Problem? Frameworks and Methods from Policy Analysis for Analyzing Complex Problems," *Intelligence and National Security* 32, no. 5 (2017).

[392] Donald P. Carter, "Clouds or Clocks: The Limitations of Intelligence Preparation of the Battlefield in a Complex World," *Military Review* 96, no. 2 (2016).

[393] Eddie J. Brown, "Conveying the Complex: Updating U.S. Joint Systems Analysis Doctrine with Complexity Theory," ed. School of Advanced Military Studies and United States Army Command and General Staff College (Fort Leavenworth, KS 2013).

[394] Thomas D. Pike and Eddie J. Brown, "Complex Ipb," Smallwarsjournal.com, (accessed 16-3-2019); Eddie J. Brown and Tomas D. Pike, "Complex Intelligence Preparation of the Battlefield," in *International Studies Association Conference* (Baltimore, MD 2017). (Conference paper); See also: Victor R. Morris, "Complex

with attention to different groups and their behaviour and interactions. This is transformed into an agent-based model to examine how the system of the operational environment reacts to changes. Agent-based models are computational models of large ecosystems that enable to study the interaction and adaptation of many agents. It is a common feature in complexity research and as such several publications address it in the context of improving intelligence analysis.[395]

Menkveld focuses on the uncertainty of analysing complex intelligence problems.[396] He states the complexity of an intelligence problem can be approximated by combining the estimated number of entities involved in the problem with the estimated number of interactions. It is not about ascertaining the complexity of a single problem but the value lies in realising what factors contribute to the level of complexity. An increase in complexity (more involved entities and connections) also constitutes an increase in available, relevant intelligence. However, because relevance is not immediately obvious, increased collection does not equal an increase in relevant intelligence. This means the gap between available relevant intelligence and collected available intelligence grows exponentially with an increase of complexity. As a result the uncertainty in analysis grows.

4.1.3 Resulting uncertainty

How to engage complex problems and associated uncertainty is a central theme in complexity science and complexity approaches in other fields. There are also several ideas and concepts in intelligence that deal with uncertainty. Although these do not directly and explicitly fit this current synthesis of intelligence literature on complexity, they are very helpful in understanding the problems intelligence encounters when dealing with fundamental uncertainty as a result of complexity. Three of these ideas on uncertainty will be presented briefly: a Clausewitzian

Intelligence Preparation of the Battlefield in Ukrainian Antiterrorism Operations," *Military Review* 97, no. 1 (2017).

[395] Aaron Frank, "Computational Social Science and Intelligence Analysis," *Intelligence & National Security* 32, no. 5 (2017); Daniel Javorsek and John G. Schwitz, "Probing Uncertainty, Complexity, and Human Agency in Intelligence," ibid.29 (2014); "A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis."

[396] Christiaan Menkveld, "Understanding the Complexity of Intelligence Problems," *Intelligence and National Security* 36, no. 5 (2021).

approach to intelligence, the Rumsfeld matrix, and a critical look at intelligence hypothesis testing.

Building on the puzzle/mystery/complexity typology Agrell and Treverton compare two intelligence approaches to uncertainty based on the strategists Antoine-Henri Jomini and Carl von Clausewitz (see Table 7).

Jomini	**Clausewitz**
Goal is to eliminate uncertainty.	Goal is to assess uncertainty.
There is a 'right' answer.	'Fog of war' is inescapable.
More information and better concepts narrow uncertainty.	Single-point high-probability predictions both unhelpful and inaccurate.
Large uncertainty indicates shortcomings in analysis.	Better analysis may identify more possible outcomes.

Table 7: Jominian versus Clausewitzian Intelligence.[397]

Agrell and Treverton state that in Jomini's perception strategy is a series of problems with definite solutions. Mathematical logic could uncover fundamental principles of strategy that, if followed, could eliminate uncertainty. Contrary, Clausewitz, with his ideas of friction and fog of war, believes strategy to be about the interplay of many possibilities and thus uncertainty is a constant. For Jomini analysis is about information and the goal is to reduce uncertainty. With Clausewitz analysis begins where information ends and uncertainty can only be assessed. While intelligence pays lip service to a Clausewitzian understanding of war in practice it often seeks to eliminate uncertainty in the vein of Jomini. In other words, intelligence is tempted to turn all intelligence problems into puzzles. While a Clausewitzian approach cannot negate this temptation it can serve to improve issues of problem definition and so keep analysis from neglecting issues.[398] This leads to the (in)famous reply by then US

[397] Agrell and Treverton, *National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*, 37.

[398] Ibid., 36-39; For another contrasting perspective on Clausewitz and Jomini see: Ismael R. Rodriguez, "Uncertain About Uncertainty: Improving the

Secretary of State Donald Rumsfeld during a press conference on 12 February 2002 regarding suggestions on the absence of a link between the regime of Saddam Hussain and terrorists seeking weapons of mass destruction. Rumsfeld said *'there are known knowns: there are things we know we know. We also know there are known unknowns: that is to say we know there are some things [we know] we do not know. But there are also unknown unknowns—the ones we don't know we don't know'*.[399]

While the comment has often been ridiculed as political rhetorical obfuscation it connects to thinking about epistemic (un)certainty since Socrates and closely resembles the Johari window self-reflection method.[400] Though Rumsfeld never mentioned known unknowns, his words are often made into a matrix similar to the one below:

	Known	**Unknown**
Known	Things we know we know.	Things we know we do not know.
Unknown	Things we do not realise we know.	Things we do not know we do not know.

Table 8: The 'Rumsfeld matrix'.

Known knowns can be factual certainties or assumptions about possessed knowledge. Known unknowns are knowledge – or better, intelligence – gaps and can be seen as missing puzzle pieces (puzzles or tame problems). Unknown knowns were not mentioned by Rumsfeld but can be seen as tacit knowledge or simply failure to retrieve information from a database. Unknown unknowns are the domain of complexities (or wicked problems) where knowledge is unknown and undiscovered. Mysteries are between known unknowns and unknown unknowns as we are aware of some of their aspects but their outcome is still contingent. Attempting to reduce unknown unknowns can be framed as intelligence' aim to not miss a threat. This is

Understanding of Uncertainty in Mi Doctrine," *Military Intelligence Professional Bulletin* 37, no. 2 (2011): 40.

[399] Donald Rumsfeld, *Known and Unknown: A Memoir* (New York: Sentinel, 2011), xiii.

[400] Joseph Luft and Harry Ingham, "The Johari Window, a Graphic Model of Interpersonal Awareness," *Proceedings of the western training laboratory in group development* 246 (1955).

linked to the difference between science and intelligence when it comes to hypothesis testing. Science usually is aimed at proving causal connections. In other words, reducing the α, the chance of incorrectly concluding that there is a relation between phenomena. This is also known as a Type I error, or false positive. Intelligence is primarily concerned with not missing a threat. It seeks to reduce the β, the chance of not discovering a link between phenomena (Type II error or false negative).[401] This is especially the case with unknown unknowns where there is no previous information, conception or pattern to start from. However, while some intelligence publications touch upon β aspects – for example when covering SATs such as scenario building or red teaming – the literature on β-reasoning, let alone with regard to research design, seems to be non-existent according to De Valk.[402]

The puzzles/mysteries/complexities typology, the Jominian and Clausewitzian understandings of intelligence, the Rumsfeld matrix and a β-approach to intelligence combine into a rough cognitive map, or problem space, and associated wording that is grounded in intelligence literature to relate to complexity in the following chapters of this research. Overall, the body of literature on the convergence of complexity and intelligence is small and often discusses how complexity is applicable to intelligence on a general level. However, few publications show how intelligence can actually be improved with complexity science by applying concepts. This is not strange given the apparent novelty of complexity research into intelligence. These observations, together with the usage of complexity terminology in the Trinity of Intelligence Transformation and the evolution of the intelligence habitus from the previous chapters, strongly resemble the status of the convergence between complexity and international relations, of which intelligence studies is considered a subfield, that is described by Bousquet and Curtis in a very apt manner: *'There have […] been a number of disparate studies applying specific aspects of complexity theory to problems and debates in IR, as well as a wide range of scholarly output in which conceptual language developed to a sophisticated degree within complexity is*

[401] Giliam de Valk and Onno Goldbach, "Towards a Robust B Research Design: On Reasoning and Different Classes of Unknowns," *Journal of Intelligence History* 20, no. 1 (2021): 73; Giliam de Valk, "Case Studies into the Unknown - Logic & Tooling," *Romanian Intelligence Studies Review*, no. 21 (2019): 245.

[402] Valk and Goldbach, "Towards a Robust B Research Design: On Reasoning and Different Classes of Unknowns," 73, 74; Valk, "Case Studies into the Unknown - Logic & Tooling," 247, 52; See also: Rus Patrick, "Exploring Unknown Unknowns in Intelligence Analysis," ibid., no. 19-20 (2018): 11.

employed but a full appreciation of that underlying sophistication is absent or left unstated. Furthermore, a number of rich ontological debates have emerged within IR over the past decade that resonate with many of the characteristics of a complexity ontology, although so far these connections have been insufficiently drawn out."[403]

To avoid grounding this research on complexity without an appreciation of its sophistication the next two sections will aim for a deeper understanding.

4.2 Introducing complexity science

This section will start with comparing the terms simple, complicated, complex, and chaos – to gradually introduce concepts and associated terminology from complexity science. Next, complexity science itself is introduced. Several topics will be examined: the problems regarding a definition, its origins and ensuing scientific paradigm shift, and descriptions of complex adaptive systems. The last part of this section examines the nexus of complexity and the study of war and warfare, or military science.

4.2.1 Simple, complicated, complex, and chaos

Simple and complex are etymologically related through the Indo-European root 'plek'. In Latin it gives the verb 'plicate', which means 'to fold'. This leads to the term 'simplex' that literally translates to 'once folded' from which the English word 'simple' is derived. However 'plek' also constitutes the Latin past participle 'plexus' that means braided or intertwined and from which 'complexus', literally 'braided together', is derived.[404] It is obvious that when something is once folded, its parts are easily recognisable and can be separated but if something is intertwined this is less so.

Weaver uses the concepts of simplicity and complexity to explain the progress of science.[405] Prior to 1900, physical science was largely concerned with 'problems of simplicity', the study of problems with only two variables. Around 1900 it began to deal with problems with a great many variables: 'problems of disorganized

[403] Antoine Bousquet and Simon Curtis, "Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations," *Cambridge Review of International Affairs* 24, no. 1 (2011): 44.

[404] Murray Gell-Mann, "Let's Call It Plectics.," *Complexity Journal* 1, no. 5 (1996): 3.

[405] Warren Weaver, "Science and Complexity," *American Scientist* 36, no. 4 (1948).

complexity'. Weaver calls these problems disorganised because the variables' behaviour is individually erratic or even unknown. However, *'the system as a whole possesses certain orderly and analyzable average properties'*.[406] Probability theory and statistical mechanics allow scientific inquiry to explain and solve problems of disorganised complexity. The law of large numbers, where outliers are evened out by normal behaviour, making the average close to the expected outcome, is valid in disorganised complexity.

The middle region between problems with two variables and problems with a great amount of variables is inhibited by 'problems of organized complexity', according to Weaver. These possess a moderate amount of variables; more than two but less compared to disorganised complexity. More important, as apparent from the name, these problems, in contrast to the erratic nature of disorganised complexity, possess an organising feature. Organised complexity is about problems that deal *'simultaneously with a sizable number of factors which are interrelated into an organic whole'*.[407] Many problems in the biological, medical, psychological, economic, and political sciences are far more difficult than problems of simplicity, while at the same time they cannot be statistically explained in average behaviour. Drawing on experiences from the Second World War, Weaver saw two possible methods to deal with organised complexity: the power of computational development and the interdisciplinary approach from operation analysis. The development of science and the role of computational and mixed team approaches to tackle complex problems, are revisited later on. For now both the distinction and relation between simplicity and complexity, especially the latter's distinguishing interrelational and organisational feature, will suffice to work to understanding complexity.

Another useful and often used distinction to build understanding of complexity is the difference between complicated and complex.[408] The term complicated is often used to describe something that is difficult to understand because it consists of many parts. Star-restaurant cooking or landing a robot on Mars are complicated undertakings. They are both difficult to do but the recipe or Mars does not change.

---

[406] Ibid., 538.

[407] Ibid., 539.

[408] See, for example: John H. Miller and Scott E. Page, *Complex Adaptive Systems: An Introduction to Computational Models of Social Life* (Princeton, N.J.: Princeton University Press, 2007), 9-10.

As with disorganised complexity, the laws of physics help to solve the problem. With ample time and resources both can be accomplished and, over time, a standard procedure can be formulated. Kreienkamp and Pegram summarise the differences between complicated and complex systems in the following table:

Complicated systems	Complex systems
Complicated systems are closed, their boundaries relatively fixed, impermeable and easy to determine.	Complex systems are open, making it difficult or impossible to determine their boundaries.
Complicated systems are ordered and deterministic. They can be fully understood in terms of the properties of their component parts and they always tend towards equilibrium.	Overall behaviour of complex systems is not determined by the properties of their elements but their interactions. The system is usually far from equilibrium but without dissolving into random disorder, it exists 'at the edge of order and chaos'.
Cause and effect relationships are linear such that for each input to the system there is a proportionate output. We can identify a clear cause for each observed effect and predict system-level outcomes of change.	The relationship between cause and effect is non-linear and effects are the result of several interacting causes. Due to feedback loops, we cannot establish clear cause-and-effect relationships or predict system-level outcomes.
Complicated systems can only evolve with the help of an external force. System elements are static and not able to adapt […] on their own. If a key part of the system breaks down, the whole system will stop functioning, unable to repair itself.	Elements in a complex system are able to learn and adapt to changing conditions. Simultaneously adapting elements give rise to self-organisation. As a result, complex systems can display remarkable resilience and sometimes even continue functioning if key elements break down.
Because cause and effect relationships in complicated systems are stable over time, any kind of change is reversible.	In complex systems, change creates path dependencies that may be difficult to alter. If we could turn back time to the same starting conditions, the system is unlikely to evolve exactly the same way.

Table 9: Complicated or complex? Key differences[409]

[409] Julia Kreienkamp and Tom Pegram, "Governing Complexity: Design Principles for the Governance of Complex Global Catastrophic Risks," *International Studies Review* (2019): 7.

Chaos in scientific terms is also described as sensitive dependence on initial conditions, or sensitivity to initial conditions, meaning a small changes in input can lead to vastly different outcomes.[410] This is popularly known as 'the butterfly effect' metaphor in which the flap of a butterfly's wings in one part of the world can create a hurricane in another part, meant to illustrate the complexity and unpredictability of meteorological systems.[411] This is not the same as randomness. Where in chaos there is still a link between cause and effect, with randomness there is none. Complex systems that produce randomness are also very sensitive to initial conditions. Complexity lies between order and chaos and between order and randomness.[412]

Another method to reflect on different problems, or systems, is the Cynefin framework by Dave Snowden (Figure 3). Cynefin will be part of the analysis of the research data, see section 5.2.3. For now its use is to explain how different problems relate to each other. Cynefin consists of four domains (clear, complicated, complex, chaotic) that act as reference on how to see the world and act accordingly.[413] Cynefin is a framework meant to determine what approaches one should adopt, depending on the domain one is in or wants to move to. This is important as Cynefin is not meant to merely categorise different types of problems, but to enable moving between the domains as the situation demands; in other words, adaptation. The space between the domains is one of confusion. This is caused because one does not know in which domain one is.

[410] John H. Holland, *Emergence: From Chaos to Order* (Oxford University Press, 2010), 43. Melanie Mitchell, *Complexity: A Guided Tour* (New York, NY: Oxford University Press, 2009), 20.

[411] Edward Lorenz, "Predictability: Does the Flap of a Butterfly's Wing in Brazil Set Off a Tornado in Texas?" (paper presented at the American Association for the Advancement of Science, Cambridge, MA, 1972).

[412] Page, *Diversity and Complexity*, 32-33.

[413] R. Greenberg and B. Bertsch, eds., *Cynefin: Weaving Sense-Making into the Fabric of Our World* (Singapore: Cognitive Edge Pte Ltd, 2021); Dave Snowden and Alessandro Rancati, "Managing Complexity (and Chaos) in Times of Crisis," (Luxembourg: Publications Office of the European Union, 2021).

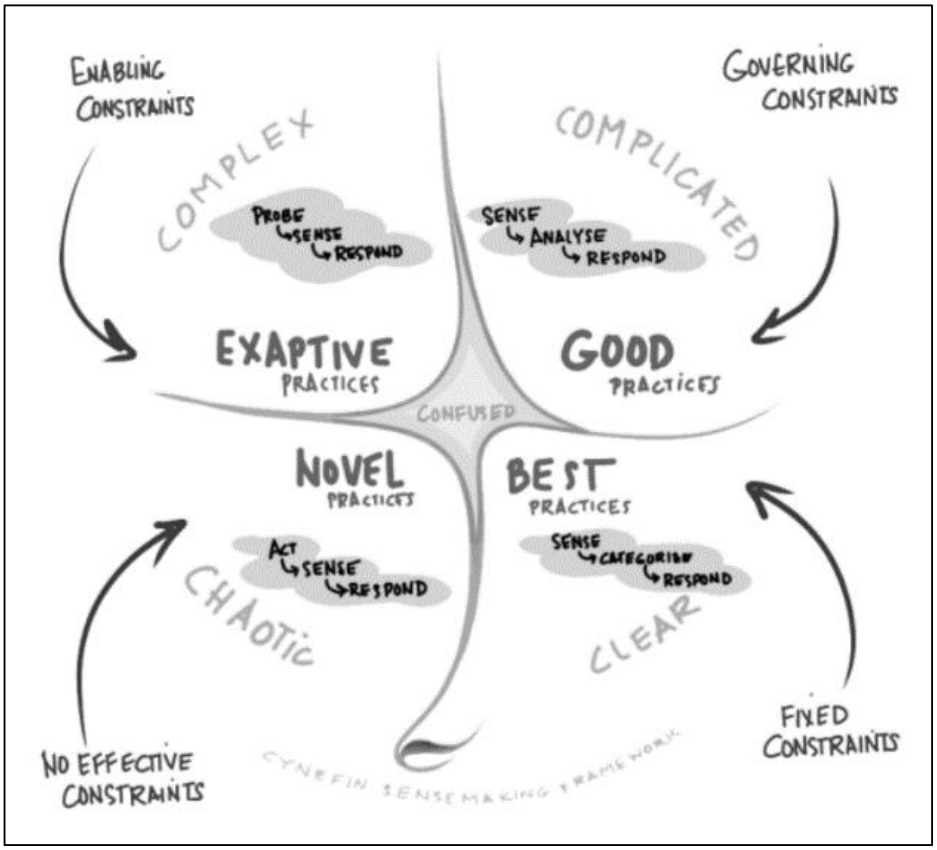


Figure 3: Cynefin framework.[414]

The four domains are expressed in three features; how well the cause and effect relations (constraints) can be observed, the type of practice that is employed, and the decision model needed to address the problem. These are discussed below.

The type of constraints for the Clear and Complicated domains constitute order. Order is constrained, meaning future outcomes are predictable as long as the constraints can be sustained. There is however also a difference between the constraints of the two domains. The fixed constraints of Clear means the relationship between cause and effect is self-evident, or clear. In a way the system is static and single-point forecasts are possible. The governing constraints in Complicated means causal relationships exist in chains that are difficult to understand. They are hidden

[414] Website The Cynefin Company, 'The Cynefin framework', accessed 6-10-2021. https://thecynefin.co/about-us/about-cynefin-framework/

or unknown, and require expertise or analysis to be discovered. Hereby the (future) state of a system is derived from its properties. Forecasts are along a range of probabilities of main-driving factors of causality, such as with scenario-planning. This is valid only as long as the system is stable. The Complex domain has enabling constraints meaning cause and effect are perceivable but not predictable because cause and effect stem from many interacting agents. This defies any description of a single and stable state of the system, rather the states of the system appear in emergent patterns. These are however not readily discernible or understood and as a result there is no clear linear causality. Forecasting or any prediction is therefore impossible but examining the system from multiple perspectives may gain knowledge on the nature of the system. Chaos means the absence of effective constraints; there are no perceivable cause and effect relations whatsoever. The system is turbulent meaning anything resembling a general understanding, let alone prediction of the system is impossible. The only knowledge is limited to feedback when interacting with the system. This knowledge is unique and only valid in the context of own actions and their particular circumstances.

The type of practice used in a domain is determined by the constraints. In the Clear domain this is best practice based on proven solutions over time from comparable clear problems and situations. Manuals and Standard Operating Procedures (SOP) ensure efficiency and consistency for proven processes. For Complicated, the expert advice and analysis needed here constitute good practices. The approach works for now but it is unknown if it is the most effective over time. In the Complex domain the emergent patterns of cause and effect require multiple perspectives to gain knowledge on the nature of the system. As a result practice is a re-purposing of existing capability, and is exaptive, or emergent. In Chaos practice is novel and accidental.

The decision models following from the constraints and the type of practice are as follows: In the Clear domain the problem input is sensed, put into existing frames of reference (categorisation) and this allows a standard response. For Complicated problems the problem input is sensed but does not fit to existing explanations. Therefore analysis of the problem is needed to respond. Complex problems lack any clear input on the situation. Instead of passively receiving input one has to probe the problem to sense its behaviour or pattern before responding. Chaotic situations defy

any sensible input, passively or actively, and therefore one has to act first to generate input. Only then can this input be sensed and responded to.[415]

It was the Cynefin framework by Snowden that inspired Treverton's 'complexities' category, and Cynefin is also mentioned several times in intelligence publications.[416] In his turn Snowden has applied Cynefin and associated thinking to intelligence such as Singapore's Risk Assessment and Horizon Scanning program.[417] While the idea of Cynefin remains the same, the framework evolves over time. For instance, earlier the Clear, Complicated, and Complex domains were expressed as known knowns, known unknowns, and unknown unknowns (Chaos being unknowable).[418] This brings Cynefin very close to the Rumsfeld matrix.[419]

The take-away is that complexity is concerned with systems with intricate dynamics, for example the workings of the human brain or the global economy. The behaviour of these systems is not determined by the properties of the individual parts but by the interaction between these parts. Out of these interactions, in a bottom-up process, the macro-level organisation emerges. In other words, complexity deals

---

[415] Cynthia F Kurtz and David J. Snowden, "The New Dynamics of Strategy: Sense-Making in a Complex and Complicated World," *IBM systems journal* 42, no. 3 (2003); Dave Snowden, "What Cynefin Is in Brief," in *Cynefin: Weaving Sense-Making into the Fabric of Our World*, ed. R. Greenberg and B. Bertsch (Singapore: Cognitive Edge Pte Ltd, 2021).

[416] Magdalena Adriana Duvenage, "Intelligence: Lessons from Knowledge Management," in *International Studies Association* (San Francisco2013); Kwa, "Postmodern Intelligence: Strategic Warning and Crisis Management," 109; James L Lawrence, "Activity-Based Intelligence: Coping with the" Unknown Unknowns" in Complex and Chaotic Environments," *American Intelligence Journal* 33, no. 1 (2016).

[417] David J Snowden and Mary E Boone, "A Leader's Framework for Decision Making," *Harvard business review* 85, no. 11 (2007): 2; Dave Snowden, "Cynefin: A Tale That Grew in the Telling," in *Cynefin: Weaving Sense-Making into the Fabric of Our World*, ed. R. Greenberg and B. Bertsch (Singapore: Cognitive Edge Pte Ltd, 2021), 46.

[418] Snowden and Boone, "A Leader's Framework for Decision Making," 7.

[419] Sonja Blignaut, "Introduction," in *Cynefin: Weaving Sense-Making into the Fabric of Our World*, ed. R. Greenberg and B. Bertsch (Singapore: Cognitive Edge Pte Ltd, 2021), 14.

with phenomena where the whole is more than the combination of its parts. This is examined further in the next section.

4.2.2 What is complexity science?

Defining research on complexity is not easy. Research on, or the study of, complexity would logically be called complexity *science*. However, the idea that there exists a single science of complexity can be disputed. Instead, there are rather several sciences that differ enough not to be considered a unified science.[420] Furthermore, the term complexity itself has many definitions, just as intelligence. *This 'reflects less a lack of agreement than an inability of any single approach to capture what scientists mean by complex'*, or intelligence for that matter.[421] Complexity *theory* is an ambiguous term as well. Capra and Luisi differentiate between scientific theory and mathematical theory. A scientific theory, is *'an explanation of a well-defined range of natural phenomena, based on systemic observation and formulated in terms of a set of consistent but approximate concepts and principles'* and a mathematical theory (citing mathematician Ian Stewart) is *'a coherent body of mathematical knowledge with a clear and consistent identity'*.[422] According to Capra and Luisi complexity theory is a mathematical theory as it is no scientific advance of itself but a basis for new scientific theories to explain non-linear phenomena.[423] Irrespective of this distinction many publications use complexity theory in a scientific theoretical meaning.

To add to the ambiguity, scientific theory itself is no clear and singular phenomenon either. For instance, there is a difference between physics and social science when it comes to matters of accuracy and truth value with regard to theoretical deductive implications, definitions, measurement and sampling sizes.[424] This does not help for the interdisciplinary approach that is (required for) the study of complexity. Therefore it is helpful to regard complexity – whether theory or science – not as a

---

[420] Mitchell, *Complexity: A Guided Tour*, 95.

[421] Page, *Diversity and Complexity*, 24.

[422] Fritjof Capra and Pier Luigi Luisi, *The Systems View of Life: A Unifying Vision* (Cambridge University Press, 2014), 98.

[423] Ibid., 89-99.

[424] Steven Bernstein et al., "God Gave Physics the Easy Problems: Adapting Social Science to an Unpredictable World," *European Journal of International Relations* 6, no. 1 (2000).

definitive and unified theoretical body but as a collection of conceptual tools that still show enough coherence and complementarity.[425] This enables a methodological pluralism that is necessary to try to understand complex issues in all their aspects.[426] This somewhat loose interpretation is how complexity in this research is seen: a toolkit of minor theories and concepts that are bounded by the idea that systems cannot be explained by their components but rather by the component's interactions, and from this, the whole becomes more than the combination of its parts. For all the ambiguity and definitional problems regarding a *science* or *theory* of complexity, this research uses complexity *science*, but will mainly just refer to complexity.

In scientific terms the idea that the whole is more than its combined parts constitutes a paradigm shift. It disrupts established ideas on how to see the world and study it. Ever since the Scientific Revolution the world was regarded as a machine that operates according to mathematical laws formed by the scientific ideas of e.g. Copernicus, Galileo, Descartes and Newton. This mechanistic universe could be studied because it works according to linear causality. Associated with this is the method of analytic thinking whereby difficult problems can be broken up into their constituent parts whose properties explain the behaviour of the whole, also known as reductionism.[427] Scientific progress however led to discoveries that are inconsistent with the mechanistic paradigm. For instance in biology, if cell development proceeds by splitting into exact copies with the same genetic information how can cells specialise and become bone cells or muscle cells? Ideas began to develop that organisation, behaviour between parts, could perhaps explain what makes the whole more than the sum of its parts. In the early 20th century the term system came in usage to denote an integrated whole whose essential properties stem from interactions between its parts. This in turn gave rise to 'systems

[425] Bousquet and Curtis, "Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations," 45; Sylvia Walby, "Complexity Theory, Systems Theory, and Multiple Intersecting Social Inequalities," *Philosophy of the Social Sciences* 37, no. 4 (2007): 456.

[426] Kurt Richardson and Paul Cilliers, "What Is Complexity Science? A View from Different Directions," (2001): 12.

[427] P. W. Anderson, "More Is Different," *Science* 177, no. 4047 (1972); Capra, *The Web of Life: A New Synthesis of Mind and Matter*, 19-20. For a more detailed account, see: Capra and Luisi, *The Systems View of Life: A Unifying Vision*, Chapters 1-3.

thinking', the idea that wholes cannot be explained by their parts but rather by their organisation in the context of the whole. Systems thinking and the closely associated concept of network – which emphasises interconnectedness and exchange rather than organisation – provided a language to define the departure from the mechanistic paradigm.[428]

One of the most influential disciplines that came from systems thinking and would heavily influence complexity is cybernetics that developed in the 1940s. Cybernetics comes from the Greek word for governance. In its modern scientific meaning it was introduced by Norbert Wiener who was inspired by war-time mechanical control systems such as servomechanisms and artillery targeting systems. Wiener developed a general theory of organisational and control relations in living and artificial systems and published it as *Cybernetics: Or Control and Communication in the Animal and the Machine* (1948). Cybernetics examines closed systems with behaviour that is *'regular, or determinate, or reproducible'*.[429] As such early cybernetics, employing an engineering approach, was interested in linear processes as this makes systems simple to build and predict. The central idea of cybernetics is the concept of feedback; reinserting results of past performance back into the system. A feedback loop is a circular connection of causally related elements in which an initial cause moves through the loop whereby each element has an effect on the next, until it feeds back into the initial element. Feedback can be self-balancing (negative) or reinforcing (positive). Negative feedback means the energy and matter produced in the feedback is absorbed again and the system keeps its balance. Conversely, positive feedback means it self-amplifies and disturbs systemic balance; it spins out of control.

Cybernetic research into self-regulation, self-control and feedback led to the concept of self-organisation, that would become central to complexity. Early cybernetics still kept close to the mechanistic paradigm.[430] This changed with the advance of what became known as the second-order cybernetics in the 1970s. Whereas the engineering approach of first-order cybernetics tends to study a system as a passive and objective 'thing' second-order cybernetics sees the system and the observer as

[428] Capra, *The Web of Life: A New Synthesis of Mind and Matter*, 24-42.

[429] Ashby, *An Introduction to Cybernetics*, 1.

[430] Capra and Luisi, *The Systems View of Life: A Unifying Vision*, 88.

interacting agents that influence the results of the observation.[431] Next to the parts to the whole shift, this disappearance of the distinction between the problem at hand and its observer also constitutes a major break with the mechanistic paradigm. The certainty of scientific knowledge is replaced with a scientific approach that acknowledges itself to be limited and approximate because the observation, or measurement, is no longer considered to be objective and absolute, but biased.

Around 1940, systems thinking and cybernetics were applied to solve practical problems. Drawing on these, the RAND corporation transformed operations research, the analysis and planning of military operations during World War 2, into systems analysis; a cost-benefit analysis that involved mathematical models to examine the best approach to meet a defined goal. Another application is system dynamics; a method for modelling and simulating systems that exhibit feedback and accumulation.[432] The causal loop diagram, mentioned several times in this research, originates from system dynamics. The common feature of all fields that sprung forth from system thinking is the concept of self-organisation. This is the idea that even though parts of a system appear to behave randomly, over time there emerges a pattern – or order. In the early concept of self-organisation from cybernetics this pattern takes place within a limited range of possibilities, or variety pool. Survival or stability of the system depends on the requisite variety, and resulting adaptability, to match against changes in the environment. This is the law of requisite variety introduced by Ashby which will be further examined in section 4.4.1.[433]

Ideas on self-organisation in the 1970s and 80s expanded the original meaning and share three characteristics, according to Capra: (1) It can lead to new structures and behaviour outside the cybernetic limited range of possibilities. (2) These new structures and behaviour can only appear in open systems that are not stable. A constant flow of energy and matter pushes such a system far from equilibrium. Only then self-organisation can happen. (3) The components of the system are connected in a non-linear fashion. This non-linear pattern results in feedback loops and is described by non-linear equations. Capra then summarises that *'self-organization is the spontaneous emergence of new structures and new forms of behaviour in open*

[431] Francis Heylighen and Cliff Joslyn, "Cybernetics and Second-Order Cybernetics," in *Encyclopedia of physical science & technology*, ed. R.A. Meyers (New York, NY: Academic Press, 2001), 3-4.

[432] Capra, *The Web of Life: A New Synthesis of Mind and Matter*, 75-76.

[433] Ashby, *An Introduction to Cybernetics*, 202-19.

systems far from equilibrium, characterized by internal feedback loops and described by nonlinear equations'.[434] The scientific developments that break with the mechanistic paradigm, laid the foundations for complexity, see Table 10.

Traditional	**Emerging**
Reductionism.	Holism.
Linear causality.	Mutual causality.
Objective reality.	Perspective reality.
Determinism.	Indeterminism.
Survival of the fittest.	Adaptive self-organization.
Focus on discrete entities.	Focus on relationship entities.
Linear relationships.	Non-linear relationships.
Newtonian physics perspectives.	Quantum physics perspectives.
World is predictable.	World is novel and probabilistic.
Modern.	Postmodern.
Focus on hierarchy.	Focus on heterarchy (within levels).
Prediction	Understanding
Based on nineteenth-century physics.	Based on biology.
Equilibrium/stability/deterministic dynamics.	Structure/pattern/self-organization/life cycles.
Focus on averages.	Focus on variation.

Table 10: Traditional versus Emerging Worldview[435]

[434] Capra, *The Web of Life: A New Synthesis of Mind and Matter*, 85.

[435] Frans P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Routledge, 2007), 88.

The theoretical development of self-organisation was only made possible in the late 20th century because the advance of the computer, and with it new mathematical tools, made it possible to model densely interconnected living systems and their non-linear dynamics. This theoretical development enabled scientists and mathematicians to develop new concepts and techniques to engage with these complex problems, coalescing into what is now known as complexity science. This theoretical development coincides, and is likely to have caused, a turn to complexity within the social sciences. This involves the adoption of ideas and methods of complexity science to social research.[436] Mesjasz distinguishes between hard and soft complexity research. Hard research involves mathematical modelling, soft research applies qualitative complexity concepts to social science research and psychology.[437] This research is soft complexity research as it concerns qualitative concepts. Intelligence, seen generally as an approximation of social science, missed the complexity turn.[438] In studying complexity, to avoid the definition issues and paradigm shifts from the previous paragraphs, many scholars prefer to write about complex systems or complex adaptive systems, often using both terms interchangeably.[439] This research does so as well. Complexity science then, is *'the study of phenomena which emerge from a collection of interacting objects'*, or, a complex system.[440]

Mitchell proposes a definition of the term complex system*: 'A system in which large networks of components with no central control and simple rules of operation give rise to complex collective behavior, sophisticated information processing, and adaptation via learning or evolution'*. She proceeds to highlight the importance of self-organisation and emergence in complex systems and, adhering to the pluriform

---

[436] Pete Barbrook-Johnson and Jayne Carrick, "Combining Complexity-Framed Research Methods for Social Research," *International Journal of Social Research Methodology* 25, no. 6 (2021): 835; For example, see: David Byrne and Gillian Callaghan, *Complexity Theory and the Social Sciences: The State of the Art* (New York: Routledge, 2013).

[437] Czeslaw Mesjasz, "Complex Systems Studies and Terrorism," *Conflict and complexity: Countering terrorism, insurgency, ethnic and regional violence* (2015): 40.

[438] Spoor and de Werd, "Complexity in Military Intelligence," 1125.

[439] Mitchell, *Complexity: A Guided Tour*, 13.

[440] Neil F. Johnson, *Simply Complexity: A Clear Guide to Complexity Theory* (London: Oneworld Publications, 2012), 3-4.

understanding of complexity, provides another definition of a complex system: *'a system that exhibits nontrivial emergent and self-organizing behaviors'*.[441] Johnson avoids giving a definition altogether. Instead he describes the workings of complex systems. For Johnson a complex system contains many interacting agents. The interactions take place because agents are in close proximity, belong to the same group or hold certain information in common. A collection of such agents with a shared aspect is a network. Therefore the study of agents and networks is an integral part of complexity science. In a network the behaviour of the agents is influenced by memory, or feedback. This means information from past experience can influence present behaviour and so agents adapt their strategies to improve performance. The system is open, so it can also be influenced by its environment. This results in system behaviour that is characteristic of complexity; The system appears to be alive. It constantly evolves and changes because of the interactions and adaptation of its agents. The behaviour of a complex system is a mix of order and disorder and it moves between these extremes on its own without any form of central control.[442] As explained briefly in chapter one a complex system consists of agents that are diverse and connected and that interact and adapt. These characteristics allow intricate and long interactions between the agents. The concept of complexity refers to the shifting patterns of these interactions, making precise repetition or prediction impossible.

Page refers to Wolfram's *A new Kind of Science* (2002) who classifies systems as producing one of four types of outcomes. While Wolfram gives his categories numbers Page characterises them as fixed points, simple structures/periodic orbits, randomness and complexity, whereby complexity is between simple structures and randomness.[443] As such, complex systems contain contradictions. They are often robust, meaning they have the ability to maintain functionality after perturbations and can resist changing conditions without adapting their initial configuration. Despite this redundant feature complex systems are also capable of producing large and catastrophic events. Complex systems can reach a state of balance, whether fixed point or simple pattern, but also produce long random sequences. Acknowledging the pluriform meaning of complexity Page gives two core principles of complexity; it lies between order and randomness, often referred to as 'the edge

[441] Mitchell, *Complexity: A Guided Tour*, 13.

[442] Johnson, *Simply Complexity: A Clear Guide to Complexity Theory*, 13-16.

[443] Stephen Wolfram, *A New Kind of Science* (Champaign, IL: Wolfram media 2002), 231, 35; in: Page, *Diversity and Complexity*, 26-27.

of chaos', and complexity cannot be easily described, evolved, engineered or predicted.[444]

4.2.3 Complexity in the study of war and warfare

This part examines complexity applications in the study of war and warfare. This is done to lessen the theoretical focus of the two previous parts and to explore how related fields deal with complexity.

The paradigm shift that is complexity and its cybernetic precursor are also described by Bousquet who, based on the mutual influence between science and warfare, distinguishes four regimes of a scientific way of warfare with chaoplexic being a combination of chaos and complex, see Table 11. These regimes represent specific theoretical and methodological underpinnings and are associated with a piece of technology as central conceptual and metaphorical phenomenon emblematic of the particular scientific frameworks.

	Mechanism	**Thermodynamics**	**Cybernetics**	**Chaoplexity**
Key technology	Clock.	Engine.	Computer.	Network.
Scientific concepts	Force, matter in motion, linearity, geometry.	Energy, entropy, probability.	Information, negentropy, negative feedback, homeostasis.	Information, non-linearity, positive feedback, self-organisation, emergence.
Form of warfare	Close order drill, rigid tactical deployments.	Mass mobilisation, motorisation, industrialisation.	Command and control, automation.	Decentralisation, swarming.

Table 11: The four regimes of the scientific way of warfare.[445]

[444] *Diversity and Complexity*, 17, 32.

[445] Antoine J. Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (London: Hurst & Company, 2009), 30.

This research is only concerned with the development from cybernetics into the chaoplexic regime. Bousquet states cybernetic war strives for complete predictability and control. Traditional command was complemented with control to keep the system of waging war in a stable condition. War was reduced to mathematical functions and cost-benefit calculations to be optimised with operations research and system analysis. As a result uncertainty and unpredictability were seen as mere information deficiencies. However, the US failure of the war in Vietnam showed cybernetic warfare did not guarantee victory.

According to Bousquet chaoplexic warfare abandons cybernetic command and control for decentralisation and self-organising networks. This is in stark contrast with the rigid hierarchy in many intelligence cultures and organisations.[446] There are more publications that use complexity to establish that war and warfare are complex phenomena, or complex adaptive systems, or that draw on complexity to examine military strategy and theory.[447] Often concepts from complexity science are shown to be applicable or phenomena from practice are viewed while drawing on complexity.

However, the real impact of complexity thinking on war(fare) is not in individual publications that combine complexity with elements of the military, be it the environment, organisation, or combat. As Lawson and Osinga both show, fundamental aspects of modern military theory are heavily influenced by

[446] Ibid., Chapters 5 & 7.

[447] David S Alberts and Thomas J Czerwinski, "Complexity, Global Politics, and National Security," (Washington D.C.: National Defense University, 1997); Yaneer Bar-Yam, "Complexity of Military Conflict: Multiscale Complex Systems Analysis of Littoral Warfare," (New England Complex Systems Institute, 2003); Andrew Ilachinski, "Land Warfare and Complexity, Part Ii: An Assessment of the Applicability of Nonlinear Dynamics and Complex Systems Theory to the Study of Land Warfare," (Alexandria, VA: Center for Naval Analyses 1996); Sean T. Lawson, *Nonlinear Science and Warfare: Chaos, Complexity and the U.S. Military in the Information Age* (Milton Park, Abingdon, Oxon: Routledge, 2014), 106-27; Steven R Mann, "Chaos Theory and Strategic Thought," *Parameters* 22 (1992); James Moffat, *Complexity Theory and Network Centric Warfare* (Washington, DC: CCRP Publication Series, 2003); Samuel Solvit, *Dimensions of War: Understanding War as a Complex Adaptive System* (Paris: L'Harmattan, 2012).

complexity.[448] In the early days of complexity several strategists among whom are John Warden and John Boyd formulated stratagems based on complexity thinking. This led to Boyd's famous OODA-loop (Observe, Orient, Decide, Act) that represents decision-making process in war (see section 4.3.4) but also manoeuvre warfare, mission command, NCW and C4ISR, see section 3.3.1. The common denominator is that both enemy and own organisations are seen as systems or networks. Physical manoeuvre and information warfare are aimed at destroying and disrupting the connections and coherence in the enemy system. This overwhelms his understanding of the battlefield and negates his adaptability.

A more recent example of the application of complexity is military design thinking.[449] As opposed to traditional linear thinking, military design thinking *'as an emerging practice evokes eclectic combinations of philosophy, social sciences, complexity theory, and often improvised, unscripted approaches in a tailored or "one of a kind" practice'*.[450] It rejects standard operating procedures and formats for mindful attention to detail in an iterative manner to adapt to changes in the problem (environment). Design thinking sees military operational art as making sense of complexity by assuming multiple perspectives (paradigms) on a problem, including reflexive examination of how the problem is framed and formulated.[451] Another, relatively, recent application of complexity in military science concerns the study of

---

[448] Lawson, *Nonlinear Science and Warfare: Chaos, Complexity and the U.S. Military in the Information Age*; Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd*, 115-21; "Organizing for Insecurity and Chaos: Resilience and Modern Military Theory," in *Netherlands Annual Review of Military Studies 2016: Organizing for Safety and Security in Military Organizations*, ed. Robert Beeres, et al. (The Hague: T.M.C. Asser Press, 2016).

[449] Cara Wrigley, Genevieve Mosely, and Michael Mosely, "Defining Military Design Thinking: An Extensive, Critical Literature Review," *She Ji: The Journal of Design, Economics, and Innovation* 7, no. 1 (2021); Ben Zweibelson, *Understanding the Military Design Movement: War, Change and Innovation* (Taylor & Francis, 2023).

[450] "An Awkward Tango: Pairing Traditional Military Planning to Design and Why It Currently Fails to Work," *Journal of military and strategic studies* 16, no. 1 (2015): 12.

[451] "'Design' Goes Dutch: Army Considerations for Unconventional Planning and Sensemaking," *Atlantisch perspectief* 39, no. 6 (2015).

peacekeeping and peacebuilding.[452] The general idea is that a peacekeeping mission takes place in a complex adaptive system. The belligerent actors, peacekeepers, and the population constitute a dynamic with non-linear interactions. As such, complexity offers an alternative to mainstream peacekeeping that has *'strong preference for linear models of change, where the input of a range of activities (e.g. patrolling, infrastructural development, technical support, training) is presumed to result in improved security and prospects for peace'*.[453] Other streams of research focus on adaptability of peacekeeping in relation to the volatile crisis situation and warring factions, or what complexity lessons there are for leading peacekeeping operations.[454]

There is criticism on the application of complexity to the study of war and warfare too. An often heard argument is that there was complexity on the battlefields of the past as well and not everything is mired in complexity today.[455] The adoption of complexity thinking into military theory and practice does not mean armed forces are turning into complex systems themselves. Kerbel argues that doctrine often uses complexity terminology far removed from its meaning in complexity science.[456] Two such doctrinal examples are the US Army Operating Concept called *Win in a Complex*

[452] e.g. Emery Brusset, Cedric De Coning, and Bryn Hughes, *Complexity Thinking for Peacebuilding Practice and Evaluation* (Springer, 2016); Cedric de Coning, Rui Saraiva, and Ako Muto, *Adaptive Peacebuilding: A New Approach to Sustaining Peace in the 21st Century* (Springer Nature, 2023).

[453] Adam Day and Charles T. Hunt, "A Perturbed Peace: Applying Complexity Theory to UN Peacekeeping," *International Peacekeeping* 30, no. 1 (2023).

[454] Soili Paananen et al., "Embracing Dynamic Tensions: Peacekeeping as a Balancing Act of Complexity," *Public Administration Review* 82, no. 6 (2022): 1169.

[455] Dale C. Eikmeier, "Simplicity: A Tool for Working with Complexity and Chaos," *Joint Force Quarterly: JFQ*, no. 92 (2019); Clay Mountcastle, "The Myth of the New Complexity," *Military Review* 96, no. 2 (2016); Harri Raisio, Alisa Puustinen, and Jaakko Jäntti, "'"The Security Environment Has Always Been Complex!": The Views of Finnish Military Officers on Complexity," *Defence Studies* 20, no. 4 (2020).

[456] Josh Kerbel, "The US Talks a Lot About Strategic Complexity. Too Bad It's Mostly Just Talk." (9-3-2021), Defenseone.com.

World and the Australian *Army's Future Land Operating Concept: Adaptive Campaigning*.[457]

4.3 Characteristics of complexity

Within complexity science many concepts and terminology are used. This section focuses on four characteristics of complexity: self-organisation, emergence, non-linearity, and adaptation. These serve to deepen the understanding of complexity but also have value of their own. Together with the concepts from the previous sections they are well suited to form the language for the following case study chapters of this research. As such the terms in this chapter will be used to operationalise interview questions for the case study research and serve as analytic lens as well.

Furthermore, apparent from their occurrences throughout the preceding pages the four characteristics lie at the very core of complexity. As with complexity, the four characteristics are not easily defined. They are interrelated which also shows from many books on complexity where they mention or refer to each other in the index. Aside from their close relation, the relative newness of the study of complexity does not help either, as Mitchell explains: *'We use words such as complexity, self-organization, and emergence to represent phenomena common to the systems in which we're interested but we can't yet characterize the commonalities in a more rigorous way. We need a new vocabulary that not only captures the conceptual building blocks of self-organization and emergence but that can also describe how these come to encompass what we call functionality, purpose, or meaning […]. These ill-defined terms need to be replaced by new, better-defined terms that reflect increased understanding of the phenomena in question.'*[458] For reasons of clarity, however, the four characteristics will be explained separately. As with the preceding section, examples from the study of war and warfare will be used to illustrate the often abstract concepts of complexity science.

---

[457] e.g. U.S. Army Training and Doctrine Command, "The U.S. Army Operating Concept: Win in a Complex World," (Fort Eustis, VA: United States Army Headquarters, 2014); Head Modernisation and Strategic Planning - Army and Australian Army Headquarters, "Army's Future Land Operating Concept: Adaptive Campaigning," (Canberra 2009).

[458] Mitchell, *Complexity: A Guided Tour*, 301.

4.3.1 Self-organisation

The first characteristic, self-organisation, means a system is not regulated by a central controller or coordinator. Instead, the entities in the system organise themselves. This does not mean there is no external influence, but it does not directly changes the organisation of the system. It is the system itself that initiates the change. This is referred to as co-evolution between a system and its environment. An adaptation of the system that is triggered by the environment, in its turn, feeds back into the environment and changes it, after which the process is repeated. The extent to which NATO co-evolved with its changing environment permeates the entire case study. As mentioned earlier, self-organisation was already touched upon by cybernetics where it refers primarily to a limited range, or variety, of self-regulatory processes. Complexity science broadens self-organisation *'to the creative, self-generated, adaptability seeking behavior of a complex system'*.[459] Self-organisation came from the natural sciences but it also applies to social systems because these also aim at maintaining a stable but dynamic mode as they incorporate new members and ideas.[460] As such the idea of self-organisation is also applied to studying terrorism.[461] This also directly relates to intelligence. If terrorist networks are self-organising this has implications for the analysis of these networks and how useful leadership targeting is.

A central idea in self-organisation is that a complex system is in a position between order and disorder, referred to as at the edge of chaos. The system is far from equilibrium but not yet in a chaotic state.[462] It is in a stable, yet temporary, position *'where the components of a system never quite lock into place, and yet never quite*

---

[459] Jeffrey Goldstein, "Emergence as a Construct: History and Issues," *Emergence* 1, no. 1 (1999): 56.

[460] Capra and Luisi, *The Systems View of Life: A Unifying Vision*, 136-37.

[461] Bousquet, "Complexity Theory and the War on Terror: Understanding the Self-Organising Dynamics of Leaderless Jihad."; e.g. Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century* (Philadelphia, PA: University of Pennsylvania Press, 2008).

[462] For more background see e.g. 'autopoiesis' in: Humberto R Maturana and Francisco J Varela, *Autopoiesis and Cognition: The Realization of the Living* (Springer Science & Business Media, 1991); And 'dissipative structures' in: Ilya Prigogine and Isabelle Stengers, *Order out of Chaos: Man's New Dialogue with Nature* (London: Flamingo, 1985).

dissolve into turbulence, either'.[463] Self-organisation means that the system is always near a state of change, or at the edge of chaos. In this state, there is always the chance that a small change can create a big or catastrophic event. This is referred to as self-organised criticality and was introduced in a paper by Bak, Tang and Wiesenfeld.[464] In the paper they presented a statistical physics experiment in which single grains of sand were dropped randomly into a pile of sand to study the dynamics of avalanche distribution. They found that most of the time small avalanches would happen but sometimes very large avalanches were caused. However, this was not according to the statistical normal distribution where one would see a bell curve when plotted in a graph. Instead the curve has a very long tail and is called a power law distribution, see Figure 4.

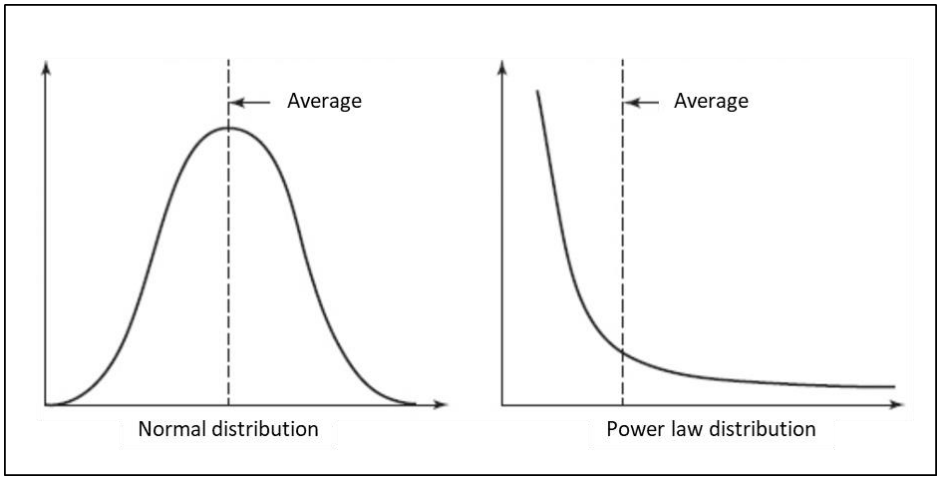


Figure 4: Normal distribution (bell curve) and power law distribution (long tail).[465]

A power law means that there is a higher probability of large events than with a normal distribution. Power laws are found with earth quakes and forest fires, but are also present in war. There are power laws in the frequency of wars related to the total number of casualties per war or force ratio of attacks related to the casualties per attack. The interesting thing is that these power laws are found regardless of

[463] Mitchell M. Waldrop, *Complexity: The Emerging Science at the Edge of Order and Chaos* (New York, NY: Simon and Schuster, 1992), 12.

[464] Per Bak, Chao Tang, and Kurt Wiesenfeld, "Self-Organized Criticality: An Explanation of the 1/F Noise," *Physical review letters* 59, no. 4 (1987).

[465] Compiled by author.

when or where conflict takes place.[466] Despite the seemingly chaotic nature of war there appear to be deeper patterns.

This is an important discovery because it enables war to be studied with the same mathematical tools that are used for other networked phenomena. It also leads to other perspectives in the study of war and with it, in intelligence. There is often a focus on trigger events or root causes but if, instead, war depends on the network of political, economic, and cultural tensions in and between societies. Forest fires are an apt analogy. The size, intensity and path of forest fires has little to do with the spark that starts them, it has more to do with drought but the biggest factor is the density (connectedness) of the forest.[467] This holds three important lessons for intelligence. First, conflict is often at the edge of chaos where seemingly small events can trigger large catastrophic events. This requires extreme flexibility in thinking because the situation is volatile and can change quickly, probably requiring a different analytic response. Furthermore, it challenges intelligence to recognise those seemingly small triggers to provide early warning. Second, qualitative analysis of social phenomena is not enough as only quantitative analysis can discover these deeper patterns and power laws. Third, whatever method or technique of analysis is used, complexity emphasises attention for the interconnections in and among phenomena rather than the phenomena themselves.

4.3.2 Emergence

The second characteristic to examine is emergence. Emergence is the formation of higher order structures and functionalities at system level, caused by interacting entities.[468] Emergence produces novel phenomena and, together with self-

[466] Aaron Clauset, "Trends and Fluctuations in the Severity of Interstate Wars," *Science advances* 4, no. 2 (2018); Johnson, *Simply Complexity: A Clear Guide to Complexity Theory*, Chapter 9; Gianluca Martelloni, Francesca Di Patti, and Ugo Bardi, "Pattern Analysis of World Conflicts over the Past 600 Years," (2018); Miller and Page, *Complex Adaptive Systems: An Introduction to Computational Models of Social Life*, 165-67; Moffat, *Complexity Theory and Network Centric Warfare*, 72-74.

[467] "Data Mining Adds Evidence That War Is Baked into the Structure of Society" (4-1-2019), MIT Technology Review, Technologyreview.com.

[468] Page, *Diversity and Complexity*, 25.

organisation, it creates new order.[469] Holland sees emergence as *'interactions where the aggregate exhibits properties not attained by summation'*.[470] As such it is overall system behaviour *'that cannot be predicted or even envisioned from the knowledge of what each component of the system does in isolation'*.[471]

Besides the impossibility of prediction, emergence is also not *'deducible from, nor reducible to the parts alone'*.[472] In a sense there is a disconnect between lower system levels/components and the aggregate outcome.[473] Emergence is a problematic concept to work with. Miller and Page state that for emergence in systems of disorganised complexity there is the law of large numbers, but an equal theorem for dealing with emergence in organised complexity is absent.[474] However, despite definitional differences the general properties that identify something as emergent according to Goldstein are[475]:

- It constitutes radical novelty; features not previously seen, or predicted.
- A certain coherence that spans and correlates separate components into higher level unity.
- The locus of emergence is at global or macro level while its components are only at the micro level.
- There are no pre-given wholes, emergence arise as systems evolve over time.
- Emergence is only recognised by showing itself (ostensively recognised).

---

[469] E. V. E. Mitleton-Kelly, "A Complexity Approach to Co-Creating an Innovative Environment," *World Futures: The Journal of General Evolution* 62, no. 3 (2006): 19.

[470] John H. Holland, *Complexity: A Very Short Introduction*, First edition. ed. (Oxford: Oxford University Press, 2014), 4. Emphasis in original.

[471] J. L. Casti, *Would-Be Worlds: How Simulation Is Changing the Frontiers of Science* (New York: J. Wiley, 1997), 82.

[472] Goldstein, "Emergence as a Construct: History and Issues," 57.

[473] Miller and Page, *Complex Adaptive Systems: An Introduction to Computational Models of Social Life*, 44.

[474] Ibid., 53.

[475] Goldstein, "Emergence as a Construct: History and Issues," 50.

An often invoked example of emergence is that wetness exists of multiple water molecules but a single molecule is not wet. This is a clear cut example from physics. For social phenomena, such as conflict, the exact point of an emergent phase transition is much more vague. When does a terrorist organisation become exactly that from what it was before? When is there enough coherence between radical people, their ideas, and willingness to perform violent acts that we call it a terrorist organisation? This requires more than mere observation, it also asks for critical reflexivity of the observer's own mental models and how these influence the observation – similar to second order cybernetics. Stated differently, beyond definitional issues there is an ontological issue. *'Are emergent phenomena part of the real, authentic "furniture of the world," or are they merely a function of our epistemological, cognitive apparatus with its ever-ready mechanism of projecting patterns on to the world?'*[476] This also asks for reflexive analysis. How do analytic thinking and methods influence the intelligence result?

Attention for reflexivity leads to different ideas on emergence. For instance strong emergence versus weak emergence. Strong emergence is the idea that higher level properties in principle cannot be derived from lower level components. This position would negate any attempts at foresight and prognostic intelligence and seems far from the reality of intelligence practice. The opposite is weak emergence. This is the idea that the relation between the whole and its parts cannot be determined for now, but only because of technical difficulties or insufficient scientific progress. This is a pragmatic argument and not as a matter of principle.[477] Or as Miller and Page state it: *'surprise and ignorance are closely related. It could be that emergent behaviour is simply reflective of scientific ignorance rather than some deeper underlying phenomenon'*.[478] This is the position of traditional intelligence and reminiscent of the idea of simply 'connecting the dots' with regard to the intelligence failure of 9/11. This idea of weak emergence is also strongly present in the case study, see section 6.3.2.

Holland sees difficulty to achieve unity in understanding emergence because of the daunting diversity of emergent phenomena. Furthermore emergence has much similarity with what he calls 'serendipitous novelty'; discoveries that are made by

[476] Ibid., 62.

[477] Capra and Luisi, *The Systems View of Life: A Unifying Vision*, 157.

[478] Miller and Page, *Complex Adaptive Systems: An Introduction to Computational Models of Social Life*, 46.

chance because the observer was looking for something else not because the discoveries are novel phenomena.[479] Interesting in this context is Treverton's idea of threat considered as covering a range. At one end are the purposive threats; terrorists and foreign states or armies that have a directed hostile intent towards a target. At the other end are systemic threats; the cumulative and harmful effect of non-hostile actions such as environmental degradation or pandemics. These are not on purpose but emerge from the total of actions in a given system.[480] Although risk would perhaps be a better term to use here and the examples given are not radically novel, they do emerge from many interacting micro-level factors.

4.3.3 Non-linearity

Self-organisation and emergence can be seen as outcomes of the non-linear dynamics of complex systems. Non-linearity is the third complexity characteristic examined in this chapter.

Non-linearity is about the relation between the interactions at the sub-system level of the entities and the system's overall behaviour.[481] These are non-linear because the whole is more than the sum of its parts. Non-linear systems have three properties[482]:

- A relative small amount of simple interactions may still give rise to unsuspected richness and diversity. Vice versa, seemingly complex and chaotic behaviour can produce ordered structures.
- There is a surprising difference in cause and effect relations because the output does not change in direct proportion to a change in any of the inputs. Small changes may give rise to large effects.
- As a result, exact prediction is often impossible.

Earlier system theories, such as cybernetics, included non-linearity to some degree in the sense that feedback loops are non-linear in nature, however these earlier theories included *'neither the "small cause, large effect", nor the intense focus on nonlinear interactivity found in emergent phenomena'*.[483] In essence, non-linearity

[479] Holland, *Emergence: From Chaos to Order*, 13.

[480] Treverton, *Reshaping National Intelligence for an Age of Information*, 43-46.

[481] Holland, *Emergence: From Chaos to Order*, 121-22.

[482] Capra and Luisi, *The Systems View of Life: A Unifying Vision*, 105.

[483] Goldstein, "Emergence as a Construct: History and Issues," 55.

refers to the unpredictable dynamics that take place between the initial conditions and emergent phenomena.

Mathematician Stanislaw Ulam is often cited regarding non-linearity of which he remarked it is equal to calling zoology *'the study of non-elephant animals'*.[484] What Ulam meant, was that linearity is the exception as scientist began to discover that non-linearity is a pervasive feature of the natural world. However, from the end of the nineteenth century scientists had developed only linear equations to model natural phenomena. Simple systems were expressed in exact, deterministic equations and systems of disorganised complexity were expressed in the equations of thermodynamics, based on the statistical analysis of average quantities.[485] Linear refers to the straight line when these equations are plotted in a graph. Contrary, complex systems are described with non-linear equations, that form a curve when plotted.[486] The advance of computers in the mid twentieth century enabled non-linear equations, which are extremely difficult to solve by head and hand, to make new models of the natural world.[487] While the whole is not the sum of its parts, the behaviour of the whole can be reduced to the lawful behaviour of its parts but only if non-linear interactions are taken into account.[488] At the same time the increased awareness of non-linearity means *'that our most useful tools for generalizing observations into theory – trend analysis, determinations of equilibria, sample means, and so on – are badly blunted'*, as Holland notes.[489] This does not mean that modelling is the only answer for scientific enquiry but there is above all a need for *'cross-disciplinary comparisons of [complex adaptive systems], in hopes of extracting common characteristics'*.[490] Intelligence, as applied social science (see section 3.5.2), should pay attention to these reservations on what non-linearity means for current methods. This also shows from the research data in section 6.3.3 with respondents

[484] James Gleick, Chaos: Making a New Science, (New York, N.Y.: Open Road Integrated Media, 2011). 139.

[485] Capra and Luisi, *The Systems View of Life: A Unifying Vision*, 104-05.

[486] Ladyman and Wiesner, *What Is a Complex System?*, 99-100.

[487] Waldrop, *Complexity: The Emerging Science at the Edge of Order and Chaos*, 64-65.

[488] Holland, *Emergence: From Chaos to Order*, 122.

[489] *Hidden Order: How Adaptation Builds Complexity*, Helix Books (Reading, MA: Perseus, 1996), 5.

[490] Ibid., 6.

problematising the causality of events in their environment in the context of a possible hybrid strategy by Russia.

A very relevant publication on non-linearity is Beyerchen's "Clausewitz, nonlinearity and the unpredictability of war".[491] Beyerchen states non-linearity permeates Clausewitz' thinking. For Beyerchen Clausewitz *'understands that seeking exact analytical solutions does not fit the nonlinear reality of the problems posed by war, and hence that our ability to predict the course and outcome of any given conflict is severely limited'*.[492] This implies a critical reflection on intelligence analysis regarding future-oriented techniques as well as applications such as Indications & Warning. In another publication Beyerchen places Clausewitz in Weaver's evolution of science from problems of simplicity to disorganised complexity to organised complexity, as discussed earlier.[493] Beyerchen argues that Clausewitz was well ahead of his time and already had a grasp of organised complexity in his thinking about war. This is very much in line with Treverton's view of Clausewitzian intelligence from section 4.1.1 and validates it as an approach for complex intelligence problems. While Clausewitz is often regarded as having a certain disdain for intelligence this is perhaps not the case. Clausewitz' perceived negative view is often based on his famous quote that in war most intelligence is contradictory, false and uncertain.[494] However, in the light of Beyerchen's articles Clausewitz' view of intelligence is perhaps better seen as a consequence of uncertainty than a general disqualification. Bousquet uses these

[491] Alan D. Beyerchen, "Clausewitz, Nonlinearity, and the Unpredictability of War," *International Security* 17, no. 3 (1992); See also: "Clausewitz and the Non-Linear Nature of Warfare: Systems of Organized Complexity," in *Clausewitz in the Twenty-First Century* ed. Hew Strachan and Andreas Herberg-Rothe (Oxford: Oxford University Press, 2007); Ralf Lillbacka, "An Outline of a Clausewitzian Theory of Intelligence," *International Journal of Intelligence and Counter Intelligence* 32, no. 3 (2019).

[492] Beyerchen, "Clausewitz, Nonlinearity, and the Unpredictability of War," 61.

[493] "Clausewitz and the Non-Linear Nature of Warfare: Systems of Organized Complexity."; Weaver, "Science and Complexity."

[494] Carl von Clausewitz, *On War*, ed. Michael Howard and Peter Paret (New York, NY: Alfred A. Knopf (Random House), 1993), 136.

Clausewitzian insights to formulate his criticism that NCW is still in part cybernetic because it sees information as absolute and true.[495]

4.3.4 Adaptation

This section further explains adaptation as the fourth, and last, characteristic of complexity. The bureaucratic adjustment of intelligence to a changing environment, or lack thereof, is addressed in section 3.6.2. While a connection with complexity theory is already briefly made there, it is conceived more generally.

Adaptation happens at the level of the entities, the system itself does not adapt. Altered behaviour by individual entities, or micro-behaviour, causes system level adaptation, or macro-behaviour. This creates a bigger range of possibilities to react to changes in the system's environment. The response-capacity to any eventuality is much bigger than with a fixed set of rules.[496] After Darwin, adaptation in a biological sense is the process whereby an organism fits itself to the environment. A record of interactions becomes enclosed in a system's structure so, over time, there forms experience and cognition. In the context of complex systems Holland extends this to include learning as well.[497] This is further expanded in complexity science with the concept of schemata. A complex system acquires information about its environment and its interaction with it. Regularities in that information are recorded into a model, called scheme, that is used to understand its environment. In psychology a scheme is a mental framework that organises data to understand the world.[498] This relates to the 'frame of reference' as mentioned with sensemaking in section 4.4.2. In this sense, for intelligence the puzzles/mysteries/complexities topology can be seen as schemata. Analysis techniques in general also function as schemata to organise intelligence.

Furthermore, schemata are not static, they are continuously combined with additional information coming from contact with the environment. Another, more concrete, example of schemata is the intelligence practice of formulating different scenario's against which new intelligence is made sense of. As such, schemata is a relevant concept for intelligence. Schemata form descriptions of observed systems, predictions of events, or a prescription for the behaviour of the complex adaptive

---

[495] Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, 220-21.

[496] Page, *Diversity and Complexity*, 25.

[497] Holland, *Hidden Order: How Adaptation Builds Complexity*, 9-10.

[498] Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd*, 98.

system itself. The results of these different schemata feed back into the system and exert 'selection pressures' whereby the viability of schemata is tested, see Figure 5.

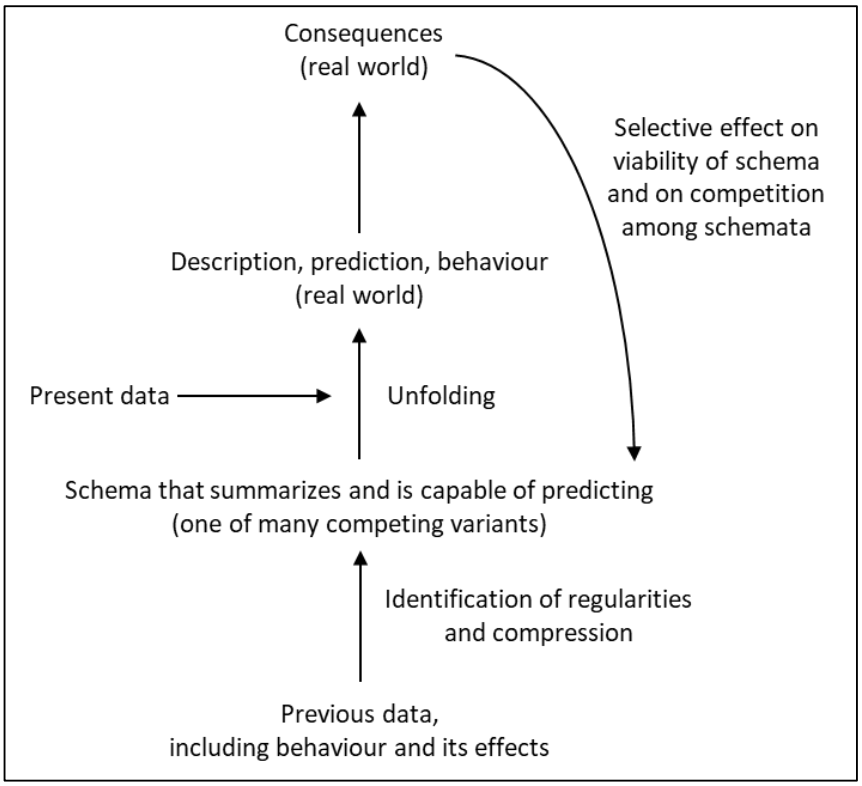


Figure 5: Adaptation of a complex system using schemata.[499]

This results in a competition among schemata in which some are demoted or eliminated and others are promoted according to their viability for understanding the environment.[500] The case study research shows that it is also possible to have a competition of schemata without result, thereby paralysing any correct response. In short, for a complex system the variety of schemata matters for its adaptive capability. For intelligence the variety of schemata matters for analytic adaptivity to

[499] Gell-Mann, *The Quark and the Jaguar: Adventures in the Simple and the Complex*, 25.

[500] Ibid., 23-24; Holland, *Hidden Order: How Adaptation Builds Complexity*, 31-32.

understand a changing, or unknown, environment. There are four forms of adaptation, described by Osinga as[501]:

1. Direct adaptation takes place as a result of the operation of a schema that is dominant at a particular time (as in a thermostat or cybernetic device). None of the behavior requires any change in the prevailing schema.

2. The next level involves changes in the schema, competition among various schemata, and the promotion or demotion depending on the action of selection pressures in the real world.

3. The third level of adaptation is the Darwinian survival of the fittest. A society may simply cease to exist as a consequence of the failure of its schemata to cope with events.

4. The fourth level is directed evolution which is caused by selection pressures exerted by individual human beings.

These four forms of adaptation all take place at different time scales.[502] When differences in time and intensity are disregarded then, at a fundamental level, evolution, adaptation and learning are all the same.[503]

Going back to schemata, their creation, demotion, or promotion is not flawless. There are also maladaptive schemata; these were once adaptive but under circumstances that are no longer prevalent. It can also be that the delay is in the mechanism that varies and selects schemata. Gell-Mann gives the example that rapidly developing situations can overtax the human ability to alter thought patterns. A maladaptive example is that, instead of changing ways of thinking, humans often cling to existing schemata and even manipulate new information to fit old

[501] Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd*, 99. After; Gell-Mann, *The Quark and the Jaguar: Adventures in the Simple and the Complex*, 292-93, 98-99.

[502] *The Quark and the Jaguar: Adventures in the Simple and the Complex*, 294.

[503] After John H. Holland in Waldrop, *Complexity: The Emerging Science at the Edge of Order and Chaos*, 146.

patterns.[504] In intelligence, among other professions, this is known as a confirmation bias.

As mentioned earlier, Boyd forms a strong connection between complexity and the study of war(fare). His OODA-loop (see Figure 6) resembles Gell-Mann's depiction of the usage of schemata in a complex system from Figure 5.[505] When discussing the Revolution in Military Affairs (RMA) and Network Centric Warfare (NCW), the loop is often invoked.[506] In a truly military interpretation the general idea is to use modern technology to speed up the OODA-loop. Going through the loop faster than the opponent is to be victorious. While this is partly true, Boyd also argued that it is about processing the evolving conflict situation and successfully adapting to it, faster than the opponent.[507] In other words, intelligence must make sense of the environment so military operations can adapt to changing circumstances. Speeding up the loop is also about overwhelming the sensemaking process of the opponent who's schemata are then behind the evolving situation.

With the misconception of the OODA loop, Bousquet formulates another topic in his critique on NCW; it has reduced OODA loop to a cybernetic decision cycle that passes info. However, Boyd stated information not only passes the system but also shapes it.[508] Bousquet's critique on the loop is similar to the observation that the intelligence cycle misses the ability to adapt, see section 2.2. As a cybernetic feedback loop the cycle only passes intelligence but is not shaped by it.

[504] Gell-Mann, *The Quark and the Jaguar: Adventures in the Simple and the Complex*, 303-04.

[505] Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, 191; Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd*, 98.

[506] Ferris, "Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?," 201.

[507] Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd*, 235-39.

[508] Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, 221.

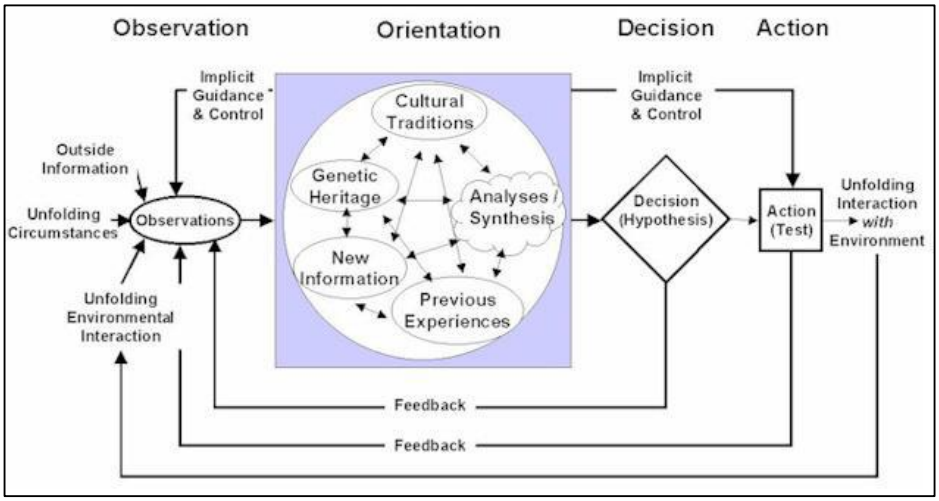


Figure 6: Boyd's OODA loop.[509]

4.4 Organising for complexity

The literature on complexity, both from complexity science proper, and fields applying it, suggest a variety of design properties a system should have to improve its relation with its environment. Three prominent design properties are the law of requisite variety, sensemaking, and organisational learning. These are described in this section. The properties are grounded in the preceding sections and are very relevant to intelligence. Together these principles form a coherence; The law of requisite variety, as the name indicates, is a precondition to understand and adapt to complex situations. By reflecting the external operational environment in the internal organisation the process of sensemaking is more effective. Organisational learning adds the actions that follow on the created situational understanding. In addition, all properties require reflexivity to explicate the role of the self in constituting these practices and achieving success.

4.4.1 Requisite variety

The first design property draws on Ashby's famous 'law of requisite variety', mentioned in section 4.2.2.[510] To reiterate, the law entails that *'for a biological or social entity to be efficaciously adaptive, the variety of its internal order must match*

[509] Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd*, 231.

[510] Ashby, *An Introduction to Cybernetics*, 202-19.

the variety of the environmental constraints'.[511] A diverse, or heterogenous system is able to produce a high degree of combinations of agents, or options (variety), for adjusting its behaviour in mirroring changes in its environment. A homogenous system, lacking diverse agents and thus variety of modes of behaviour, is far less adaptable. Because this strong relation between diversity, variety, and adaptability in constituting complexity several authors reframe the law of requisite variety as the requisite complexity that a systems needs to adapt and survive changing conditions in a complex environment.[512] Regardless, it begins with diverse agents for any variety, adaptation, or complexity to manifest.

A good stratagem to try to understand, and react to, an adversarial complex system is to have a large variety of conceptual lenses, according to Osinga.[513] This is especially true for intelligence. The real issue is to come up with such lenses. This relates directly to the diversity of the workforce in intelligence services, especially for analysts. A diverse analyst workforce results in increased variety of perceptions to understand the security environment. Diversity can be seen in two ways: in the context of a broader emancipatory call for diversity, inclusion, and equity (DEI), or as cognitive diversity. DEI concerns issues such as identity (sexual orientation, gender, ethnicity, culture), demographics (age, national origin, race), and aims for social justice and emancipation of minorities.[514] DEI literature claims that improved

---

[511] McKelvey Bill and Boisot Max, "Redefining Strategic Foresight: 'Fast' and 'Far' Sight Via Complexity Science," in *Handbook of Research on Strategy and Foresight* (Edward Elgar Publishing, 2009), 21.

[512] Yaneer Bar-Yam, *Making Things Work: Solving Complex Problems in a Complex World* (Cambridge, MA: Knowledge Press, 2004), 67-69; Max Boisot and Bill McKelvey, "Complexity and Organization-Environment Relations: Revisiting Ashby's Law of Requisite Variety," in *The Sage Handbook of Complexity and Management*, ed. Peter Allen, Steve Maguire, and Bill McKelvey (Los Angeles, CA: SAGE, 2011).

[513] Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd*, 126.

[514] e.g. Hamilton Bean and Mia Fischer, "Queering Intelligence Studies," *Intelligence and National Security* 36, no. 4 (2021); Bridget Rose Nolan, "From the "Lavender Scare" to "out and Equal": Lgbtqia+ Diversity in the U.S. Intelligence Community," *International Journal of Intelligence and CounterIntelligence* 35, no. 4 (2022); Jess Shahan, "'Don't Keep Mum": Critical Approaches to the Narratives of Women Intelligence Professionals," *Intelligence and National Security* 36, no. 4 (2021).

diversity in intelligence services results in improved performance.[515] This is based on the idea that the intelligence workforce must better reflect the society it must protect to reduce bias. On top of that, several authors also claim improved diversity is needed to better understand the increased complexity of the intelligence threat environment.[516]

However, the law of requisite variety does not mean that an equal variety is of itself an effective response, but it is necessary. The different states of the system that come from its variety must still generate effective responses that match against the environmental conditions.[517] In an intelligence context Gentry comments on those voicing more demographic diversity in intelligence services. He rejects claims that this logic, without adjustment, also applies to foreign intelligence tasks.[518] Therefore cognitive diversity is a better term. It includes identity and demographics, but also education, intellect and problem-solving skills. It is a broader concept on the different ways people think, interpret, process information, solve problems, and make decisions. Cognitive diversity better relates to the conceptual lenses, or schemata, that a system needs to have a sufficient variety of options to adapt to changes circumstances. Meanwhile, identity and demographic diversity, receive plenty attention, both in academia and practice, but cognitive diversity is understudied within intelligence.[519] Hackman et al. advocate to balance the cognitive

[515] See also: William Y Chin, "Diversity in the Age of Terror: How Racial and Ethnic Diversity in the US Intelligence Community Enhances National Security," *Fla. A & M UL Rev.* 6 (2010); T. Dao, J. Patterson, and P. Roberts, "Diversity and Inclusion: A Mission Imperative for the Intelligence Community," in *Intelligence after Next* (Mitre Centre for Technology and National Security, 2021).

[516] Mendosa, "Expanding Mental Models in Intelligence through Diverse Perspectives," 627; Damien Van Puyvelde, "Women and Black Employees at the Central Intelligence Agency: From Fair Employment to Diversity Management," *Cambridge Review of International Affairs* 34, no. 5 (2021): 30-31.

[517] Yaneer Bar-Yam, "Multiscale Variety in Complex Systems," *Complexity* 9, no. 4 (2004): 37.

[518] John A. Gentry, "Demographic Diversity in U.S. Intelligence Personnel: Is It Functionally Useful?," *International Journal of Intelligence and CounterIntelligence* 36, no. 2 (2023): 772.

[519] Irena Chiru, Cristina Ivan, and Ruben Arcos, "Diversity in Intelligence: Organizations, Processes, and People," ibid. (2022): 11.

skills of intelligence analysts working in teams.[520] Kritz shows cognitive diversity increases problem solving, working through complexity, and improves decision-making.[521] However, not much more publications exist within intelligence literature. Complexity literature contains more on the benefits of diversity, see recommendations in section 9.3. What is clear however, is that diversity has benefits for intelligence analysis. Managing workforce diversity is difficult but essential.[522] The case study also show that managing the diversity is challenging even though everybody realises its benefits.

4.4.2 Sensemaking

The second design property, sensemaking, is often used within organisation science to study complexity.[523] It originates from social psychology where it relates to processes that people use to make sense of the world. In general, sensemaking entails the social practice in which groups of people define and give meaning to their environment.[524] Sensemaking closely resembles intelligence as it is defined as *'the thinking process by which people assign meaning to experience by placing information in context to create understanding and develop beliefs about things, associations, and causality'*.[525]

Weick describes sensemaking as structuring the unknown whereby attention is given to what is constructed, how and why this takes place, and what the effects are. Sensemaking is about putting stimuli into a framework, which is often called a 'frame

[520] JR Hackman, SM Kosslyn, and AW Woolley, "The Design and Leadership of Intelligence Analysis Teams," *Unpublished Technical Report* 11 (2008).

[521] David Kritz, "Coming Together: Strengthening the Intelligence Community through Cognitive Diversity," *Global Security & Intelligence Studies* 7, no. 1 (2022).

[522] Oya Aytemiz Seymen, "The Cultural Diversity Phenomenon in Organisations and Different Approaches for Effective Cultural Diversity Management: A Literary Review," *Cross Cultural Management: An International Journal* 13, no. 4 (2006).

[523] E. H. Kramer, B. van Bezooijen, and R. Delahaij, "Sensemaking During Operations and Incidents," in *Managing Military Organizations: Theory and Practice*, ed. J. Soeters, Paul C. van Fenema, and Robert Beeres (London: Routledge, 2010), 126.

[524] Weick, *Sensemaking in Organizations*.

[525] Edward Waltz, *Quantitative Intelligence Analysis: Applied Analytic Models, Simulations, and Games* (London: Rowman & Littlefield, 2014).

of reference'. This enables comprehension, understanding, explanation, attribution, extrapolation and prediction.[526] Klein et al. describe sensemaking as follows: *'By sensemaking, modern researchers seem to mean something different from creativity, comprehension, curiosity, mental modeling, explanation, or situational awareness, although all these factors or phenomena can be involved in or related to sensemaking. Instead, sensemaking is a motivated, continuous effort to understand connections (which can be among people, places, and events) in order to anticipate their trajectories and act effectively.'*[527]

The resemblance, again, between sensemaking and intelligence is remarkable. However, sensemaking is mentioned only several times in intelligence publications and only explored in depth in publications by Moore.[528] This is all the more remarkable because sensemaking offers an alternative to traditional intelligence that operates to solve puzzles by 'connecting the dots', as the 9/11 report reads (see section 3.4.2). The traditional model is a Kentian and positivist idea of intelligence, commented on by Kendall as pulling out tape from a machine and reading it (see section 3.5.1). From a sensemaking perspective Klein et al. also take issue with this analogy of connecting the dots and point to the complexity of intelligence sensemaking: *'We've often seen this metaphorical description of cognitive work, especially in reference to the intelligence analyst's job. It trivializes cognitive work. It misses the skill needed to identify what counts as a dot in the first place. Of course relating dots is critical, but the analyst must also determine which dots are transient signals and which are false signals that should be ignored.'*[529]

---

[526] Weick, *Sensemaking in Organizations*, 4. Weick references and quotes several different authors in his explanation. For reasons of clarity only a paraphrase of Weick given.

[527] G. Klein, B. Moon, and R. R. Hoffman, "Making Sense of Sensemaking 1: Alternative Perspectives," *IEEE Intelligent Systems* 21, no. 4 (2006): 71.

[528] Moore, *Sensemaking: A Structure for an Intelligence Revolution*; David T Moore and Robert R Hoffman, "Data-Frame Theory of Sensemaking as a Best Model for Intelligence," *American Intelligence Journal* 29, no. 2 (2011); D. T. Moore et al., "Sensemaking for 21st Century Intelligence," *Journal of Intelligence History* (2020).

[529] Klein, Moon, and Hoffman, "Making Sense of Sensemaking 1: Alternative Perspectives," 72.

Compounding the difficulty in intelligence sensemaking is that the adversary is actively trying to mislead and avoid detection. Furthermore, all sorts of (cultural) bias and language barriers distort the data, or dots. In the case of hybrid threats the whole idea is to mislead and hide; *'the dots are missing because they fall below the threshold, they look different due to deception or disinformation, or are impossible to understand due to some kind of encryption'*, see also section 2.4.[530] From a post-positivist perspective it is also practically impossible to distinguish between false and true signals because these meanings are very much contextual and situated with the beholder and do not necessarily reflect the values of the opposing party. The case study will show the difficulties that emerge with values and truths when sensemaking is largely absent from the intelligence process.

4.4.3 Organisational learning

The third property for organisations to address complexity is organisational learning (see also section 3.6.2, and 'learning' throughout Chapter 4). Organisational learning is about studying how organisations sense and respond to changes in their environment. Many definitions of organisational learning exist. These can be arranged into two categories: a cognitive perspective about acquiring new knowledge, and a behavioural perspective that focuses on using this new knowledge for organisational efficacy.[531] While new knowledge can serve several objectives the initial aim is almost always behavioural change for the better.[532]

In essence organisational learning is about the relation between acquiring new knowledge and the actions that follow from it.[533] While improved performance is the ultimate goal this does not mean it follows automatically. The acquired knowledge can suffer from flaws and/or the resulting behaviour fails to bring improvement.[534] Within a security context this would be the division between an intelligence failure

[530] Sebastiaan Rietjens, *A Warning System for Hybrid Threats-Is It Possible?* (European centre of excellence for countering hybrid threats, 2020), 5.

[531] Wout Broekema, "When Does the Phoenix Rise? Factors and Mechanisms That Influence Crisis-Induced Learning by Public Organizations" (Leiden, 2018), 24.

[532] Cyril Kirwan, *Making Sense of Organizational Learning: Putting Theory into Practice* (London: Routledge, 2016), 142.

[533] Richard Freeman, "Epistemological Bricolage: How Practitioners Make Sense of Learning," *Administration & society* 39, no. 4 (2007): 490.

[534] George P. Huber, "Organizational Learning: The Contributing Processes and the Literatures," *Organization Science* 2, no. 1 (1991).

or a policy failure. Furthermore, organisational behaviour can lag behind changes in the environment. *'Evidently, this notion is highly relevant to military organizations, where the environment is to a large extent shaped by adversaries […] Moreover, the adversary will strive to adapt to the actions of the enemy and the environment as well.'*[535]

Organisational learning is the combined, or synergetic, effect of individual learning, enabling organisations to adapt to changing circumstances. For this to happen Baudet et al refer to four preconditions: (1) openness across boundaries, (2) resilience or the adaptivity of people and systems to respond to change, (3) knowledge and expertise creation and sharing, (4) a culture, systems and structures that capture learning and reward innovation.[536] Taking these preconditions into account, intelligence organisations are poor at organisational learning: '*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*.'[537] This critique relates directly to Zegart's adaptation failure from section 3.6.2. Features of it, the rotation of military personnel, learning in a non-structured way, and slow responsiveness to change, also manifest in the case study.

[535] Martijn van der Vorm, "War's Didactics a Theoretical Exploration on How Militaries Learn from Conflict," (Breda: Faculty of Military Sciences; Netherlands Defence Academy, 2021), 14-15.

[536] V.J. Marsick and K.E. Watkins, "Learning Organization," in *International Encyclopedia of Adult Education*, ed. L.M. English (London: Palgrave, 2005).

[537] Baudet et al., "Military Intelligence: From Telling Truth to Power to Bewilderment?," 15.

4.5 Conclusion: How does complexity science relate to intelligence?

This chapter shows complexity offers a radical different way than reductionism and linearity to explain phenomena and their cause and effect relations. In general, intelligence missed the complexity turn in social science. When it comes to incorporating complexity, intelligence has only just reached the point where individual publications are examining complexity for its value. Parallel to complexity approaches in international relations, a bigger debate and cumulative knowledge has yet to emerge. Formulating broadly acknowledged intelligence stratagems, let alone explicit incorporation into doctrine, is still far away. It is also good to remember here that the intelligence cycle, though under growing critique, keeps intelligence firmly placed in the cybernetic age, as seen in section 2.2. This is compounded by the almost complete absence of intelligence in the examinations of the complexity of war and warfare. If it is mentioned, it is often equated to information and any form of analysis, assessment or interpretation is ignored. The broader military sciences do apply complexity, though not all applications are explicit or rich in theoretical foundation.

The examination of existing intelligence publications offers several ideas and perspectives based on, or related to, complexity science; The puzzles/mysteries/complexities typology, Cynefin, Jominian and Clausewitzian understandings of intelligence, Rumsfeld matrix and a β-approach to intelligence combine into a rough cognitive map, or problem space, of complexity intelligence. Next to these characteristics from the intelligence-complexity nexus, the four characteristics of complexity (self-organisation, emergence, non-linearity, adaptation), and the three design properties (requisite variety, sensemaking, organisational learning) offer tools to examine the complexity of intelligence in the case study in the following chapters. How these are operationalised, is presented in the next chapter.

5. Approach to case study research

This present chapter connects the preceding theoretical chapters to the empirical part of this research; a case study into NATO Multinational Corps Northeast. It does so by presenting the methods used to examine the research question *How do military intelligence organisations deal with their complex operational environment?* In the same way that the previous chapters followed from one another according the cascading research structure (see section 1.4), this chapter follows from them. In moving from theory to practice this chapter condenses the preceding chapters into a conceptual design with which to engage practice. Where in Chapter 3 great power politics, technological developments and formative events are characterised as the practice dimensions of the intelligence habitus, this chapter builds towards examining the actual performance, or organisation, of intelligence from a complexity perspective.

This chapter is divided into two parts. The first part will present the research strategy and the underlying ontological and epistemological orientation. The second part, research design, addresses the case study approach this research applies. It closer examines the research question, the case study, and issues of data collection, analysis and research quality. The interview questions are given in Annex A. An overview of how theory is operationalised to questions is depicted in Annex B. Annex C shows how answers are coded and analysed.

5.1 Research strategy: A qualitative orientation

A research strategy is *'a general orientation to the conduct of social research'*.[538] A research strategy follows from the research question. In this case the research question is explanatory and aims to trace understanding developed over time with reflection on theory and practice. It does not aim to establish any measurements and quantification but emphasises the usage of words and the meaning of social phenomena. Therefore this research employs a qualitative approach.

Intelligence in general is undertheorised as explained in the second chapter but – more importantly, as apparent in Chapter 4 – the intersection of intelligence and complexity is even less extant. This makes generating new qualitative theory a logical step to address a niche in intelligence research and to contribute to the overall body

[538] Alan Bryman, *Social Research Methods*, Fifth edition. ed. (Oxford: Oxford University Press, 2016), 32.

of intelligence theory. Contrary, the traditional scientific method (deductive) is more poised to refine and extend existing knowledge.[539] This is what Kuhn referred to as the conduct of 'normal science'. This research is abductive in that it draws conclusions on a small empirical base. It does not seek to make a truth claim with regard to explaining the data, but it looks for a probable explanation. In doing so it follows an iterative process to match theoretical concepts and empirical data.

A research strategy also entails the ontological (what is true) and epistemological (what can be known) orientation of a research.[540] Because intelligence theories have been examined in Chapter 2, ontology and epistemology are only reviewed briefly here. Chapter 2 gave three labels for philosophical approaches that are not positivist; post-positivist, critical theory, and postmodern. As of yet this research did not explicitly adopt such a label. Post-positivism is a broad term that is applicable when the focus is on the problematisation of knowledge and not on a specific version of how the problematisation is done. This is useful when any specifics lack but it is clear that a value-based approach is concerned. For this reason the worldview of the research subjects, i.e. the interview respondents, will be either positivist or post-positivist. When talking about the specific stance of the research as the perspective of the researcher, it is postmodern. It finds that Rathmell's perception of postmodern intelligence offers a better view of intelligence (research) than a strictly positivist one. Furthermore, the pluriformity of postmodernism already has an established link with complexity, connecting it to the central topic of this research. The emancipatory agenda of a critical approach is not present in this research, but its idea of history, culture, and social positioning as constitutive forces is part of a postmodern perspective as well.

5.2 Research design: single-case study

A research design is *'the logical sequence that connects the empirical data to a study's initial research questions and, ultimately, to its conclusions'*.[541] The design of

[539] Dennis A. Gioia, Kevin G. Corley, and Aimee L. Hamilton, "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology," *Organizational research methods* 16, no. 1 (2013): 15-16.

[540] Bryman, *Social Research Methods*, 16-34.

[541] Robert K. Yin, *Case Study Research: Design and Methods*, 4th ed., 4th print. ed., Applied Social Research Methods Series ; Vol. 5 (Los Angeles: SAGE Publications, 2009), 26.

this research is a single-case study with one scientific unit of analysis; the intelligence organisation of MNC NE. However, while the unit of analysis is viewed as holistic, the military hierarchy, from headquarters to subordinate units and commands, gives a multi-level approach. This section revisits the research question and explains the case – including the rationale for the case study approach, how the empirical data is collected and analysed, and issues of research quality.

5.2.1 Research question, case selection, and secrecy

The purpose of this research is to examine intelligence through a complexity perspective. The case study is aimed at the research question *How do military intelligence organisations deal with their complex operational environment?* The case study investigates how military intelligence practitioners, that make up organisations, experience and handle complexity. The practitioners are not seen as private individuals but as members and representations of the military intelligence organisation of MNC NE. This has an effect on how the practitioners see the world. They are shaped by the organisational (sub)cultures of the military and intelligence professions that have their own norms and rules regarding uniformity, discipline, hierarchy, etc.[542] How these different (sub)cultures manifest themselves within the MNC NE intelligence organisation will emerge in the research results.

The research question is not only about to what extent they perceive complexity but also how they are equipped to address this complexity. Assuming the world is socially constructed, the qualitative focus is *'on the means by which organization members go about constructing and understanding their experience'*.[543] The intelligence cycle, intelligence theory, and paradigm debate are part, or means, of constructing and understanding, or organising, intelligence practice. Questioning practitioners on these, results in a thick description and interpretation of the world view of military intelligence practitioners. Therefore a case study approach is chosen, because it *'is*

[542] John A Gentry, "Intelligence in War: How Important Is It? How Do We Know?," *Intelligence and National Security* 34, no. 6 (2019); Jeff Rogg, "Military–Intelligence Relations: Explaining the Oxymoron," *International Journal of Intelligence and CounterIntelligence* (2023); Joseph Soeters, "Organizational Cultures in the Military," in *Handbook of the Sociology of the Military*, ed. Giuseppe Caforio and M. Nuciari (Cham, Switzerland: Springer, 2018), 836.

[543] Gioia, Corley, and Hamilton, "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology," 16.

an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context'.[544]

Furthermore, case study research enables a detailed and extensive analysis of a case. This often relates to the complexity and particular nature of the case.[545] Case study research *'focuses on understanding the dynamics present within single settings'*.[546] The interrelatedness of case and context, where it is often unclear where the border between the two is, is in line with both the postmodern approach and the complexity lens of this research. It is also very much applicable to operational military units, and intelligence in particular, as military operations are about the dynamics between the environment and the self, as is implied in the research question.

In short, with the unit of analysis being the intelligence organisation of MNC NE, the broader organisation (corps and its echelons, as well as NATO at large) is considered just as external as the operational environment. Together, the higher organisation and the operational environment, form the environment of the intelligence organisation of MNC NE. This research takes the form of a single-case study because it is interested in the dynamics within the corps' intelligence organisation (internal) as well as between the intelligence part and the higher organisation, and the operational environment (external). Other research methods are less suited for this research aim: An experiment as research method deliberately separates a phenomenon from its context. A survey is extremely limited to investigate context because it seeks to limit the variables to be analysed in order to put effort into maximising the amount of surveys to be held. A history does deal with the entanglement between phenomena and context but, as the name implies, does not deal with contemporary events.[547]

In selecting a case study the criteria, as apparent from the research question, are that it must be a military intelligence organisation, excluding civilian intelligence organisations. It must be operational, i.e. to some degree directly exposed to the environment it seeks to understand. It must be about intelligence at the level of military operations, excluding strategic or national security intelligence. Obviously, this operational environment must be complex. Furthermore, the interviews have to

---

[544] Yin, *Case Study Research: Design and Methods*, 18.

[545] Bryman, *Social Research Methods*, 60-61.

[546] Kathleen M. Eisenhardt, "Building Theories from Case Study Research," *Academy of management review* 14, no. 4 (1989): 534.

[547] Yin, *Case Study Research: Design and Methods*, 18.

take place in the working environment of the respondents so the respondents are actively living what they are talking about. This makes matters pressing and provides much colour and depth for a thick description. The condition of respondents being interviewed in their working environment of a military mission also brings several other advantages. It means that, because of the more austere working conditions and reality of working closer to a conflict, there is less bureaucracy and strict compartmentalisation than is the case with strategic intelligence and national services. This means it is more feasible to generate an overview of working relations and processes that is needed for answering the research question. A final criterion was the possibility of access. While getting access is an issue with doing interviews and field work in general, it is especially pertinent when doing research into the secret practice of intelligence. The role of secrecy in intelligence research is described shortly, for now it is enough to underline the importance of access to the point that it is practically considered a criterion.

Considering these criteria, the first and most practical consideration, would be to look for national opportunities. However, at the time the Netherlands was not actively deployed with a large number of troops to provide enough intelligence respondents. Research access to military missions, and especially their intelligence officers, of other nations deemed too difficult. NATO offered several points of access through Dutch nationals working for the alliance. The current NATO operations in Kosovo (Kosovo Force, KFOR) and Iraq (NATO Mission Iraq, NMI) do not offer enough intelligence volume – mainly because they are peace-support (KFOR), and non-combat advisory and capacity building missions (NMI). However NATO's reaction to Russia since 2014 offers other opportunities. The details of NATO's changing its posture from deterrence to defence are presented in Chapter 6. In short, for now, NATO is moving from its peace support legacy form to a warfighting form – with far reaching implications. It means NATO units and commands are being strengthened and organised to defend the alliance territory. In this changed security context and environment, NATO troops actually responsible for holding the border area against a possible Russian attack are planning and practicing to do so in quite some detail. Their environment, even with the absence of actual war, has become more operational than it ever was since the Cold War ended. Overall, the Russian

aggression against Ukraine and hybrid warfare against its member states is challenging NATO to adapt to a complex environment.[548]

This presents the situation that there are military units with a large enough intelligence organisation that is tasked to understand its complex and operational environment. This covers the criteria derived from the research question. The two other, related, criteria are that the interviews can be held at the respondents' working environment and that there already exists some form, or potential, of access. Exploring research possibilities through Dutch contributions to enhanced Forward Presence (eFP) units and NATO Force Integration Units (NFIU) in NATO states that border Russia proved difficult to realise. Then the opportunity to do research at MNC NE presented itself based on earlier contact with the corps headquarters and a contribution to an internal conference by MNC NE. As a case study the corps meets all the criteria and is a very relevant case given it is responsible for defending NATO's North-eastern flank.

As already mentioned, the big issue of research into intelligence is secrecy. While intelligence is not unique in this it poses a more severe challenge.[549] Secrecy influences *'the bounds of the possible'* in researching intelligence.[550] For instance, it *'limits research opportunities and influences key methodological choices'*.[551] Practically, this means topics regarding sources and methods are off-limits for research. Another consequence for this particular research is that the fieldwork took place in restricted working areas. Data carriers were not allowed, so interviews were recorded with pen and paper. These notes were later worked out, compared between researchers, and transcribed on a Word-file. As such, secrecy permeates the entire case study.

---

[548] *Coping with Complexity in the Euro-Atlantic Community and Beyond*. Riga Conference (Latvian Institute of International Affairs, 2016); Denis Mercier, "NATO's Adaptation in an Age of Complexity," *PRISM* 7, no. 4 (2018); Jamie Shea, "NATO in the Era of Global Complexity," *New Perspectives on Shared Security: NATO's Next 70 Years* (2019).

[549] Coulthart, Landon-Murray, and Van Puyvelde, "Introduction: A Pluralistic Approach to Intelligence Sholarship," 2.

[550] M. Phythian, "Framing the Challenges and Oppertunities of Intelligence Studies Research," ibid., 12.

[551] Damien Van Puyvelde, "The Why, Who and How of Using Qualitative Interviews to Research Intelligence Practices," ibid., 49.

Not only does secrecy impacts data collection and analysis, it also requires *'strategies of access, ethics and (data)security'*.[552] Regarding access, outside researchers often lack access because intelligence organisations remain very closed and inside contacts are hard to obtain. There is also the practical matter of needing a security clearance to even enter a working place. This was made easier because this researcher is on active duty and in possession of a security clearance. Having experience in the military and with intelligence, knowing the language, social codes, and culture also helped in establishing contact with the respondents and interviewing them. Furthermore, given the secrecy associated with intelligence work and it being a particular 'tradecraft' shared among a select few, the insider status of this researcher generated a level of trust and willingness to share information and experiences with the respondents that is unreachable for outside researchers.[553] Sjøgren et al. reflect the experience of this researcher when they state '*the researcher's position as either insider or outsider directly implicates the level of access that can be granted to them, the questions that they can ask, and, ultimately, the research that can be carried out'.*[554] All in all, especially given the context of the war in Ukraine, the possibility to do this research is unique.

There is also an ethical dimension to this trust. Intelligence researchers should always be aware of the potential damage that information gained, can do to intelligence organisations and intelligence practitioners that reveal the information. While classified information is off-limits for this research, there is still the possibility that some information gained can be sensitive or damaging nonetheless. The closeness of the researcher to the respondents, and the associated trust, has the risk that the respondents may reveal information of the sensitive or damaging kind. It is the responsibility of the researcher to guard against this by simply not talking notes, or asking if the interview at that point is still unclassified to make the respondent aware. Secrecy also requires the researcher to think about issues of data security.

---

[552] Esmé Bosma, Marieke de Goede, and Polly Pallister-Wilkins, "Introduction: Navigating Secrecy in Security Research," in *Secrecy and Methods in Security Research*, ed. Marieke De Goede, Esmé Bosma, and Polly Pallister-Wilkins (Routledge, 2020), 1.

[553] Van Puyvelde, "The Why, Who and How of Using Qualitative Interviews to Research Intelligence Practices," 56.

[554] Søren Sjøgren et al., "Military Security and Research Ethics: Using Principles of Research Ethics to Navigate Military Security Dilemmas," *Scandinavian Journal of Military Studies* 7, no. 1 (2024): 36.

For this research, the respondents remain anonymous and the data is aggregated and generalised. Administration and correspondence containing any identity information are stored on an encrypted flash drive.

5.2.2 Data collection

In the same way that the research question is leading in choosing a qualitative research strategy and case study method, it also influences the way data is collected. As previously stated, the research question is explanatory and seeks insights that developed over time from reflection on theory and practice. This requires interviews with persons involved in the events because it must be a contemporary event, as opposed to a historical event to be able to conduct interviews.[555] Going back to the research question, it requires probing respondents' experience and perspectives. This asks for enough space for the respondents to tell their own story. Yet some structure in the form of questions is needed to initiate these stories, making the interviews semi-structured.

The data collection is done according to two sets of questions, see Annex A. The first set is aimed at how military intelligence practitioners see their environment. The underlying assumption here is that this environment is complex and is characterised by self-organisation, emergence, non-linearity and adaptation – along which the questions are formulated. The second set of questions is specifically designed to question the sources about the intelligence cycle and intelligence theory. Annex B provides a more detailed account of how theory is operationalised to questions.

As stated, the respondents are seen as representing the intelligence organisation. Everything outside this is considered as external, this pertains the broader non-intelligence NATO organisation as well as the operational environment. The intelligence paradigm is seen as the dynamics between the intelligence organisation and its organisational and operational environment. While the paradigm concept was initially meant to operationalise questions, it is better suited to infer answer to other questions, and serve as analysis framework. See the last chapter for a reflection on this methodological adjustment.

[555] Yin, *Case Study Research: Design and Methods*, 9-11.

The data collection is done during six visits to MNC NE locations between May and October 2022:

- Headquarters Multinational Corps Northeast, Szczecin, Poland (two visits).
- Multinational Division Northeast, Elblag, Poland.
- Multinational Division North, Adazi, Latvia.
- NATO Force Integration Unit, Tallinn, Estonia.
- MNC NE intelligence conference, Szczecin, Poland.

Additionally, during these visits, several interviews were held with personnel from both the Polish and Latvian NFIU and eFP, and the Latvian Mechanized Infantry Brigade. The visit to the internal intelligence conference was not for pure data collection but preliminary findings were discussed, and validated.

During several of the field visits the researcher was supported by prof.dr.ir. Sebastiaan Rietjens (Szczecin 2x, Adazi and Tallinn), and by dr. Erik de Waard during the first visit to Szczecin. Different empirical data was collected during the visits. Next to interviews, data was also gathered by informal conversations, participant observations, (insight into) documents, and desk review. The interviews form the bulk of the data. The characteristics of this data are discussed next.

In this period the team conducted 49 semi-structured interviews (46 in person and three via video conference) with a total of 56 key persons (42 intelligence personnel, 14 non-intelligence). The respondents worked at nine units and commands within MNC NE, including the headquarters. They served in functions such as analysis, intelligence requirements management and collection management (IRM&CM), or command positions such as branch and section heads, e.g. intelligence production, intelligence operations, or serve as general intelligence officer. The non-intelligence respondents are from joint operations division (J3), joint plans division (J5), civil-military coordination division (CIMIC), strategic communications (STRATCOM), political advisor (POLAD), or commanders, that have staff relations with their intelligence divisions. See Table 12.

49 interviews	56 respondents	9 units/commands
46 in person.	42 intelligence.	analysis, IRM&CM, branch & section heads, general intelligence officers.
3 video conference.	14 non-intelligence.	operations, plans, CIMIC, STRATCOM, POLAD, commanders.

Table 12: Interview data characteristics.

The interviews lasted between 30 minutes and three hours, with most interviews being around 90 minutes. Most interviews are with one respondent, and several interviews were with more respondents. Of the interviews, 20 took place in Szczecin, nine in Elblag, eight in Adazi, while 12 interviews were held in Tallinn.

The respondents are all military except one civilian, and have 14 different nationalities, the biggest groups being United States (16) and five nationalities with one respondent, see Table 13.

Nationality	# Respondents
United States	16
Poland	9
Denmark	7
Estonia	6
Netherlands	4
Germany	3
Lithuania	2
Canada	2
Hungary	2
Slovakia	1

Romania	1
United Kingdom	1
Latvia	1
Croatia	1

Table 13: Number of respondents per nationality.

The rank of the respondents varies from colonel to corporal but most are major (20), see Table 14.

Rank	**# Respondents**
Major	20
Lieutenant-colonel	13
Captain	9
Colonel	3
Lieutenant	3
OR-8	2
OR-7	2
Corporal	2
OR-6	1
Civilian	1

Table 14: Number of respondents per rank.

As with intelligence, social science research aims for a triangulation of sources. Collected data is more valuable if it is corroborated by multiple sources. *'Data supported by different strategies of data collection make them much stronger and*

convincing'.[556] Therefore the interviews are supported, where relevant, with secondary research, containing popular media, practitioner and academic publications. Regarding MNC NE there is hardly any literature. The only publications that have the corps as its main subject are a research report and an article derived from it by Gareis & Vom Hagen.[557] All other publications only mention the corps as part of bigger NATO developments. Contrary, a lot is written about the operational environment of the corps, with Russian military activities as the most covered subject.

Some remarks can be made regarding interviews. While they are very suited for research that aims at a deep understanding of social phenomena, interviews are not perfect. Events or practices can be remembered inaccurately because of memory lapses, personal attitudes or political preferences.[558] Still, given the challenging nature of intelligence as a research field and the ability of interviews to conduct research in a manner that is both probing and explanatory, interviews have become increasingly common in intelligence research.[559] However, underlining the underrepresentation of military intelligence in the context of intelligence studies, empirically-based research into intelligence as part of military operations is thin.[560]

---

[556] Chiara Ruffa and Joseph Soeters, "Cross-National Research in the Military: Comparing Operational Styles," in *Routledge Handbook of Research Methods in Military Studies*, ed. Joseph Soeters, Patricia M Shields, and Sebastiaan Rietjens (Routledge, 2014), 222.

[557] Sven Bernhard Gareis et al., "Conditions of Military Multinationality the Multinational Corps Northeast in Szczecin ; Report of the Trinational Research Team Strausberg, Copenhagen, Warsaw," *Forum International* 24 (2003); Sven Bernhard Gareis and Ulrich vom Hagen, "The Difficult Practice of Military Multinationaly: The Multinational Corps Northeast in Szczecin," in *The European Armed Forces in Transition: A Comparative Analysis*, ed. Franz Kernic, Paul Klein, and Karl W. Haltiner (New York: Peter Lang, 2005).

[558] Van Puyvelde, "The Why, Who and How of Using Qualitative Interviews to Research Intelligence Practices," 50.

[559] Ibid., 48.

[560] Johnson, "The Development of Intelligence Studies," 13.

5.2.3 Data analysis

This section explains how the collected data is exactly analysed with the so called 'Gioia method' propagated by Dennis Gioia.[561] This method focuses on staying close to the words and worldview of research subjects to exclude theoretical assumptions on the side of the researcher.[562] The method performs *'extraordinary efforts to give voice to the informants in the early stages of data gathering and analysis and also to represent their voices prominently in the reporting of the research'*.[563]

The method consists of a first and second order analysis. In the first order analysis the focus is on respondent-centric terms. The interviews are conducted without any preconceived terminology or statements on the researcher's part nor do they contain directive leading questions. The goal here is to stay as close as possible to the respondents' world view and experience. While trying to avoid 'going native' and adopting the respondents' view this first order analysis comes down to making elaborate and detailed notes (thick description). In the end, by making explicit the respondents terms when formulating theory is to pursue scientific rigor and credibility.

In the second order analysis the researcher considers him/herself as a knowledgeable agent who simultaneously thinks at the level of the respondents and at a more abstract theoretical level. The second order analysis has two abstraction levels; themes and aggregate dimensions. First is the level of themes where the abstraction takes the form of trying to connect respondents' terms to existing literature and/or highlight terms that lack any firm theoretical ground. When further coding or enrichment of categories no longer provides or promises new knowledge or links to relevant existing literature the second level of abstraction investigates if it is possible to distil the emergent themes even further into 'aggregate dimensions'. Annex C presents the terms, themes, and aggregate dimensions in a table.

---

[561] Gioia, Corley, and Hamilton, "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology."

[562] Ibid., 17. e.g. ; Dennis A. Gioia and Evelyn Pitre, "Multiparadigm Perspectives on Theory Building," *The Academy of Management Review* 15, no. 4 (1990); Rajiv Nag and Dennis A. Gioia, "From Common to Uncommon Knowledge: Foundations of Firm-Specific Use of Knowledge as a Resource," *The Academy of Management Journal* 55, no. 2 (2012).

[563] Gioia, Corley, and Hamilton, "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology," 17.

The terms, themes, and dimensions provide a clear overview how the respondent's worldview connects into higher aggregate levels of observation – however it is yet not a theory. To formulate such a theory, grounded in the data, it is necessary to describe the dynamic relationships among the data, themes and dimensions and make clear all relevant raw data-to-theory connections. What needs to be established is *'that the essential concepts […] contained in the data structure are well represented in the model, but that the relational dynamics among those concepts are now made transparent'*.[564] Bryman characterises this quality of theoretical reasoning in case study research as follows: '*How well do the data support the theoretical arguments that are generated? Is the theoretical analysis incisive? For example, does it demonstrate connections between different conceptual ideas that are developed out of the data? The crucial question is not whether the findings can be generalized to a wider universe but how well the researcher generates theory out of the findings.'*[565]

To make sure the data and theory are logically connected, they are compared continuously. This enables a constant refining of emergent constructs to better match the data quality and quantity and so validate the constructs on which theory is based.[566] Practically, analysis means that when the interviews are transcribed, these transcripts are loaded into NVivo to enable digital coding. The coding results from using the Gioia method. Coding from the respondent-centric first level of analysis will be more descriptive and categorising, while the second level of analysis will produce codes that relate back to theory and concepts from Chapters 2, 3, and 4. The coding is a mix of emergent labels and existing ones that are inherent to the research questions.

The coding also includes the paradigm concept. This is inferred from answers to other questions, including questions on the intelligence cycle and intelligence theory, which concepts are also incorporated in the paradigm. Still, the idea of an intelligence paradigm is too vague to have any analytical value and generate labels from. To operationalise the idea of a paradigm (shift) the Cynefin framework, already introduced in section 4.2.1, is used. As explained there, the domains of Cynefin are based on different understandings of causality, knowledge creation and the role of

[564] Ibid., 22.

[565] Bryman, *Social Research Methods*, 64.

[566] Eisenhardt, "Building Theories from Case Study Research," 541-42.

the self. As such, they are equated with paradigms for this research. These three characteristics help to operationalise and formulate coding concerning paradigms.

5.2.4 Research quality

Regarding qualitative research in general, and case study method in particular, there are many questions and reservations with the reliability, replicability, and validity of social science when compared with the applications of these criteria, or measurements, in the natural sciences. With regard to case study research, a pertinent issue is the external validity, or generalisability. The answer to that is pretty clear according to Bryman who states *'It is important to appreciate that case study researchers do not delude themselves that it is possible to identify typical cases that can be used to represent a certain class of objects'*.[567] This seems a common understanding, also within academic intelligence studies, as *'few intelligence researchers have sought to generalize their inferences beyond the limited number of cases they looked at.'*[568] The case study here is not seen as a statistical representation of all potentially comparable units of analysis.[569] However, MNC NE being a NATO unit, works with NATO doctrine that, in different degrees, is adopted by member states, or overlaps with national doctrine. Research into a single NATO entity therefore has value for the whole of NATO, and its member states. More general, NATO intelligence doctrine, and practice, can be seen as a specific case, or variation, of the Western intelligence system as described in Chapters 2 and 3.

In other words, while full generalisability is ruled out, the sampling logic is based on the expectation that topics are present, or will emerge, that are transferable to other cases. For example, the archetypical intelligence cycle is a widespread conceptualisation of intelligence, and military intelligence in general tends to follow it. The cycle is very often used by respondents to describe their work and is also widely used by NATO and many Western intelligence organisations. Therefore an examination of the intelligence cycle within the MNC NE intelligence organisation has much value for other intelligence organisations.

Another way to ensure the credibility of this research's findings is using multiple sources, as is already explained. Being a qualitative case study this research is concerned with in depth investigation of phenomenon within their context. This

---

[567] Bryman, *Social Research Methods*, 62.

[568] Van Puyvelde, "The Why, Who and How of Using Qualitative Interviews to Research Intelligence Practices," 51.

[569] Yin, *Case Study Research: Design and Methods*, 54-56.

requires a rich account of the culture regarding the subject. This is known as a 'thick description' that acts as a way to judge issues of transferability, or relatability, of findings to other settings. The road to this thick description, consisting of e.g. concepts and their explanations used in the semi-structured interviews, transcripts and the methods used for analysis, are kept and archived. This is done to establish an audit trail that provides a look beneath the final result and to scrutinise the road taken should any other researcher wish to do so.

Next to the description being 'thick' another quality indicator is its coherence. Does the research logically links its questions to appropriate methods to findings and to conclusions? The interview process, where most interviews were done with at least two researchers who both made notes, is another quality indicator – as is the volume of interviews and respondents. From the 49 interviews, nine were done by only the lead researcher, ten were held with three interviewers and the remaining thirty were done with two interviewers.

An initial report with the research findings was provided to five respondents and four of their colleagues who were not interviewed. The initial report was checked for security issues and factual errors only. While this is inherent in the choice to examine the intelligence organisation of MNC NE, only several revisions were deemed necessary but these rather meant taking away several details without impacting overall results. This member check, or respondent validation, further solidifies the credibility of the research results.

The final criterion to ensure the quality of this research stems from its postmodern stance and is called reflexivity. It is about acknowledging and mentioning the role of the researcher and his/her particular position in social space and the implications this can have on the knowledge construction of the research.[570] The researchers' knowledge of and proximity to the practice of intelligence are obviously of influence, as already mentioned in section 5.2.1. Next to enabling access that is not available to others, this can also have negative consequences. The position of the researcher brings with it inherent bias. This is a scientific constant but even more so when the researcher is closely connected to the research subject and case study as with this particular research. More important, closeness of the researcher to the subject can lead to emotional involvement or preconceptions and interpretations too far

[570] For a detailed account of alternative criteria for qualitative evaluation, see: Bryman, *Social Research Methods*, 384-90.

removed from the respondent's data. This is countered by staying close to the idea of thick description and the wording of the respondents explaining their worldview.

6. Case study, part I; case introduction & environment

This first chapter of the case study consists of three parts. First, Multinational Corps Northeast (MNC NE) is introduced. The second section describes the environment of the intelligence organisation of MNC NE. This description is respondent-centric and reflective of the terms used by the respondents during the interviews (first order). The third section is researcher-centric and provides an analysis on higher-level themes (second order) by connecting empirical data with existing scientific theory. The fourth section presents a subconclusion. The organisation of intelligence itself, within the environment described in this chapter, is presented in the next two chapters.

6.1 Case study introduction

The case study is introduced in two parts. The first part situates MNC NE in the current international security environment. The second part describes MNC NE and its intelligence organisation.

6.1.1 Setting

The war in Ukraine is a daily reality for MNC NE. The corps is the focal point for the NATO response against the Russian aggression against Ukraine. This is logical as the corps' mission is to defend Poland and the Baltic States that share borders with Russia and the Kaliningrad oblast, Belarus, and Ukraine. This has resulted in significant changes of MNC NE's role and force structure. These changes are part of NATO's Readiness Action Plan (RAP) that was rectified at the 2014 Wales summit and developed during subsequent NATO summits. The RAP is to ensure a swift and firm alliance response to new security challenges and resulted in significant reinforcements of NATO's collective defence.[571] The plan includes assurance measures for NATO allies in Central and Eastern Europe such as exercises focused on collective defence and crisis management.

[571] Website NATO Supreme Headquarters Allied Powers Europe, 'Readiness Action Plan', accessed 12-12-2021. https://shape.nato.int/readiness-action-plan

The RAP also entails adaptation measures that are to support NATO forces and command structure.[572] The measures relevant to MNC NE are:

- Establishment of NATO Force Integration Units (NFIUs) – small headquarters – to enable fast reception of NATO units into North-eastern Europe.
- Increased readiness and capabilities of headquarters Multinational Corps Northeast.
- Establishment of enhanced Forward Presence (eFP) consisting of four multinational battle groups in Poland and the Baltic States.
- Establishment of Multinational Division Northeast (MND NE) in Elblag, Poland in 2017 to coordinate the activities in the NATO battlegroups in Poland and Lithuania.
- Establishment of Multinational Division North (MND N) in Adazi, Latvia with a component in Karup, Denmark.

Furthermore, the decision at the 2022 NATO Madrid Summit to establish a 'forward defence' places a premium on deterrence by denial, being the defence of the Baltic states and Poland.[573] The Russian invasion of Ukraine is also a pressing matter for the respondents, both in professional and in personal/emotional attention. Besides Russian military activities in Ukraine, there are Russian hybrid activities directed against the Baltic states such as influencing the Russian ethnic minority, or cyberattacks on state and banking institutions.

This all forces NATO to adapt. Still, NATO programmes of adaptation are nothing new. With its origins in the Cold War it had to adjust to the fall of the Soviet Union, the war on terror, and since 2014 to Russian aggression against Ukraine.[574] With

[572] For a detailed description of these measures see: Kamila Sierzputowska, "NATO Institutions in the Territory of Poland" (paper presented at the Security Forum, Banská Bystrica, Slovakia, 2018).

[573] Douglas Barrie et al., "Northern Europe, the Arctic and the Baltic: The ISR Gap," (London: The International Institute for Strategic Studies, 2022), 7.

[574] Michał Baranowski et al., "What Next for NATO? Views from the North-East Flank on Alliance Adaptation," (Tallinn: International Centre for Defence and Security, 2020), 1; Mercier, "NATO's Adaptation in an Age of Complexity," 3-4.

regard to intelligence, improved intelligence, surveillance and reconnaissance (ISR) coverage of Russia, is a topic of attention.[575]

Instead of these macro changes in organisation and strategy at NATO strategic level, this research looks at the complex habitus of the intelligence organisation of MNC NE within the context of its operational environment. As stated the corps is at the forefront of NATO's reaction to Russian aggression against Ukraine. It is therefore all the more striking that the corps is not the subject of more academic study. Regardless, the changing strategic environment and the implications of a responding NATO mean both change and uncertainty regarding the role of the corps. Polish Army Lieutenant General Sławomir Wojciechowski, commander Multinational Corps Northeast from 2018 to 2021, describes the situation following the Russian annexation of Crimea in 2014: '*the events that occurred over the last few years have contradicted the world order that stemmed from the collapse of the bipolar system. This is shocking. We've been having problems in understanding what is happening and in reacting quickly. […] We are so interconnected that a cough in one place could trigger an avalanche in another.'*[576] The next section describes MNC NE and its intelligence organisation in more detail.

6.1.2 MNC NE and its intelligence organisation

MNC NE is the only NATO command that is responsible for NATO ground forces in the Baltic Sea Region to defend Poland and the Baltic States, see Figure 7. The general task of the corps' intelligence organisation is to gain situational understanding on (possible) threats on NATO's north-eastern flank to support decision-making. This logically means that Russian military activities in the Western military district, Kaliningrad, and Belarus are the primary focus of intelligence. The war in Ukraine is of course intertwined with these.

[575] M.E. Ferguson, C. Harper, and R.D. Hooker, "NATO Joint Intelligence, Surveillance, and Reconnaissance in the Baltic Sea Region," (The Scowcroft Center for Strategy and Security, 2019), 7-8; Barrie et al., "Northern Europe, the Arctic and the Baltic: The ISR Gap."

[576] Jakub Bornio, "20 Years of NATO's Flagship Multinational Corps Northeast: An Interview with Lieutenant General Sławomir Wojciechowski," *New Eastern Europe* 3, no. 41 (2020): 107-08.

Figure 7: MNC NE area of responsibility and location of headquarters.[577]

The corps does not have to be deployed as it is permanently situated in its area of responsibility, with the corps headquarters at Szczecin, Poland.[578] The headquarter of MNC NE has a staff of 445 people with 25 nationalities. No public information on the exact size of the entire corps personnel could be found, but in general an army corps consists of two divisions or more with some 20.000 to 60.000 troops. However, the peacetime organisation of MNC NE does not reflect the corps at war strength.

[577] Compiled by author.

[578] Ulrich Pfützenreuter, "20 Years of Multinational Corps Northeast – from Political Symbol to Regional Responsibility," *Baltic Amber magazine* 2020, 12.

Nevertheless, MNC NE has the status of high-readiness force headquarters, able to deploy initial units within ten days and the entire force within sixty days. The organisational structure of MNC NE, during peace time, is as follows:[579]

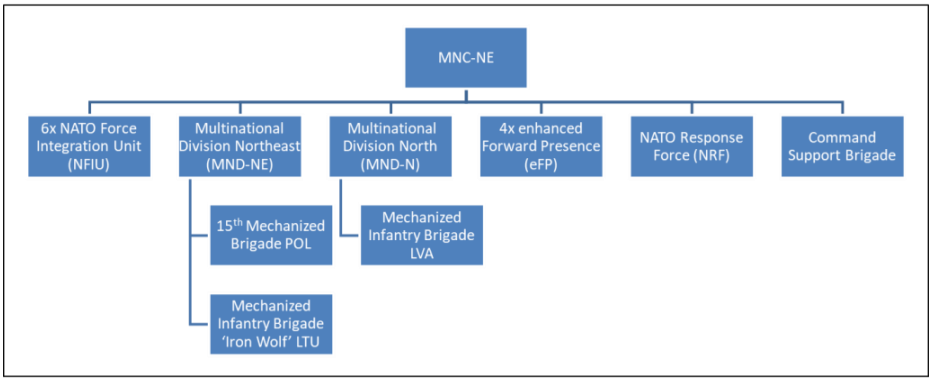


Figure 8: Peacetime organisation of MNC NE.[580]

Each of the units and commands has their own intelligence division or section, next to other functional divisions. The intelligence division will be described shortly. First the General Staff System, used to structure the functions in a military staff, is explained. In this system each staff is organised along functional divisions designated with a number; 1 for personnel, 2 for intelligence, 3 for operations, 4 for logistics, 5 for plans, 6 for ICT, 7 for training, 8 for finance and 9 for civil-military cooperation (CIMIC). These divisions are in turn divided into branches or cells along their own subfunctions. For intelligence this can be i.e. analysis, current intelligence, or IRM&CM. The number and type of divisions, branches, and cells is dependent on the level of command. This is designated with a letter. Army uses the letters G and S. G stands for the staff of a level of command lead by a general, S stands for the staff at the command level from major to colonel. For staffs composed of two or more military branches (army, air force, navy, marines) the letter J is used to designate the joint composition of the staff.

[579] The organisation as described here is a reflection of the organisation at the time of the field research. Several changes took place since then: The NFIUs are now under command of Joint Force Command Brunssum, but MNC NE gained an Estonian division.

[580] Compiled by author.

In the corps, the intelligence organisation is formed by the joint intelligence (J2) division at headquarters and the NFIUs, the intelligence section of a general staff (G2) at divisional level, and the intelligence staff section (S2) at brigade and eFP level. Because an exact description of the corps' intelligence organisation would be classified, only general characteristics are given here. The number of personnel at each echelon varies from a few dozen at corps J2 to about half a dozen at S2. Several functionalities, or branches/cells, are generally present at every level, such as analysis and current intelligence, but differ in size from a divisional cell to a single person at S2. The higher the level of command, the more branches are present. For instance, IRM&CM and plans are only separate branches at corps and division level. The intelligence levels from J2 to S2 are connected because of the chain of command of their units but there is also a variety of intelligence-specific communication between the levels such as meetings, ordered reporting, products, and requests for information. Furthermore, in general all levels have access to the same NATO intelligence systems and databases.

6.2 Environment of MNC NE intelligence organisation - respondent view

With the case study introduced, this section begins by describing the environment of the corps' intelligence organisation in a respondent-centric manner. When respondents talked about the challenges of their intelligence jobs they made no difference between their own organisation or Russia as the problem space. Rather, they differentiated between their own intelligence section on one side and their own unit/echelon, the corps, NATO – as well as the broader strategic environment of Russian grey zone activities and military aggression on the other. While this observation is perhaps remarkable, it is in line with the research approach described in Chapter 4 that states that with the corps' intelligence organisation as the unit of analysis, every entity outside that organisation is seen as external; broader NATO as well as Russia.

When expanding on this observation, many respondents used terms concerning issues of mandate for a peacetime organisation in a grey zone context, the disconnect between exercise and reality, and national agenda's that are not always in line with NATO. This section presents these emergent, institutional dynamics and their interrelatedness.

6.2.1 Peacetime, hybrid, or Article 5?

While the Russian invasion of Ukraine has put the alliance on alert, the corps remains in peacetime condition as long as NATO's Article 5 is not invoked. As a result, MNC NE is not fully manned and equipped and has a limited mandate. At the same time, Russia engages in a mode of warfare, also against NATO countries, that respondents often labelled as hybrid. As section 2.4 shows, this is a contested concept, without clear definitions. As a result, the analytical value of grey zone and hybrid is problematic.[581] Furthermore, hybrid acts may be misinterpreted as an accident or an isolated incident and vice versa.[582] The concept of hybrid makes it difficult not to miss a threat because acts are often covert or otherwise obfuscated and a larger pattern, or cohesion, is not obvious. It involves many unknown unknowns. Contrary, intelligence is about reducing the β chance of not discovering a link between phenomena (Type II error or false negative). In intelligence practice this leads to confusion on what to do. An analyst that specifically had to cover hybrid aspects had a telling anecdote: 'W*hen I started my hybrid analyst position at the headquarters I asked my predecessor what actually constituted hybrid warfare. I was looking for some sort of analytic model to do my work. However I got the answer that "it's what you make of it", because there were no frameworks or characteristics to assess the phenomena.'*

Still, regardless of terminology or definitions, the respondents found that countering hybrid (or grey zone) activities is not well reflected in MNC NE's peacetime mandate and organisation. MNC NE, for example, has very limited intelligence collection capabilities and has no legal basis to conduct ISR operations. These capabilities therefore hardly contribute to addressing the hybrid threats that occur during peacetime.[583] In response to this, one analyst from MND N remarked: *'we need to rethink our perception of peacetime'*. Adding to the confusion is that some

[581] Bettina Renz, "Russia and 'Hybrid Warfare'," *Contemporary Politics* 22, no. 3 (2016): 283.

[582] Rasmus Hindrén and Hanna Smith, "Understanding and Countering Hybrid Threats through a Comprehensive and Multinational Approach," in *The Academic-Practitioner Divide in Intelligence Studies*, ed. Rubén Arcos, Nicole K. Drumhiller, and M.ark Phythian (Lanham, MD: Rowman & Littlefield, 2022), 148.

[583] See also: Alexander Lanoszka and Michael A. Hunzeker, "Evaluating the Enhanced Forward Presence after Five Years," *The RUSI Journal* (2023): 4-5.

respondents believed that MNC NE should not even address hybrid threats, mainly because its resources and mandates are not adequate.

The tension between peacetime and wartime modalities of MNC NE also influences the focus of the intelligence efforts. Frustrated with the limitations during peacetime conditions, a respondent at MND N stressed that *'intelligence in peacetime in a NATO country means you cannot do anything'*. Another shortcoming that was experienced, is that MNC NE's mission implies an intelligence focus that is mainly aimed at assessing enemy strength. As a result, most intelligence analysts were land analysts that study Russian military units, their equipment, and movements. In practice, however, MNC NE operates under peacetime conditions and is confronted with grey zone threats. A recurring topic was Russia's influence operations on the Russian minorities in the Baltics states. Especially Narva in Estonia, that has an especially high concentration of ethnic Russians and Russian-speaking people, was seen as particularly threatened. Another often heard topic was the Belarussian migrant crisis that saw tens of thousands of refugees being brought in by Belarus only to be directed across the border into Latvia, Lithuania and Poland after deteriorating EU-Belarusian relations.[584] These topics make it essential to have a comprehensive intelligence focus, that also includes societal, economic, and political issues. The intelligence analysts were hardly able to cover all these issues. Other branches such as CIMIC and STRATCOM were asked to address these.

6.2.2 Exercise mode versus real life

MNC NE and its subordinate units prepare for war by means of exercises. While several respondents stressed the importance of exercises, most were very critical. On a positive note, during exercises intelligence branches possess collection capabilities that they do not have during their routine activities. Also, respondents stressed the opportunity to practice with certain systems, tools, and command and control relations. As one respondent from MND N remarked: *'We have a battle rhythm during an exercise; can't we have one outside the exercise?'* In addition, during exercise periods, battle staffs are bigger and many augmentees are available. As an example, an HQ analyst mentioned the presence of a provost marshal, who, during the exercise, was able to provide information that was relevant to many

[584] Aurel Sari, "Instrumentalized Migration and the Belarus Crisis: Strategies of Legal Coercion," in *Hybrid CoE Paper 7* (The European Centre of Excellence for Countering Hybrid Threats, 2023).

intelligence requirements. When the exercise ended, however, the task relationship with the provost marshal almost entirely ceased to exist.

Most respondents were very critical on the role of exercises in MNC NE and its subordinate units. This critique revolved around three main themes. The first theme is the inability of exercises to reflect reality and thus adhere to the mantra 'train as you fight'. The exercise Steadfast Jupiter that was held in October 2021 illustrates this well. Several respondents felt the exercise was more set in the context of counterinsurgency than in a context of major combat. The scenario therefore did not match the threat of large-scale warfare under Article 5 that was already looming before the 2022 invasion of Ukraine. Due to the limited timeframe in which these exercises take place, most are heavily scripted and lack rigour. During an exercise, for example, the intelligence staff always knows much about the enemy forces. In reality, however, this will not be the case and staff will probably be confronted with many unknowns such as the enemy's centre of gravity or the imminence of a counterattack. This disconnect limits the opportunities to train the intelligence staff. Part of the underlying problem is the generation of a Main Events List and Main Incidents List (MEL/MIL) to guide the exercise script. These lists are often too deliberate and limit natural conditions and behaviour. In response to the suggestion to make the exercise script more complex, respondents countered that they need more resources, including subject matter experts (SMEs). However, this they deemed infeasible.

The limited reflection of reality also concerns the timing and location of the exercises. Most are held at the regular office buildings with a static and stable ICT network. Yet, it is unclear what interoperability issues will appear when communication happens in a tent or on the move. Also, most exercises have a limited timeframe. This is problematic according to one officer from the plans division at corps HQ, especially when regarding complexity: '*In exercises there's too much events and decisions in a short time span. So it distracts from the actual time it takes for everything to work out. However, complexity only shows over time. In this way commanders get a bastardised sense of the effect of their decisions.'* Finally, the exercises do not run on a 24/7 schedule. Yet, on some occasions in reality, the corps had to operate around the clock for several days.

The second main critique involves the perverse effects that the exercises produce. Many respondents stated there is a real 'exercise mind-set' within the units. This focus leads people to spend much of their time on exercises. As one HQ respondent stated: *'We have too much administrative work and exercises: why should I need to*

know about the situation in Russia?' An intelligence officer from MND N added: *'We create exercises, we don't do intel'*. With an exercise completed, most are regarded a success. Many respondents, however, criticised the evaluation system. The multinational character of MNC NE makes evaluations a very sensitive issue and many stressed that, within NATO, *'nobody will fail at something'* in the words of an officer from the HQ staff. Overall, this creates a situation in which people act within an exercise mode, are positively evaluated, but at the same time realise the many downsides of their performance.

The third theme relates to the second and involves the inability to incorporate lessons learned in the organisation once an exercise has ended. During the exercises, NATO's Lessons Learned system is applied. After an exercise, however, respondents received hardly any feedback, nor does it become clear what lessons are learned. As a result, very few lessons are incorporated, little actual learning takes place, and people return to working like they did before the exercise.

6.2.3 National versus NATO interests

The third dynamic is the tension between national interests and those of NATO. This is apparent in two ways. First, national considerations regularly prevail over NATO policy, often referred to as national caveats. Within the intelligence domain, the most prominent caveats relate to intelligence sharing. Based on their own considerations, nations decide what to share with NATO. Several troop contributing countries have large national intelligence resources as well as different mandates that enable them to generate intelligence on the *area of intelligence responsibility* of the corps. While sharing this intelligence with NATO can enhance the intelligence position within the alliance, it can also jeopardise national sources and methods. This and other reasons greatly limit intelligence sharing of the individual nations with NATO's intelligence structure.

The second way in which the dynamic between national and NATO interests materialises, is through staffing NATO intelligence billets. NATO personnel varies widely in terms of how well they are prepared, what experience they have, and what knowledge they possess. While some countries thoroughly prepare their personnel before deployment, other countries pay less attention to this, or are less able to do so. As part of this, several individuals complained that they were not able to attend a NATO course to prepare for a position. As a result, time had to be invested in training people on the job. Also, newcomers can feel less confident in doing their work, causing feelings of anxiety on a personal level. One divisional current

intelligence officer even stated *'it takes you years to realise what you should be doing'*.

With regard to experience, the personnel had widely differing levels. While some were seasoned intelligence officers, others had very limited experience in working with intelligence. In addition, working at a corps or division level was new to many respondents, in particular those of the smaller troop contributing countries that do not have such command levels. Next to experience, knowledge of Russia, the Russian way of warfare, and the Russian language is important to the mission of the corps in general and for generating intelligence on the environment in particular. Several respondents considered it even a critical condition. In this respect, proximity to Russia matters. In general, the closer a country is to Russia the better its personnel understands Russian culture and thinking. As a result, MNC NE personnel that originates from former Warsaw Pact countries (e.g. Baltic States, Poland, Romania) generally have more knowledge of Russia and master the Russian language to a greater extent than their western colleagues. This relation however is no consideration in filling NATO billets. These different national perspectives are examined in more detail in section 7.2.3. All in all, one intelligence leader at the J2 summarised the billet staffing issue as: '*You never know what you're going to get. Sure, we can ask for somebody with a specific expertise or knowledge, but it's not sure we'll get somebody.'*

6.3 Environment of MNC NE intelligence organisation - analysis

The preceding section on institutional dynamics pointed to the separation between the intelligence organisation of the corps on one side, and the broader corps and NATO organisation, and the strategic environment on the other. This section further investigates these dynamics between the intelligence organisation of the corps and its environment. To do so, a complexity perspective is used that consists of the characteristics of self-organisation, emergence, non-linearity, and adaptation, from Chapter 4. These provide different perspectives to the institutional dynamics that manifested from the interviews.

6.3.1 Self-organisation

The first complexity characteristic, self-organisation, enables an examination of these dynamics along three topics. First is the idea of co-evolution. This is the mutually influencing relationship between a system and its environment whereby changes in one lead to changes in the other. Co-evolution between the corps'

intelligence organisation and its organisational and operational environments is severely limited. The corps is confronted with hybrid issues that are not necessarily covered by its conventional combat mode under peace time restrictions. Furthermore, exercises do not always reflect reality. While hybrid threats are a topic of concern, the corps lacks any mandate or capabilities to address hybrid threats.

While the Wales Summit of 2014 already called attention to hybrid threats (see section 3.4.2), this seems hard to put into practice – at least for the tactical level of the corps. Another perspective is that the legacy of the NATO counterinsurgency operation in Afghanistan and the attention for hybrid threats delayed the renewed focus on combat operations. This is reflected in the largest command post exercise in NATO, called Steadfast Jupiter. The respondents' claimed that Steadfast Jupiter 2021 lacked a sufficient combat scenario. This is backed up by the website of NATO's Joint Warfare Centre (JWC) that is responsible for joint operational level warfare training. According to the JWC website Steadfast Jupiter 2021 used a 'pre-Article 5' scenario to train deterrence. A year before, in 2020, the exercise was 'non-Article 5'. Only in 2022 the exercise focused on combat operations based on an Article 5 scenario.[585] However, the cause for these co-evolutionary problems lie with the NATO organisation level, not the corps intelligence level. Only one divisional respondent mentioned a co-evolutionary issue that is at the corps level. The respondent stated that while the war in Ukraine gets a lot of attention, the precise intelligence implications for the defence task of the two MNDs is not clear. At the time of the interview indications and warning was just being synchronised, according to the respondent.

Second, self-organisation also concerns the stability-disturbance dynamics of a system. The respondents gave varying statements with regard to the operational environment being stable or changing. The war in Ukraine is an obvious disturbance to many respondents, and many also mentioned the Belarusian migrant crisis as a disruptive event. At the same time many respondents saw the war in Ukraine as fitting in their personal threat assessment, and therefore see little change or imbalance in the operational environment. One officer at J2 even stated *'There are*

[585] Website NATO Joint Warfare Centre, accessed 7-10-2022.
https://www.jwc.nato.int/articles/steadfast-jupiter-2021-concludes
https://www.jwc.nato.int/articles/nato-exercise-steadfast-jupiter-jackal-2020-concludes
https://www.jwc.nato.int/articles/steadfast-jupiter-2022-concludes

no real strategic changes in the last 20 years'. A J2 analyst found that *'the daily situation does not change much and staying up to date with the operational environment does not take much time'*. There were also more nuanced perspectives. As already mentioned, familiarity with Russian culture is important in understanding the operational environment. As a result, respondents often mentioned that, in general, officers from countries that border Russia and have experienced Soviet occupation tend to see less imbalance than their NATO colleagues without these experiences. Russian behaviour, against NATO or in its war in Ukraine, is less unpredictable for these officers. Other respondents recognised (relative) stability in the strategic context and in NATO's focus but, within these confines, experienced *'constant change in what is asked for'* in daily practice. Some respondents problematised the idea of balance/imbalance and mentioned that perceived stability can also be false because hybrid warfare and grey zone activity, at least in its early stages, are designed to be below any detection or attribution threshold. The idea behind this is that the target senses no changes, but if it does the changes are minor and it is not clear who is behind it.

Third, self-organisation means the absence of a central controller. Many respondents experienced flaws, or even a general lack, with direction on the intelligence effort within the corps. This perceived lack of direction relates strongly to the notion of the absence of a central controller. The flaws with direction, originating from outside the corps' intelligence organisation, give some room for initiative. One respondent, who's function was in IRM&CM originally, became known as 'the OSINT guy' in his unit because he used his skills and experience to compile open source reports on the war in Ukraine. This respondent received quite some praise for his initiative as the product is considered high-quality and useful. The requests for the product eventually came from other branches within the respondent's own unit as well as from other units and echelons. The reliance on open sources but the lack of open source expertise that is widely experienced, is addressed here by specific local circumstances.

Individual initiatives at lower levels, that get incorporated into practice – albeit locally and temporarily – were mentioned by many respondents. The dynamic is often the same; a lack of direction results in intelligence personnel picking their own topics and coming up with new products. The feedback from customers then results in direction. Even though a military (intelligence) organisation is considered very hierarchical, without intelligence direction there is an opportunity for low-level intelligence initiatives to self-organise.

6.3.2 Emergence

This section deals with the second complexity characteristic: emergence. This relates to events that have a small probability to happen but will have major impact. It is about the sudden appearance of novelty, or surprise, stemming from the interaction of many underlying events. As seen in the preceding section, large events are often the indications for perceived balance or imbalance. The Russian invasion of Ukraine in 2022 often fitted the personal threat perception of respondents and therefore was considered no disturbance. The invasion itself, how the phenomenon manifested in time and space, was no surprise either for many respondents. There were many indicators in both intelligence and news reports, even when regarding aspects of information war. The real surprise was the poor Russian performance during the invasion and the strong Ukrainian resistance. Many respondents also mentioned the Russian annexation of Crimea in 2014 as a real surprise. The Belarussian migrant crisis was often mentioned, both as a surprise and as no surprise. This depended on the perspective of the respondent. Those who looked broader rather than to focus only on the military capabilities of Russia, especially when applying some sense of hybrid warfare, saw it as no surprise. Not only did it fit notions of hybrid warfare, there is also a comparable event from 2015 with stories about Russia directing part of the refugees from Syria across its borders to Finland and Norway.[586]

The empirical data shows that the level to which an emergent event is experienced as novel and surprising very much depends on the nationality and related knowledge of Russian culture and warfare of the respondents. This points to weak emergence in the context of this case study. This means the ignorance of many aspects of the intelligence problem rather point to a lack of knowledge or attention then to a phenomenon that is radically novel. Weak emergence means that the lack of knowledge is a practical/technical problem that ultimately can be solved. It is eventually a known unknown. Contrary, strong emergence entails that macro behaviour of a system cannot be related to its micro dynamics. It is a fundamental issue instead of a practical one. The uncertainty here remains hidden in unknown unknown. The empirical data showed mostly instances of weak emergence. This has

[586] Reuters, "Finland, Norway Bridle at Migrant Flows from Russia," (2016); Reid Standish, "For Finland and Norway, the Refugee Crisis Heats up Along the Russian Arctic," *Foreign Policy* 26 (2016); Piotr Szymański, Piotr Żochowski, and Witold Rodkiewicz, "Enforced Cooperation: The Finnish-Russian Migration Crisis," in *OSW Analyses* (Centre for Eastern Studies, 2016).

a strong relation with the positivist tendencies of intelligence and the military in general. If the world can be objectively known, then any surprise comes from a lack of knowledge, or ignorance.

Weak emergence in the context of this case stems from ignorance regarding Russian language, culture, and way of war. This relates strongly with the 'taxonomy of surprise about security threats' created by Ikani et al (2022).[587] This taxonomy broadens the idea of surprise beyond a binary perspective. Ikani et al. distinguish between three dimensions of surprise: perfect, significant, and partial. The amount of surprise depends on three aspects:

1. Dissonance, the gap between event and previous assessment.
2. Scope; how much of the threat characteristics were known?
3. Spread; who is most affected, analysts or decision-makers?

Ikani et al. show the intervention and annexation of Crimea was a perfect surprise for most European decision-makers, and a significant to perfect surprise for analysts.[588] This is in line with the view of most respondents, however respondents who share a national border with Russia declared to be only partially surprised. Contrary, the 2022 invasion was a partial surprise at most to the majority of analysts, if it was not a lack of surprise. There were no respondents whose answers related to ideas of strong emergence.

Aside from the surprise aspect of emergence, the concept also refers to lower-level dynamics culminating into high-level novel behaviour. On a general level, the combination of the Russo-Ukrainian war, Belarusian migrant crisis and support of Russia's war effort, and Russian influence operations on Russian minorities in the Baltics constitutes an operational environment that is novel. This makes it a case of strong emergence whereby uncertainty is fundamental. In a way, both the

[587] Nikki Ikani et al., "Expectations from Estimative Intelligence and Anticipatory Foreign Policy: A Realistic Appraisal," in *Estimative Intelligence in European Foreign Policymaking: Learning Lessons from an Era of Surprise*, ed. Christoph O. Meyer, et al. (Edinburgh: Edinburgh University Press, 2022), 44.

[588] Christoph O. Meyer and Nikki Ikani, "The Case of the Ukraine-Russia Undeclared War 2013/2014: Lessons for the Eu's Estimative Intelligence," ibid., 140.

organisational and the operational environment amplify the disconnect with the intelligence organisation of the corps.

6.3.3 Non-linearity

The third complexity characteristic of non-linearity deals with the cause-effect relations between the entities in the operational environment. Non-linearity in this regard is an extreme and unpredictable cause-effect relation. Remarkably, regardless if respondents experienced any imbalance or surprise in their external environment, many were convinced causality can be knowable, or observable even. The difference between the two was often seen as only a matter of capacity or effort. Most respondents were convinced that with enough sensors and reporting, and professional standards, causality can be observed. This strongly relates to the idea of weak emergence from the previous section. The biggest non-linearity, and therefore also surprise, experienced by the respondents was not the perceived strength and capabilities of the Russian Armed Forces but their poor performance in Ukraine. Even several respondents with much knowledge on the subject, stated they did expect performance problems but were still struggling to understand the actual performance.

Respondents in general believed that causality can be knowable. However, when questioned further, quite some respondents had difficulties with several more specific events and circumstances in the operational environment. Several respondents mentioned that the operational focus of the corps, as a geographic land command, does not take into account military aspects of the Baltic Sea or the arctic region, while these can indirectly influence the geographic area of responsibility. An intelligence officer at HQ stated that: '*Modern technology and the information saturation of the operational environment have led to the idea that if you know the right things, then you're ok. We think we know everything and can also act upon it.'*

Many respondents problematised causality in the context of hybrid warfare. As already mentioned by respondents, hybrid warfare and grey zone activities are designed to hide causality with ambiguity. Furthermore, even if causes are detected, it is not immediately clear how they relate to each other or to some strategic effect. A captain analyst at the J2 noted that these non-linear characteristics of hybrid warfare *'relate poorly to NATO's military decision making process'* (MDMP). MDMP is an iterative planning methodology to understand a situation and related mission, develop a course of action, and produce a plan. It is originally meant for combat but also applied to counterinsurgency, however, understanding hybrid ambiguity and formulating a plan proves more difficult. Here the mismatch between the

intelligence organisation and the operational environment is aggravated by the organisational environment.

Other respondents pointed towards disinformation, often associated with hybrid warfare. Russian false narratives are often based on actual news events. This is difficult to unravel and understand as it is, the effect they're seeking even more so. The big analytic question is what the opponent's objectives and intentions are. Is the disinformation narrative only for Russian national audience or also meant for NATO or other audiences? Are there more activities (military, political, social) that relate to the narrative? Intentions are difficult to ascertain, even more so when hybrid and grey zone activities are designed to be ambiguous. Compounding this problem is the general lack of analytic tools to understand hybrid and grey zone activities as mentioned by respondents.

A final, often mentioned, non-linear event relating to hybrid warfare was the Belarusian migrant crisis. While the corps considered itself not a responder in this, as it fell to the member states to deal with the situation, the corps was confronted with member states withdrawing national resources and troops from NATO to improve border security. In this situation a low-level event had consequences for the national security policy of Lithuania, Latvia and Poland and the capabilities of a NATO tactical command that is directly responsible for defending the alliance and deterring Russia. This fits the idea that non-linear effects are disproportionate to input, in other words; small causes can generate large effects.

6.3.4 Adaptation

The fourth and last complexity characteristic is adaptation. This concerns a behavioural change as a result of pressure from the environment. On an abstract level this also relates to issues of learning and evolution. When talking with respondents on issues of adaptation the single most mentioned topic was the so-called headquarters adaptation program. As discussed in section 6.1.1, NATO formulated its Readiness Action Plan as a reaction to Russian aggression against Ukraine. This included many measures for MNC NE such as increased readiness and capabilities. While these measures came to the corps from the broader NATO organisation, the headquarters adaptation program is driven by MNC NE commander lieutenant general Jürgen-Joachim von Sandrart. This is a clear case of directed evolution which is steered by individual human beings, see section 4.3.4. This is a result from the war in Ukraine and a clear case whereby the operational environment directly impacts the organisational environment. It also fits in the broader motive of NATO adaptation from counterinsurgency to combat operations

against (near)peer militaries. The adaptation program is about transforming the corps from a planning command to a warfighting formation. This means that, instead of conducting and monitoring exercises as it currently does, the corps must be able to translate operational objectives into tactical activities and command combat operations. In essence, the corps intends to change its scheme that determines how it engages with its environment. What this will mean exactly for the role and functions of intelligence is unclear to the respondents. While this uncertainty is accepted – as part of military life, but also because the adaptation program was still in an infant stage – there still were questions on how the process will be organised.

While adapting is inherently part of the military profession, also reflected by the motto of the corps (*Ready Today. Prepared for Tomorrow. Adapting for the Future.*), this does not mean there are no challenges. There was quite some scepticism regarding learning and implementing lessons for improvement within NATO. As a result, while the headquarter adaptation program is meant to be about more than only issues of manning and procedures, one respondent from the HQ wondered how far it will actually go. He questioned if the corps is *'willing to change the structure of the headquarters to adapt'*, referring to the broadly accepted notion that the staff structure is too stovepiped. There was also scepticism that, even though the plan of the commander addresses issues experienced by many respondents, the middle-management dynamics will eventually neutralise most initiatives for change. One officer from HQ commented *'this system does not like changes'*.

The institutional dynamics show that the peacetime organisation of the corps faces hybrid threats while exercises do not reflect current operational circumstances. This section so far has described how this leads to issues of adaptation by changing from a planning command to a warfighting formation. In aggregation, this can be seen as a situation of competing schemata (see section 3.3.4); The contrast between hybrid, peacetime, and exercise circumstances – and between national and NATO interests – demand different modes of operating and organising. This means whatever scheme, or mode, is maintained, it never fully covers the intelligence practice that is needed. The co-existing and competing schemata result in continuous selection pressures leading to a certain level of constant flux, and uncertainty, regarding what the intelligence focus should be.

6.4 Subconclusion

When comparing the first and second level of analysis several observations can be made. The respondents talked about the broader NATO organisation and the operational environment as interconnected and external factors. This interconnectedness is seen as the origin of many challenges that exist within the corps' intelligence organisation, and the intelligence habitus as a whole. Still, empirical data contains more on problems within NATO than about Russia or other threats. While the interconnectedness of the external factors is recognised, the interviews emphasised the effect it has on NATO. Many respondents even considered the organisational workings of NATO as more difficult to understand than Russian behaviour towards Poland and the Baltics. One J2 respondent even spoke of *'self-imposed complexity'* in reference to the three dynamics: peacetime/hybrid/Article 5, exercise mode versus real life, and national versus NATO interests. These dynamics caused frustration and confusion among the respondents because their job to understand the intelligence habitus was experienced more difficult as a result from it. It must be noted that respondents only differentiated in levels of difficulty without necessarily meaning complexity as constituted by complexity science.

The four complexity characteristics (self-organisation, emergence, non-linearity, adaptation) generate an image of moderate overall environmental complexity experienced by the respondents; They saw little self-organisation. In general the environment was seen as stable. While the Russian invasion of Ukraine is seen as a major and disruptive event, it did not cause any imbalance as the event fitted the threat perceptions. This is underlined by the limited co-evolution where NATO, and thus also the corps intelligence organisation, are lagging behind. However, when looking at self-organisation as the absence of a central controller, it is remarkable that regardless of military hierarchy there was room for low-level initiatives to develop.

Emergence is mostly formed by the overall operational environment. The Russo-Ukrainian war, the Belarusian migrant crisis, and Russian influence operations on ethnic-Russian minorities in the Baltics present situations that NATO is not always prepared for. This is the result from a lack of knowing rather than the events being unknowable. Emergence was not strongly perceived by the respondents and almost always seen as weak emergence; not knowing something because of lack of resources instead of a fundamental uncertainty, i.e. strong emergence.

Regarding non-linearity, many respondents were convinced that cause and effect relations can be known or even observed. Only several examples were mentioned where the cause-effect relations were unknown, regardless of any efficient intelligence effort to understand the phenomena. The exception is hybrid warfare which is considered to be ambiguous by design. Therefore many respondents accepted more uncertainty here regarding causal relations.

The biggest adaptation issue is the self-initiated headquarters adaptation program. How this will impact the respondents was not yet clear. In this aspect, the adaptation program as a result from changes in the operational environment, is another instance where external factors affect the intelligence organisation of the corps. In general, adaptation is determined by the currently competing schemata of peacetime, hybrid, exercise and combat. Without one of these becoming dominant, changes and uncertainty will remain.

This moderate experience of environmental complexity by the respondents differs from the general consensus in professional and academic literature regarding the increased complexity of the military operational environment. Two factors seem fundamental in this. First is the tendency to make all problems simple. This is intuitive and by training, as well as enforced because the methods and processes are designed for simple problems. Second, knowledge on complexity was lacking among the respondents. Only several US officers were familiar with the concept of complexity from lessons at their Command and General Staff College.

The next two chapters build on the empirical data concerning the difficulties for intelligence with regard to the organisational workings of NATO – that often outweigh the difficulties in understanding Russia. Both chapters extent the dominant theme of this current chapter to examine the organisation of intelligence.

7. Case study, part II; The organisation of intelligence – respondent view

The previous chapter examined the organisational and operational environment, as part of the military intelligence habitus of MNC NE. This chapter focuses on the corps' organisation of military intelligence. In this chapter the first order of analysis is presented. In other words, it stays very close to the respondents' terms. It is dived into three parts: the intelligence cycle, respondent reflections on practice, and issues of alignment. The second order, researcher-centric, analysis is presented Chapter 8.

7.1 The intelligence cycle

The workings of the intelligence cycle within the corps are described in the four steps that make up the cycle according to NATO doctrine (see section 2.2). Adhering to the intelligence cycle here does not mean it is used as an analytic model. Rather, the cycle forms the basic language of intelligence. As such, its terminology emerged often during the semi-structured interviews, also when questions were not directed towards the intelligence cycle.

7.1.1 Direction

The direction of the intelligence process takes place on different hierarchical levels and in several different ways. At HQ MNC NE, the commander is the principal driver of the intelligence process. This happens periodically through several mechanisms, the main ones being the commander's update brief and the coordination board meeting of the command staff. Outside these fora, the commander's operations and planning staffs had very little direct contact with the intelligence staff to provide additional direction to the intelligence process. Finally, in rare occasions, the operational level (Joint Forces Command Brunssum, JFCBS) or the strategic level (Supreme Headquarters Allied Powers Europe, SHAPE) provided specific intelligence direction. Overall, many respondents considered the direction to be ad-hoc, short-term, or even absent. Although MNC NE has formulated a complete Intelligence Collection Plan with a breakdown of priority intelligence requirements (PIRs), specific intelligence requirements (SIRs), and essential elements of information (EEIs), these hardly direct the intelligence process. As one officer at J2 remarked, *'the PIRs do not drive the intelligence process. The main focus is on what shows up on a daily basis'*. A divisional current intelligence officer stated the direction is *'more focussed on common sense than the ICP'*.

At the subordinate units a similar situation is observed. At MND N respondents remarked that there is a complete lack of direction as well as an absence of PIRs. In response, the intelligence staff started to produce basic intelligence reports. This provoked questions, and direction as such, by the commander as well as the operational and planning staffs. But still, an IRM&CM officer at division level raised *'I have not been able to have the commander look at the PIRs'*.

The direction problems have several underlying reasons. First, many respondents pointed at the inability of the units to adapt their intelligence requirements to reflect the changing operational environment. Prior to the Ukrainian invasion, most direction centred around the Russian Zapad exercises. Russian troops remaining after Zapad 2021, however, led to a renewed interest and input for the direction process. Upon arrival of lieutenant general Von Sandrart, some of the PIRs were updated. But still, the formulation of most intelligence requirements did not change much and, in the words of a J2 analyst, were *'woefully outdated with a single focus on conventional forces'*. Some respondents referred to the national sensitivities and politics that make it difficult to change the formulation of intelligence requirements. A J2 production officer nuanced this perspective by stating that *'there is stability in focus, but a constant change in what is asked for'*. This leads to stable PIRs but changing SIRs and EEIs that reflect the emerging circumstances, according to the officer.

Secondly, several respondents questioned the validity and focus of the intelligence requirements. The requirements focussed on conventional land forces and emphasised issues such as the forces' disposition, their capabilities, and leadership. The requirements, however, hardly paid any attention to less tangible aspects, including morale of the troops or their mode of operation. The concept of reflexive control, one of the key determinants of the Russian way of warfare, illustrates this well.[589] This concept was discussed in several interviews. Although many respondents recognised its importance, only very few respondents were truly

[589] A. J. H. Bouwmeester, "Lo and Behold: Let the Truth Be Told -- Russian Deception Warfare in Crimea and Ukraine and the Return of 'Maskirovka' and 'Reflexive Control Theory'," in *Winning without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, ed. Paul A.L. Ducheine and Frans P.B. Osinga (The Hague: T.M.C. Asser Press, 2017); C. Kamphuis, "Reflexive Control: The Relevance of a 50-Year-Old Russian Theory Regarding Perception Control," *Militaire Spectator* 187, no. 6 (2018).

familiar with the concept. Having discussed possible implications, each of them acknowledged that it should have been embedded in the set of intelligence requirements. In a similar vein, the intelligence focus is very much land-centric because the corps is a tactical army command. Meanwhile, many respondents acknowledged the threat the Russian fleet on the Baltic Sea posed, as well as that of the air units in the Russian Western Military District. However, in military command hierarchy, this is the responsibility of the operational level Joint Forces Command Brunssum.

Thirdly, to gain a comprehensive understanding of the operational environment, intelligence direction should include different functional areas (horizontal alignment) as well as different hierarchical perspectives (vertical alignment). Incorporating the different functional areas at the corps is done by adopting the PMESII framework (Political, Military, Economic, Social, Infrastructure, Information). Whereas the intelligence staff was responsible for the military aspects, other branches and individuals covered the other areas. These included the CIMIC staff for social and economic issues, STRATCOM for information issues, the political advisor, and engineers regarding infrastructural issues. This division of labour contributed to a stovepiped approach with only very limited attention to the alignment of the separate functional areas. One divisional analysts stated: *'traditional military silo's do not work anymore'*. This is elaborated on in section 7.3. Closely related to this aspect is the vertical alignment between the different hierarchical levels. From a design perspective it is important that the intelligence requirements of the subordinate units are nested in those of the MNC NE. This, however, did not seem the case. Staffs at the subordinate levels hardly paid attention to the intelligence requirements of the MNC NE. And in the case of the NFIU Estonia, the PIRs were even derived from the Estonian MoD and those of the MNC were considered less relevant.

A fourth reason underlying the direction challenges was the malfunctioning of the IRM&CM functionality. According to NATO's intelligence doctrine, this should be the accelerator of the intelligence process and link each intelligence activity to at least one intelligence requirement. Within the corps headquarters, however, IRM&CM did not have a central function. Most respondents considered IRM&CM simply a bureaucratic function, as opposed to an administrative one that coordinates the intelligence process. Many J2 personnel circumvented IRM&CM. In turn, many incoming questions and request were received by an individual and not through the IRM&CM process. One IRM&CM officer complained: *'If there is a synchronisation*

meeting […], I don't have anything to bring to the table.' As a result of this, IRM&CM was often narrowed to RFI (Request for Information) management. Adding to the problem was that many submitted RFIs were not properly submitted. Especially the sections 'background' and 'justification' of the RFI format seem difficult to formulate. As a result, requests were not prioritised or, in some cases, not even processed.

Another remark the respondents made, was that submitting an RFI takes too long for an answer, or that it is simply pointless to even submits RFIs because all echelons possessed the same databases and products. A final reason for the malfunctioning of the IRM&CM process was the headquarters' battle rhythm. According to another IRM&CM officer '*MNC NE is a product driven organisation. In combination with the battle rhythm this is what turns the wheels. We decide ourselves what we put into an analysis. It does not matter if the reports do not relate to the PIRs.'*

The last issue contributing to influencing the direction was the discrepancy between the Area of Responsibility (AoR), the Area of Intelligence Responsibility (AoIR), and the Area of Intelligence Interest (AoII). Whereas the AoR of MNC NE consists of Poland, Estonia, Latvia and Lithuania, the AoIR includes non-NATO territory as well. Until the escalation of the conflict in Ukraine in February 2022 the focus and tasks were rather clear. However, since then many respondents realised that to gain intelligence on the Russian troops related to the AoIR, it is essential to assess the Ukrainian conflict and their role within. Studying the Ukrainian conflict, one should be able to assess the mode of operating of the units involved, the capacities, and leadership of the units – as well as the changes that take place during the current conflict. Because of these reasons many intelligence officers included the Ukraine war in their efforts. At MND NE the intelligence staff even provided regular updates (three times a week) to their commander on the situation in Ukraine. Meanwhile, several key respondents disagreed and stated that *'Ukraine is way out of our area of interest'*. They argued that the lack of intelligence collection assets simply prohibits them from getting a sufficient understanding of the situation on Ukraine.

7.1.2 Collection

MNC NE and its subordinate levels do not have organic intelligence collection assets or mandates. This lack of assets is related to the institutional setting as described in section 6.1. As long as NATO's Article 5 is not invoked the corps is not fully manned and equipped, and has a limited operational mandate. Due to the sovereignty and legal systems of the host nation countries Poland and the Baltic States, MNC NE is not allowed to covertly collect intelligence in this geographical area. Along similar lines, MNC NE is faced with peacetime collection restrictions. And while the corps

can submit collection requirements (CRs) to higher echelons, such as JFCBS or SHAPE, the respondents voiced the same complaints as with RFIs. While echelons were repeatedly invited by corps J2 to submit CRs, this did not led to an increase in volume of CRs.

This all seriously complicated the focus and scope of intelligence activities and the quality of the intelligence products. For this to change, one J2 major stated, good legal frameworks were needed to broaden collection capabilities, otherwise *'we can only read newspapers and keep our fingers crossed that nothing will happen'*. As a result, intelligence staffs were reliant on intelligence liaison, open sources, and databases. As one of the J2 analysts commented: *'I'm relying on the collection others do. I'm at their mercy.'* As most intelligence staffs did not have dedicated liaison personnel, the level and quality of liaising depended first of all on the personal networks of the staff. In particular people from the host nation of a particular staff possessed strong networks that they were able to tap into. Also, officers from the larger member states seemed to effectively draw upon their national networks. Their personal contacts and previous deployments enabled them to gain some national intelligence products and verify the quality of data they already possessed. This, however, generally did not involve highly classified material.

In addition to relying on personal networks, the organisational relationship between NATO units and the host nation stakeholders is important. This relationship differs between the host nation countries. NFIU Estonia, for example, was very well connected within the Estonian intelligence network. As a result, they received much information by the Estonian services and MoD, both formally and informally. And being an Estonian himself, the then commander of NFIU Estonia played a large role in facilitating these relationships. In most other cases, NATO units had more limited contacts with the host nation authorities. Apart from personal relationships, geographical proximity seemed to influence this relationship as well. Since NFIU Poland is situated at great geographical distance from the Polish authorities in Warsaw, building and sustaining relationship proves more difficult. NFIU Estonia, on the other hand, is located on walking distance from their national partners. This clearly facilitates their relationship.

However, liaison will not compensate for all the collection deficiencies. As one analyst at J2 stated: *'We have so many systemic issues here that even the best network of liaisons does not work.'* Finally, it is remarkable that the NATO units do not have many relationships with organisations outside NATO's military chain of command and the host nation authorities. There was no relation with think tanks,

academia, centres of excellence (e.g. European Centre of Excellence for countering hybrid threats, NATO Strategic Communication Centre of Excellence) and government organisations (NGOs). Developing and sustaining stronger relationships with these organisations could significantly contribute to the collection effort.

In addition to liaising, another mechanism is to collect information from open sources. Most of this collection takes place digitally and includes news sites, blogs, fora, social media or websites of relevant organisations such as Institute for the Study of War or Bellingcat. Open sources provide a great wealth of information, in particular on the current Ukrainian conflict. Many respondents therefore stressed that open sources are their preferred way to collect information. In doing this, they faced several challenges.

First of all, the technical access. For security reasons there was a limited number of computers that have access to the open internet. And in many cases the connection was limited in bandwidth, thereby affecting search activities. Secondly, there were no specific open source collection tools available within MNC NE and its subunits. Meanwhile, many relevant tools have been developed that facilitate structuring, focusing, and automating the collection of open sources as well as facilitate access to the deep and dark web. Thirdly, intelligence staff had little knowledge of, and experience with, conducting OSINT. Almost none of the respondents followed a course or training on how to conduct OSINT, although these are widely offered. Language was another challenge for personnel that conducts OSINT. The sources that report in English are generally easy to read. However, a large share of the sources are in Russian, Polish, or in one of the Baltic languages. While the units were able to cope with information in the Polish or Baltic languages through personnel of the host nations, open sources in the Russian language posed significant problems. Most staff did not master the Russian language to the extent that they could easily collect and interpret open sources. There was general agreement that the lack of Russian language capabilities hampered collection efforts.

The final challenge consisted of the magnitude of open sources that are available. For many respondents this resulted in sheer information overload. Together with the lack of intelligence direction, this made it very difficult for the respondent which sources to select and focus on. An additional point of concern is the invalidated nature of the open source data. As such, a major question for the intelligence staff was whether or not the data can be trusted. As one section head remarked: *'The main challenge of the operational environment is the confirmation of a piece of*

information that is open source.' In the next section this issue is explained in more detail.

The last mechanism to collect intelligence for MNC NE was by making use of the available databases and information systems. The main source the intelligence staff used was NATO's database service with intelligence reports. Respondents considered the system troublesome to use. One respondent told that when looking for new entries on the Russo-Ukrainian war, the first search hit was an irrelevant event in Kosovo. Some nuance existed as well. One IRM&CM officer stated: '*You have great databases: it might not include the answers you are looking for, but you have at least something to tell to your commander.'*

Since a large share of the respondents neither had experience in working with the system, nor received a training prior, only part of the intelligence staff made use of the system. While at the corps headquarters this was a relatively large part, at the NFIUs, however, hardly anybody used the system much. In addition, members of the other staff branches (e.g. CIMIC, STRATCOM, Military Engineers) that were responsible to gain situational awareness on the non-military issues (e.g. socio-economic, strategic communication, infrastructure) were largely not aware of the system and thus did not make use of it, if they even would have access. In addition, a second NATO system was used to collate products. On average, respondents found it easier to use this second system to look for information and products. When asked how the content of the two systems compared, the respondents could not explain how the two relate to each other, or what the overlap and differences were. In addition, within the corps several other systems were used as well, thereby further complicating the development of a common operating picture. This issue of the interoperability of these systems is discussed at the end of section 7.3.

7.1.3 Processing

The third phase of the intelligence cycle is labelled processing. According to NATO's intelligence doctrine, raw data and information are now turned into intelligence. At the headquarter of MNC NE the intelligence production branch was responsible for this. The production branch consisted of many individual analysts that are responsible for processing the incoming data and information as well as to perform the intelligence analysis. While intelligence personnel focused on military issues, personnel of other branches such as CIMIC and STRATCOM covered the non-military parts of PMESII. Whereas most intelligence organisations have dedicated personnel to do the collation of data, this was not the case within MNC NE. Analysts were tasked with collecting the data and information as well. Or, as one J2 analyst

remarked: *'I'm a one man's intelligence cycle.'* At the subordinate levels a similar configuration was in place.

In terms of processing, judging the reliability of the data and information was particularly challenging. Due to the lack of organic collection assets most of the analysts relied on the information in the databases as well as on open sources. Many respondents indicated that documents that were available frequently did not include the original sources. In addition, respondents remarked that the inclusion of metadata in the database was limited. This further complicated determining the reliability of sources, as well as searching the database. It also fuelled circular reporting, which is discussed at the end of this section. As to the open sources, staffs found it challenging to determine their reliability and validity. Some respondents argued that the F6 system, that is traditionally used to grade sensor reporting and judge the credibility of the source (score between A-F) and reliability of the information (score between 1-6), is difficult to apply to open sources. For a sensor report the source is either the sensor itself (observation, imagery) or a human source (SIGINT or HUMINT). However, when determining the source for an online news article, the F6 system leaves room for interpretation. Is the news company the source or the medium? If the article is based on several sources, some cited from other media, what is the source then? How to be specific; What information to grade from which source? The F6 system is especially difficult if disinformation is tied into existing phenomena and real news facts. Several respondents did realised the limited reliability of open sources. A J5 officer illustrated: '*Social media is only about extremes; every nuance is filtered out by algorithms. It's a common mistake to think that social media is an actual reflection of the world and of people's perceptions and ideas.'*

With regard to the validity of open sources, many respondents pointed to the lack of classified intelligence assets. This made it difficult for them to verify information that is available in open sources. Given these difficulties, it is not clear whether the use of open sources at the corps is mere collation of publicly available information, or if it entails some form of analysis or enrichment that turns it from information to OSINT. The lack of sourcing, the difficulty in determining the reliability of data and information, and the reliance on open source and databases had severe consequences. It resulted not only in circular reporting, but also in increased risk *'of importing propaganda, misinformation, and disinformation'*, as one divisional lieutenant-colonel stated. In particular in the context of the current information war,

respondents considered this potentially harmful.[590] This danger is real, as Varzhanskyi shows. Using the concept of reflexive control he studies how in the Russo-Ukrainian war disinformation is used to influence open source information and intelligence to ultimately influence the opponent's decision-making.[591]

In terms of actual analysis, significant differences seemed to occur. At each level there was staff that made thorough intelligence analyses. Topics that were addressed, include Russian land forces, maritime activity, and hybrid threats. However, many respondents indicated the analysts lack the time and resources. As one IRM&CM officer remarked on the role of the analysts: '*They recycle reports. There's no time for analysis. Everybody is busy with meetings, briefings and exercises that there's very little time left for doing the actual job properly.'* When the analysts were able to do analysis, the majority was qualitative and historical in nature. Most of the analysts did not use structured analytic techniques (SATs)[592]. Analysts were either simply not aware of their existence, had not received training to apply these techniques, and did not realise the conditions for applying them.[593] They also argued that, since they mostly work with finished intelligence products, there is no sense in doing a thorough analysis.

Exceptionally, analysts did use structured techniques. These included a SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis or statistical pattern analysis. The latter was performed on maritime threats at the headquarters of MNC NE and is one of the rare examples of quantitative analysis. Analyses such as these are extremely valuable and significantly added to the intelligence position of MNC

---

[590] Timothy Clark and Robert Johnson, eds., *The World Information War: Western Resilience, Campaigning, and Cognitive Effects* (London: Routledge, 2021).

[591] Illia Varzhanskyi, "Reflexive Control as a Risk Factor for Using Osint: Insights from the Russia–Ukraine Conflict," *International Journal of Intelligence and CounterIntelligence* (2023).

[592] To reduce the chance for intelligence failures, the intelligence community has developed many different analytical techniques. Heuer & Pherson (2011) provide an extensive overview of over 50 of them, which have become known as structured analytic techniques. These techniques include 'Analysis of Competing
Hypotheses', 'Delphi Method' and 'Scenario Analysis'.

[593] Welton Chang et al., "Restructuring Structured Analytic Techniques in Intelligence," *Intelligence and National Security* 33, no. 3 (2018).

NE. In addition to the question whether or not to apply SATs, or doing a quantitative or qualitative study, analysis within MNC NE and its subordinate units faced several challenges. First, the intelligence analysts were all military, most of them focus on land issues and from a general background. There were only very few subject matter experts (SMEs) amongst the staff. This led to a lack of in-depth knowledge on several issues.

Secondly, the intelligence analysts pool had many different nationalities. As briefly mentioned earlier, proximity to Russia relates to better knowledge on its culture and language. With regard to analysis of the Russian threat to NATO, generally, Eastern European staff, e.g. from Poland, Baltic States, and Romania, perceive it to be higher than Western European or American staff. However taking advantage of this varied knowledge base, even though it is not reflected in filling billets, in the actual intelligence products hardly occurred.

The third challenge centred around the alignment of analyses, both horizontally as well as vertically. Horizontal alignment refers to the relationship between single analyses at one hierarchical level. The main challenge here was the cross-disciplinary analysis between the different elements of the PMESII framework. As a result of all these challenges, often only a narrow analytic focus was possible. As one eFP chief S2 stated *'assessments are done through a straw'*. Vertical alignment refers to the relationship between the analyses at multiple hierarchical levels. In other words, how do the analyses and assessments of lower hierarchical levels relate to those at higher levels. This challenge is further elaborated on in section 7.3.

The fourth, and last, challenge was circular reporting. This is a situation when a piece of information appears to come from multiple independent sources, but in reality comes from only one source. This is often the result of not referencing the original source of a piece of information/intelligence after which, when multiplicated in other intelligence products, the situation develops where several intelligence products mention the same statement (false positives). Even though the original source is never mentioned, it still looks as if the sources corroborate each other. This happens quite often, or, as one of the NCOs at an NFIU remarked: *'Of 90% I don't have a clue what the source is'*. An analyst at J2 stated circular reporting *'is horrible here. You waste much time on this'*. At the subordinate levels as well, respondents stated that circular reporting is omnipresent. While this is an internal phenomenon, as it manifests within the intelligence organisation, at least part of its origins lay within the external, own NATO organisation. Circular reporting was caused by multiple underlying organisational conditions. Because there was no mandate for ISR

operations, intelligence was very reliant on open source for up to date situational awareness. However without proper expertise and experience on intelligence analysis or OSINT specifically, a situation can develop where the same (pieces of) information get duplicated unknowingly and eventually end up corroborating itself.

7.1.4 Dissemination

As General Alfred Gray, former commandant of the US Marine Corps, already stated: *'Intelligence without communication is irrelevant'*.[594] To prevent this from happening, the final phase of the intelligence cycle, that is labelled dissemination, addresses the communication of intelligence to its consumers. At MNC NE there were four main communication channels in place to disseminate intelligence products. Each of these mechanisms was on a basis of intelligence push. As one production head remarked: *'Most commanders use the intel community as follows: "if there is something happening, the J2 will inform me".'*

First of all, many of the products were uploaded on the database. These included analyses on a single topic, but also periodic comprehensive assessments such as the Joint Intelligence Preparation of the Environment (JIPOE). In several cases, however, staff did not work with the database. The products for which they were responsible were therefore often not included in the database. This included intelligence staff, but mostly it concerned the staff from other branches such as CIMIC and STRATCOM. Secondly, intelligence products were posted on the SharePoint page of the relevant echelon. Thirdly, finished as well as unfinished products were verbally communicated in coordination meetings and commander's update briefings. During these meetings intelligence staff presents some of their products. Frequently, intelligence staff used a PowerPoint presentation, some of these contained speaker notes to provide more background information. Lastly, several products were also disseminated through email to a selected number of recipients.

Apart from these four mechanisms it was often unclear to many staff how to disseminate their products. One analyst at J2 remarked: *'I don't know who I will send my intel to and how to do this. The coordination of dissemination is entirely lacking.'* This is largely because most staff involved considered the commander at MNC NE the sole consumer of their intelligence products. The commander's time and

[594] Paul Otte, *Grayisms. And Other Thoughts on Leadership from General Al Gray, USMC (Retired) 29th Commandant of the Marine Corps* (Arlington, VA: Potomac Institute Press, 2015), 41.

attention to the intelligence products is, however, limited and there were too few mechanisms in place to feed the commander's operations and planning staff.

Regarding feedback and accountability, the respondents were rather critical. While some analysts receive individual feedback during the analysis process, generally respondents missed feedback on the (value of the) intelligence they deliver. As one J2 analyst summarised it: '*My superiors check my report and send it back to me to adjust it if needed. Then it is being published on the database. And then it's not common to get feedback. Actually, I have never gotten any feedback.'* Or, as a production branch head illustrated: *'With regard to the [a particular report] there is definitely no feedback. Sometimes, by surprise, someone will read it.'* Concentrating on accountability, a similar picture of resignation emerged during the interviews. Interestingly, many respondents drew a parallel between the functioning of MNC NE and NATO as a whole: *'[Under a NATO flag] we never objectively assess how a unit is functioning.'* An officer at the HQ added *'there are no systems or processes in place'*.

The final outcome of the intelligence process is, according to most respondents, an increased situational understanding of the commander. Since the research team was not able to speak to the commander, it was not possible to verify whether and to what extent this is the case and how it influences his decision-making process. The operational context and mandate of MNC NE, however, restricted the commander's ability to carry out operations that are driven by intelligence assessments. It must be noted that the organisational conditions described in this section are peacetime conditions. It is unclear what problems are tolerated now, but will be dealt with in a crisis situation.

7.2 Respondent reflections on practice

The empirical data regarding matters of intelligence theory show six terms frequently used by the respondents; products, frameworks, prediction, objectivity, bias, and different perspectives. These terms are transferred from the raw interview data and, being very practice oriented, describe how respondents reflect on their intelligence practice in the context of their intelligence environment. Because of their close relation the terms 'products' and 'frameworks', and the terms 'objectivity', 'bias' and 'perspectives', are addressed together, with 'prediction' being addressed as its own category.

7.2.1 Products and frameworks

In general, the intelligence battle rhythm prescribed three weekly intelligence products: a contribution to the commander update briefing, an intelligence summary (INTSUM), and a threat update on Terrorism, Espionage, Subversion, Sabotage, and Organised Crime (called TESSOC). In the battle rhythm the Intelligence Preparation of the Operational Environment (IPOE) is revised once a year. Products that appeared independent of the battle rhythm are Supplementary Intelligence Reports (SUPINTREP) or a collation/summary of relevant open source reporting. This means that the majority of production was driven by battle rhythm, not relevance or necessity.

Furthermore, these products are often structured on frameworks determined by doctrine, military order, or common usage. Examples of, what have basically become formats, are instruments of state power according to DIME (Diplomatic, Information, Military, Economic) and PMESII (Political, Military, Economic, Social, Information, Infrastructure) to describe a region or country. PMESII was often mentioned as a good framework to have a comprehensive view which is essential when looking for hybrid dynamics. However, given the limitations with intelligence collection it was also troublesome to reach enough analytic depth in each of the PMESII dimensions. With the influx of Ukrainian refugees following the Russian invasion, the analysts used DIME to describe the status of the Ukrainian state *'because PMESII is too specific to address a sudden situation'*, according to a production manager at J2. Another often used framework, or rather formula, is: intentions x capabilities x activities = threat. This widely used formula expands upon Singer's original formula of *threat perception = estimated capability x estimated intent* as examined in section 3.2.1.[595] This does not mean assessment is made easier. In practice many respondents found the categories of capabilities and activities have an overlap, which diffuses the process. The difficulties with establishing adversary intent remain unchanged.

All this standardisation is important for international coordination and cooperation but it is also resistant of change. As a result the opportunity to publish on topics not prescribed by battle rhythm and/or formats was very limited. Only one respondent, from NFIU Latvia, stated *'the knowledge of the intelligence section members was more leading than frameworks'* in producing intelligence.

[595] Singer, "Threat-Perception and the Armament-Tension Dilemma," 94.

7.2.2 Prediction

The section on the intelligence cycle covered the challenges of Structured Analytic Techniques (SATs). Here only the idea of prognostic/predictive analysis is highlighted shortly. There is a logical parallel with the observation that analysts did not use SATs. The lack of ISR and having to work mostly with finished intelligence reports severely limited the opportunity to add to already existing prognostic assessments. Furthermore, despite this limited opportunity, respondents did mostly descriptive and explanatory analysis, not prognostic. As one corps' subordinate commander, who had previously worked at the intelligence branch of JFC Brunssum, commented: *'Let history to the historians and see how you can make intelligence predictive.'* In the interviews only one clear example of prognostic analysis appeared. This concerned the statistical analysis of maritime data of the Russian Baltic Fleet as mentioned in section 7.1.3 on processing. The patterns that manifested from the data allowed prognostic assessments. Or, as the analyst in question stated: *'Pattern analysis enables prediction.'*

A specific application of prognostic intelligence is the Indications and Warning system, or method. While I&W is primarily done at NATO levels above corps to feed into policy, lower levels employ it independently to make sense of their environment. The efficiency of NATO's I&W system was a point of discussion among respondents after Russian actions in Ukraine in 2014 and 2022. Questions were raised how I&W from higher echelons such as JFC Brunssum or NATO Intelligence Fusion Centre (NIFC), but also from individual member states, relate to each other. At the same time it was unclear to the respondents how they can contribute to these, or if a similar system should be created for the corps' echelons. Respondents were weary of too much fusion regarding I&W because it would affect the value of having multinational perspectives on the threat from Russia.

The predictions and assertions regarding the Russian invasion of Ukraine in 2022 caused some reflection among the respondents regarding their methods. Before the invasion analysis of Russian capabilities was dominant. It consisted of regarding the volume of equipment, known as 'bean counting', and disposition of forces. The invasion severely complicated this dominant view on capabilities. Before the invasion the Battalion Tactical Groups (BTG) as the main combined-arms manoeuvre unit of the Russian army was the metric for assessing Russian military capabilities. Descriptions of commanders, readiness level and conscript rate provided the data for the metric. During the invasion, Russian losses and the observations of units that were not task-organised or combined caused the BTG metric to have more

uncertainties than certainties. This severely hampered predictive assessments as *'the difficulty now is updating basic intelligence'* upon which prognostic assertions can be made, according to a divisional current intelligence officer.

The poor performance of Russian troops in Ukraine and why they were overestimated was discussed among the respondents. Russia being a relatively closed society and rife with propaganda was one of the causes mentioned in these discussions. Cultural bias and too much focus on military hardware instead of moral topics such as will to fight or motivation were other causes. These practitioner discussions are reflected in a broader, more theoretical, debate.[596] The Russian invasion of Ukraine and its challenges for intelligence, practice as well as theory, also raised questions on issues of objectivity, bias, and perspectives. These are presented next.

7.2.3 Objectivity, bias, and cultural perspectives

In general, respondents were convinced intelligence can provide an objective understanding of the operational environment. One branch head production plainly stated: *'We are able to tell truth to power.'* A divisional intelligence manager also stated intelligence *'is about telling truth to power'* but, citing the difference between Russian pre-invasion threat and their actual performance, also admitted this is difficult: *'In a perfect world we could measure it.'* In fact, while acknowledging an objective truth, most respondents mentioned caveats and conditions that influence how close to the truth intelligence can get. A J2 analyst stated: *'It's hard to see the truth because of the information war.'* An intelligence officer at the Polish eFP explained: '*There is a truth to the operational environment that intelligence can ascertain, but this is limited by time and tasking. An exception is when an enemy is not committed but has forces positioned. Then there are only possibilities, conditions and factors – but no truth.'*

Getting to the truth as close as possible can be done in different ways. Increased collection or, more specifically, more sources, was the most mentioned method to reduce any bias. Another often mentioned method was the generic *'following the procedures'*. Following up on this, respondents referred to several features. From doctrine, the method to communicate so-called 'confidence levels' regarding the

[596] Robert Dalsjö, Michael Jonsson, and Johan Norberg, "A Brutal Examination: Russian Military Capability in Light of the Ukraine War," *Survival* 64, no. 3 (2022); Christopher Dougherty, "Strange Debacle: Misadventures in Assessing Russian Military Power" (16-6-2022), Warontherocks.com.

intelligence upon which assessment are made, is mentioned. The assessments themselves are written to include what is known as 'probability statements for assessments'. In general it was often remarked that analysts work alone, or separate, due to constraints in time, expertise and personnel – while at the same time cooperation was often seen as highly valuable. A member of a NFIU J2 remarked: '*Human analysts can't be unbiased, but you can get close. To counter bias there needs to be an informal process of peer review, or call in a third party.'*

In talking about the need for teamwork, in a multinational organisation, many respondents touched on the subject of different cultural perspectives (regarding Russia) among NATO member states. Overall, this was valued as a way to counter cultural bias. A non-commissioned officer analyst stated being objective is *'far more likely in a NATO environment'* where you can leverage other cultural perspectives. Specifically stated, and mentioned earlier in section 6.2.3, personnel from countries that border Russia and were part of the former Soviet Union are better apt at understanding Russian culture, language and way of war. A Romanian officer started with the Second World War to explain these differences and concluded: '*It is about understanding a certain Russian and East European human condition, but many analysts lack this. […] Eastern Europeans have totally different perspectives [from other NATO members]. […] Your threat assessment is not the same as ours.'*

A Polish officer echoed these statements: *'The Russian way of thinking and moral is close to us.'* However, the respondent also mentioned that younger generations are further removed from the Soviet experience and are less knowledgeable of Russia as a result. The difference in perception of the threat from Russia between Poland, the Baltic states, and other NATO members in East-Europe on one side and the other countries that make up the corps on the other was mentioned many times in the interviews. Regarding the Russian invasion in 2022, many respondents noted that personnel from East-Europe took the threat of an invasion very seriously while other nationalities – though not excluding this threat – were leaning more towards a limited Russian incursion. A Danish officer from MND N stated many Latvians were not surprised about the invasion, while many Danish colleagues were. The officer pointed out: '*Reading between the lines and understanding the cognitive dimension is easier the closer you are to Russia, in geography but also in mind set/culture.'* Another good example, that got a lot of media exposure, was the burning down of

Russian military facilities.[597] Western NATO members often named poor maintenance or sabotage as possible causes. Several respondents noted that officers with sufficient knowledge on Russia explained it is more likely that the fires were to hide corruption and the illegal sale of army stores that were about to be exposed with the Russian invasion of Ukraine.

The difference in perspectives also manifested with regards to the Estonian city of Narva. It is located in the north-eastern part of Estonia along the river Narva, across the river is Russia. With nearly 60.000 inhabitants it is the third largest city of Estonia. Over 90% of its population speaks Russian and over a third also holds Russian citizenship. Because of these figures many non-Estonian NATO officers regarded Narva with suspicion and as a possible hotbed for Russian activities against NATO. A very different opinion was voiced by a civilian political scientist working at NFIU Estonia who stated that the Narva issue is a 'wicked problem'. According to the respondent it is not only about Russian ethnicity. The Russian minority also faces declining economic opportunities, more corruption and is part of the Russian information sphere. At the same time, according to the respondent, it is important not to overemphasise Narva as a possible Russian jumping-off point; Russia does not need support from the minorities, they will claim it anyway and do what they want regardless.

While knowledge of Russian culture, language, and way of war are determined by geographic proximity and historical experience, on respondent level this is not always the case. Either way, there was a common awareness of co-existing perspectives influencing threat perception and strategic context. Many respondents valued this and actively sought other nationalities, or perspectives, to compliment and sharpen their own assessments. However, a structured approach to organise for this lacked and time constraints worked against it. Several respondents mentioned that, while different cultural perspectives are definitely present, at several units or commands the cultural diversity is quite limited as one nation holds the majority of positions.

7.3 Issues of alignment

During the interviews many issues regarding organisational alignment manifested. These concern mechanisms and failures to coordinate and exchange information and intelligence. Though alignment issues appear throughout the preceding sections, the

[597] Liz Sly, Annebelle Timsit, Rachel Pannett (2001, 27 April). Mystery fires at sensitive facilities compound Russia's war challenge. *Washington Post* online.

volume of issues that emerged from the interview data asks for this section of its own. First the internal alignment is discussed, then the alignment with partners outside the chain of command.

7.3.1 Internal alignment

While the organisational structure of MNC NE from Figure 6.1 looks clear, in reality this is less so. As a result of national caveats and peacetime conditions, several echelons that are part of MNC NE remain under national command, resulting in a mismatch between force and command structure. The Polish and Lithuanian brigades of MND NE illustrated this well. These brigades are under national command, but meanwhile are considered the higher echelon of corresponding eFP Battlegroups. This leads to friction in the command and control relation and hampers unity of command.

Apart from the command relationship, while looking similar on paper, many of the corps' echelons differ from each other. The divisional HQ of MND NE had a staff that is almost completely Polish staffed and had two brigades, while the HQ of MND N was smaller, divided over two locations in Latvia and Denmark and was staffed with multiple nationalities. It had one brigade. The NFIUs make a separate case. Being small headquarters, they were initially intended to enable fast reception of NATO units into North-eastern Europe. While this is still their main task during Article 5 operations, their task set during peacetime has significantly widened. It now also included support to wider deterrence and defence, support to NATO STRATCOM messaging, and to contribute to joint and comprehensive situational awareness by facilitating the exchange of information and intelligence between the host nation and NATO elements. The NFIUs were under direct command of the headquarter MNC NE and were situated at the same hierarchical level as the divisions. As a result it was unclear to the respondents what the division of tasks and responsibilities between the divisions and the NFIUs were.

To align the intelligence efforts of these different units, MNC NE had established a weekly working group to coordinate the intelligence effort. The purpose was to discuss intelligence topics and coordinate intelligence products on a weekly basis, before the commander's update briefing and the release of the INTSUM. The main topics were, current production, focussed reporting, and an outlook, or assessment. Entities that were invited came from command levels above the corps, own staff, and subordinate levels. While 11 entities of the MNC NE HQ were officially part of the working group, according to the respondents only the J2 staff, POLAD, STRATCOM and the J9 branch attended regularly.

Many respondents were appreciative of the working group as a platform to meet and see what other intelligence entities are doing. However, at the same time they were critical as to whether 'fusion' was achieved. In the working group all briefers presented their slides after which there is room for feedback. There were, however, rarely any questions posed or dilemmas presented by the briefers. In this way the working group seemed more aimed at coordination than at intelligence fusion: information is being shared, participants become aware what others are doing, and if needed they can use that information in their own efforts. However, there is no shared attempt of trying to include all the separate inputs into one aggregated understanding. As such there was also no clarity of supply and demand. As one divisional IRM&CM officer described *'nobody knows how to contribute'*. During the second interview round at the HQ the staff was aware of the problems with the working group. Measures were being devised to address the situation. As one high-level intelligence leader at the corps stated: '*The J2 leadership thought we were in synch with each other through the working group, but the work floor and the analysts were missing direction. This needs to be fixed.'*

The need to strengthen alignment between the different units of the MNC NE was well understood at the corps HQ. Its commander emphasised the need to establish work floor relations between the echelons. To this end a delegation from J2 JFC visited the corps HQ in March 2022. After a long period where Covid affected physical contact, this was considered a valuable visit. From an intelligence perspective the internal Baltic Region Intelligence Discussion Group is a platform that potentially can improve vertical alignment. This is a discussion platform meant for discussion and brainstorms not directly relating to any specific tasks or products.

A final issue relating to alignment is the interoperability of ICT systems. Because the structure of the corps developed somewhat haphazardly, many echelons have their own command and control systems and programs. This means systems are not connected by default, and interoperability issues surface. As a result, there is no common tool across all echelons to develop a bottom-up Comprehensive Operational Picture (COP). Another interoperability issue is that many systems can share intelligence up to NATO secret only, which excludes many valuable intelligence products above that classification.

7.3.2 External alignment

In addition to alignment of the MNC NE entities, aligning the efforts with external stakeholders, that operate outside the chain of command of MNC NE, is also important to generate intelligence – especially when confronted with hybrid threats.[598] In general, very few respondents reached out to entities outside their own command line or unit. And if they did, the external stakeholders were mostly host nation military or intelligence units. There was hardly any contact with think tanks, NATO centres of excellence, universities, or civil society organisations.

There are various reasons for this. Some respondents argued that time constraints and other military conditions impair contact with civilian entities. Other respondents stated that they find it already challenging enough to know their own organisations and keep contact with relevant partners inside. Or respondents stressed that they do not have a mandate to reach out to civilian entities. As one STRATCOM respondent remarked: *'We're not allowed to engage with local key leaders. This is a host nation responsibility.'* A section head at J2 described the problem as twofold: '*[the corps] is structured for tactical level combat, the outreach to non-corps entities is therefore limited. At the same time it is a balancing act to broaden the scope, but not get overburdened with data and info.'*

The NFIUs in Estonia and Latvia were clear exceptions to this. In part this is related to their mandate of connecting NATO with the respective host nation. NFIU EST had close relationships with the Estonian intelligence and military community. This was partly because of the close geographical proximity of their respective offices. Furthermore, the NFIU is equipped with sufficient systems and classified rooms that attract outside visitors to the NFIU barracks. This is in contrast with the Polish NFIU. Because of the original RSOM task (Reception, Staging, and Onward Movement) NFIU POL is located close to national logistical hubs, but far removed from the location of Polish intelligence entities.

NFIU LVA was often praised because of the quality of its intelligence. Many respondents mentioned its own intelligence coordination meeting as the main reason behind this. This meeting brought together several national and international intelligence stakeholders from all levels. As such, the meeting provided a platform for sharing and deconfliction. Furthermore, the meeting was not product-driven and

[598] Hindrén and Smith, "Understanding and Countering Hybrid Threats through a Comprehensive and Multinational Approach," 148-49.

thus provided room for discussion. This made it well suited for deep-dives and background dynamics.

7.4 Subconclusion

This chapter is a first level analysis according to the Gioia method, meaning it is a reflection of the respondents' own vocabulary. As such, three categories of terms are gained from the interview data; the intelligence cycle, respondent reflections on practice, and issues of alignment. These categories come close to the idea of habitus, as they describe theoretical underpinnings of intelligence practice at MNC NE. However, it must be noted that it concerns minor theories at the level of the unit of analysis itself.

The terms concerning the intelligence cycle in the first section are according to the doctrinal four step model (direction, collection, processing, dissemination). The cycle, as the main conceptualisation of intelligence, is part of the language of intelligence. This means the terms, and in this case also the category name, are transferred directly from the raw interview data. Overall, the respondents have problems with the intelligence cycle because it is not functioning as it should do, according to doctrine, within the corps. Most mentioned topics are the lack of direction, the absence of collection assets and procedures that are unknown or seen as cumbersome and slow – and therefore circumvented or avoided. Many respondents explicitly referred to procedural matters while there was only one explicit conceptualist, a divisional lieutenant-colonel, stating to have *'not much complaints on doctrine, but war is war'* and reality is better understood through cooperation within the cycle.

The terms of the second section (respondent reflections on practice) are transferred from the raw empirical data and are very practice oriented (products, frameworks, prediction, objectivity, bias, and different perspectives). They describe how respondents reflect on their intelligence practice in the context of their intelligence environment (operational and organisational circumstances and peculiarities). The products and frameworks used by the respondents form the methods and metrics for observing and measuring, or collection and processing in an intelligence context, of reality. Any deficiencies in this are seen as the result of a lack of resources, mandate or otherwise practical circumstances and conditions.

The terms from the third, and last, section (alignment) are internal and external alignment. While these are not literal terms from the raw data, they form logical groupings of the actual terms that evolve around coordination and exchange of intelligence across military hierarchy and among peer units, and external partners. Internal alignment is primarily frustrated because of the mismatch between force and command structure that in its turn impacts command and control. There is almost no outreach outside of the chain of command to peer units or non-military partners. Overall alignment is impacted by issue of interoperability between the many ICT systems in use among all levels of command.

The three main categories of this chapter will be further examined by connecting them to intelligence theory and complexity science in the next chapter.

8. Case Study, part III: The Organisation of Intelligence – analysis

This last chapter of the case study research deals with the organisation of intelligence on the level of second order, researcher-centric, themes. In four sections this chapter examines the interpretation of the intelligence cycle, the dominant intelligence theory, the prevailing intelligence paradigms, and the problem of alignment within the intelligence organisation of MNC NE. The fifth and last section answers the research question *How do military intelligence organisations deal with their complex operational environment?* While Chapters 6 and 7 can be read independently from each other, this chapter builds on both these preceding chapters to present an aggregate perspective. Furthermore, this chapter falls back on the theoretical Chapters 2, 3, and 4.

8.1 The intelligence cycle as missing procedure

Interviewing about the intelligence cycle means it is inevitable to use associated terminology. In other words, the researcher and respondents shared the same professional culture and language. As a result the data that features in section 7.1 is straightforward and little interpretation is needed here in this chapter to connect it to existing intelligence theory. The workings of the intelligence cycle are analysed with two concepts from Chapter 2: the proceduralist-conceptualist approaches, and the cycle as cybernetic feedback loop.

The critique of the corps' personnel on the intelligence cycle was largely of procedural nature. It concerned problems with outdated intelligence requirements, limitations on collection, and a faulty OSINT process. In their daily practice, many respondents regarded the intelligence cycle as stovepiped and IRM&CM, meant to enable interaction and feedback, was often ignored. Still, there was quite some non-linearity present in the daily practice of the intelligence cycle that is not present in doctrinal depictions of the cycle. Often this concerned respondents going against the unidirectional and linear nature of the cycle. This can be explained because there was also a strong conceptual tendency among the respondents. Regardless from doctrine, a vast majority of respondents seemed to have an expectation of the cycle that more closely resembles Hulnick's description of the cycle as a 'matrix of interconnections', or Omand's 'interactive network' (section 2.2.), than the doctrinal cycle as unidirectional and linear. However, this critique is still procedural as it

primarily concerns the workings of the cycle, independent from environmental complexity or the question if the model is still valid.

The intelligence cycle at the intelligence organisation of the corps is a manifestation of the cycle as a cybernetic feedback loop. While there was an expectation of more feedback and interconnection among the respondents, this did not manifest at the level of organisation. Intelligence direction was the only input that can make adjustments. Otherwise it was a closed and fixed system. At the corps, intelligence direction and its problems permeated the entire cycle. A lack of direction in the form of unclear and outdated intelligence requirements, combined with the lack of ISR, severely affected generating useful intelligence (collection and analysis) and contributing to decision-making (dissemination).

As a result the rest of the cycle is left to its own devices to try and adjust as it sees fit - while leverage for actual change can only come from direction. Even then, as stated in Chapter 2, the cycle only passes information but is not shaped by it. This cybernetic frame explains the challenges of open source intelligence at the corps. It is an instance of adaptation to an absence of ISR, the developments in information and (tele)communication technology, and the growing importance of open source information. However, without explicit requirements or direction on this, the internal agency to improve is limited in resources as well as expertise. The cybernetic frame also explains the observation that almost no respondent was in contact with non-military organisations outside NATO such as think tanks or NATO centres of excellence.

All respondents saw a need to improve the intelligence cycle. This underlines the value of the cycle and its doctrinal status in contributing to interoperability between NATO member states. This also means the respondents saw problems with intelligence performance as a mere malfunction of the system, without questioning the system itself. In this they mirror most of the literature on the intelligence cycle. No respondent questioned the viability of the intelligence cycle. There was no discussion if the concept applies to very different environments such as hybrid/grey zone, peace time or modern combat operations. Or puzzles, mysteries, and complexities. There was also no reflection on the cycle being geared only towards known unknowns; intelligence requirements in a collection plan, while unknown unknowns are not considered. It is more focussed on reducing the α chance, or Type I error while intelligence should focus on the β, or Type II error. In general, the cycle was very much embraced as a Jominian rule, ignoring any Clausewitzian friction or fog of war (see section 4.1.3).

Furthermore, the respondents see intelligence as serving the commander, staying very true to the book *Intelligence is for Commanders* (1948) mentioned in Chapter 2 that introduced the intelligence cycle.[599] This is a very traditional view whereas there is widespread consensus that intelligence should also be for the warfighters, a central idea in Network Centric Warfare (see section 3.3.1). And within government, intelligence is no longer reserved for a few high officials but for entire departments. Brown describes the complexity of the intelligence environment as an argument to broaden intelligence dissemination: '*In an age in which the speed, scale, and scope of overlapping national security issues have eclipsed the ability of any individual leader to keep track of them all, we must think seriously about broadening the intelligence audience. […] in a period of renewed great power rivalry that takes place under globalized, digital conditions, intelligence must no longer be for commanders—it must be for entire organizations.*'[600]

Overall, despite some non-linear appraisal, the respondents did not think outside the intelligence cycle. This is in stark contrast with critical perspectives and critique in academic literature that problematise the traditional understanding of intelligence as a command-driven cycle, applicable in any circumstance and environment. This forms another dimension in the gap between the practical dimensions of intelligence (external drivers) and theory (internal drivers), as described in section 3.7. However, where Chapter 3 draws the conclusion that the internal drivers are lagging behind a changing environment, the conclusion here is that critique on the intelligence cycle from the internal driver of debate is ahead of any critical reflection on the cycle in practice.

8.2 Nuanced positivism

Collecting data on the intelligence cycle was quite straightforward with a clear relation between question and answer, and linking the answer to theory. Interviewing on intelligence theory took a more interpretative approach. No respondent, on their own account, talked about intelligence theory or definitions. Instead, intelligence theory is the respondent-centric level look at the issues of products, frameworks, prediction, objectivity, bias and multiple perspectives – as

[599] Glass and Davidson, *Intelligence Is for Commanders*; from: Omand, "The Cycle of Intelligence," 62.

[600] Zachary T. Brown, "Intelligence Isn't Just for Commanders Anymore" (26-2-2022), Thecipherbrief.com.

appeared during the data collection. The analysis will use the positivist and post-positivist perspectives from Chapter 2.

The majority of the respondents adhered to a positivist notion of intelligence. This means they acknowledged there is an objective reality that can be observed and measured. The role of intelligence within MNC NE is then 'speaking truth to power'. As seen in section 3.5.1, this is firmly grounded in the Kentian approximation of intelligence analysis, in general, to positivist social science. This means that, at least in theory, the world is fully knowable, even predictable, and any fundamental uncertainty is excluded. In a Jominian way there is only uncertainty as a result of suboptimal analysis. This is in line with positivism being the dominant intelligence theory as stated in Chapter 2 and it is therefore no surprise conclusion.

The idea that intelligence is objective (and independent) is based on scientific ethos, as are the ideas on biases and the need to counter these. This firmly fits in the, again, Kentian and positivist tradition in intelligence. The role and perception of different national and cultural perspectives, within the corps' intelligence organisation, with regard to understanding the environment warrant more attention. Whereas all other respondent terms testify of a fact-based idea of understanding, the differences in Russian threat perception point more to a value-based approach. The geographic proximity to Russia and a shared Soviet past generate a cultural familiarity that is important in understanding Russia. In a sense, this understanding is socially constructed and therefore does not fit the otherwise dominant positivist persuasion. Still, however, the general awareness of co-existing perspectives where proximity to Russia and familiarity with Russian culture are valued over perspectives that are more distant is not full blown post-positivist. It exist more at the epistemological level than the ontological. Stated differently, the respondents still believe there is a single reality it just takes different perspectives to objectively ascertain the truth about this reality.

There is, however, another post-positivist tendency among the respondents. For this it is necessary to repeat Warner's statement from Chapter 1 who stated that it is '*a logical next step to explain intelligence as a reflexive activity, for intelligence systems under comparative scrutiny always interact with other systems (and with the world around them) in dynamic relationships and also in complex manners. Intelligence systems and the regimes that wield them, after all, comprise people, with their tendencies to biases, habits, and non-linear reactions to events'.*[601] Taking from

[601] Warner, "Intelligence and Reflexivity: An Invitation to a Dialogue," 169.

Warner, the awareness – and sometimes utilisation – among respondents of the different perspectives, combined with the institutional dynamics as experienced by the respondents, constitute a reflexive activity among the respondents that contrasts with their otherwise positivist persuasion. While Chapter 2 states positivist and post-positivist worldviews are mutually exclusive, or incommensurable, paradigms – at least some form of combination exists among the respondents, perhaps even flirting with Bourdieu's theory of practice. Though, it must immediately be stated that the overall stance of the respondents was a positivist one and nuances exist few and far between. The larger implication of this is that the military intelligence workforce employs a worldview, and methods, that are increasingly out of touch with the complexity of the practical dimensions of intelligence from Chapter 3.

8.3 Co-existing and conflicting paradigms

This section examines the dominant intelligence paradigm within MNC NE. To do so, the Cynefin framework from section 4.2.1 is used. This section first positions the two preceding sections on the intelligence cycle and intelligence theory in the Cynefin framework. Then, raw data is analysed and placed in the framework as well. The analysis in this section is done by matching the data to the three characteristics used to describe the Cynefin domains; type of constraints, required practice, and the decision model needed to address the problem – as explained in section 4.2.1. These three characteristics determine to which domain the data applies.

The predominantly proceduralist approach to the intelligence cycle relates to the clear domain; The doctrinal cycle is a best practice, it allows a standard, categorised response that anyone can apply because causality is fixed, enabling exact prediction. While there are definite conceptualist notions regarding the cycle among the respondents, these are not broadly reflected in practice to label them good practice as property of a complicated paradigm.

The implicit theoretical stance of the intelligence personnel qualifies as positivist. Their view of speaking truth to power and an objective reality point to knowable cause-effect relations, even if this is difficult to measure, and to a certain degree prediction. This places intelligence theory in the ordered paradigms (clear and complicated) of Cynefin. Then, however, it gets diffuse to relate the data to a single domain. In theory the processing phase of the cycle, containing different instances of analysis, can be seen as a good practice in the complicated domain. The data on

the value attributed to subject matter experts, i.e. people with knowledge on Russian language and culture, be it professional or accidental, points towards the need to analyse and not categorise. However, SATs (as good practices) are hardly used and analysis in general comes down to experience, subject knowledge or reporting. This contradicts the label analysis from the complicated domain, but it also contradicts best practices from the clear domain. Then again, the use of frameworks and product formats provided by doctrine does fit best practices. Overall, the implicit theoretical stance of the corps' intelligence organisation is a bit more clear than complicated.

The raw data on Cynefin, meaning the data that point toward a position in Cynefin inferred from the interviews as a whole and coded in NVivo, shows an entirely different outcome. Specifically, the data is selected because it very clearly fits one of the domains, according to the three characteristics. The data can be a respondent's observation about reality, an opinion on how things should be within the corps, or usage of certain keywords relating to a specific domain.

Remarkably, most data falls in the complex domain, whereas the intelligence cycle and theory fall in the ordered domains of clear and complicated. The reason behind this is that most data is about the organisational and operational environment of the intelligence organisation. It is about the problem of complex environmental phenomena within an organisation that is not necessarily suited to deal with complexity. Table 15 shows the number of data points for each domain, with each five respondent quotes that are illustrative for the data. Below the figure the domains are described based on the data.

Domain	Data points	Illustrative respondent quotes
Clear	15	• *'As intel creatures we very rigidly live in our own doctrine.'* • *'Cause and effect [in the operational environment] are easy to understand.'* • *'We have six SOPs [standard operating procedure] at our section, it contains all I need.'* • *'Assignments are not difficult, provided you have enough time, a good team, and good leadership.'* • *'We still use Russian doctrine and doctrinal templates from before the war [in Ukraine], while things have changed.'*
Complicated	11	• *'It's important to know who you can go to for SME opinion [subject matter expert]'.* • *'There is a repetition; it's looking back. A good chunk of my predictions becomes true.'* • *'Making intel assessments takes guts and requires seeing patterns.'* • *'[cause and] effect are difficult to see, but not impossible.'* • *'We look to the Russian psyche and culture to understand Russia, more than we use Russian doctrine or tactics.'*
Complex	38	• *'Yes environment is complex, the question is – how is it complex?'* • *'We [NATO] suffer from self-imposed complexity.'*

		• *'He [the commander] is looking for certainties where there are none.'* • *'The complexity is that a warfighting corps is different from NATO structure and experience.'* • *'The problem with intelligence and the military in general is that they want to know everything and want to do too much. That is impossible with complexity.'*
Chaos	1	• *'The Russians are good at chaos management because with them everything is always in a bad condition.'*
Confused	10	• *'It takes you years to realise what you should be doing.'* • *'It is in NATO's military culture that it's not always clear what to do. Often there's no job description and people do not feel empowered or comfortable to do their job.'* • *'Decision-making processes for exercises and operations run parallel, making it quite confusing.'* • *'I'm in the first year of my position, I'm still landing. Understanding the work comes after the first year.'* • *'At least the basics of the intelligence cycle should be known to new personnel. Often this is not the case and people are not up to the task.'*

Table 15: Data per Cynefin domain.

Data in the clear domain speaks about causality that is obvious, looking for certainties, standard solutions, and the value of doctrine. A noteworthy issue that manifests from this data is that on several instances a new intelligence requirement was answered by taking an older product and updating it with recent information and other products. While this is understandable regarding the challenges of

collection and time constraints, it is also a way to make complicated questions clear, thereby actively moving between domains.

Data relating to the complicated domain mainly concerns the value of subject matters experts and the need for analysis, as good practices. This is needed because cause and effect, in this case Russian culture and military activities, are difficult to understand and require specific knowledge. On several instances analysis was described as finding patterns in data but also with regard to Russian troop movements and activities. This ties back to a positivist worldview and causality that is knowable.

Data relating to the complex domain often has the words complex or complexity in it. More than just jargon it refers to an actual, albeit implicit, understanding of complexity. Situations such as NATO organisational constraints, the Russian speaking minorities in the Baltics, or hybrid warfare are called complex by the respondents because of ambiguity, uncertainty, and their interconnectedness. As such there is no standard response or analytic method. Re-purposing of existing capabilities to solve complex problems is not observed.

The chaos domain has only one data point. It concerns a respondents who stated the Russian Armed Forces are good at chaos management because they always struggle with poor logistics, old technology, etc. to such a degree that every endeavour is uncertain and full of risk.

Several data points fall outside, or between, the domains as they are about confusion. These concern respondents that did not know how to do their job properly because of a lack of training, mentoring or missing procedures and processes.

The result of plotting data and earlier conclusions in Cynefin reinforces the conclusion that intelligence is not geared towards its complex environment. The case study confirms the theory from Chapters 2 and 3 that intelligence missed the complexity turn while its environment is becoming increasingly complex.

8.4 Design properties

The alignment problems of the intelligence organisation of the corps, internally, with other divisions/sections, and with think thanks, academia, or NATO organisations outside the chain of command impairs performance. Issues of alignment manifest throughout all chapters and several major issues feature in section 7.3. This section focuses on how this problem can be further analysed with complexity science. It does so by using the three design properties of complex systems from section 4.4: requisite variety, sensemaking, and organisational learning.

8.4.1 Requisite variety

For MNC NE to match the variety and complexity of its operational environment, as the law of requisite variety prescribes, diversity of the workforce is most important. Within MNC NE diversity was most visible through the different nationalities of the staff. At each level of MNC NE the staff had very diverse nationalities. Staff originated from MNC NE's host nation countries (Poland, Baltic States), other Eastern European countries (e.g. Romania, Hungary), western continental European countries (e.g. Germany, Denmark) and from the Anglo-Saxon countries (e.g. US, UK, Canada). In most units, host nationals were largely represented: units that were based in Poland had relatively much Polish personnel, while the NFIU Estonia had a large share of Estonian staff.

As a result of their multinational nature, MNC NE's units were internally varied on a number of issues. These included the level of Russian language capabilities, cultural understanding, the threat perception, and the national network to tap into. However, apart from having different nationalities, most staffs were rather homogenous. With a few exceptions, they were male, had an army background, and were between 35 and 50 of age.

Within MNC NE only few staff brought different cognitive backgrounds with them. Most often these different backgrounds were the results of academic education. Examples included economics, political studies, public administration, and leadership. These perspectives clearly facilitated diverse thinking and stimulated discussion. An example is that, regardless of any expertise or background, the intelligence personnel is mainly responsible for the PMESII format of intelligence products. However, sufficient knowledge to cover the other topics is lacking and therefore done by other staff disciplines such as CIMIC and STRATCOM, see section 7.1.3. Also, MNC NE units had hardly any civilian staff, nor were civilian partners or partners outside the chain of command considered, reflecting a traditional military model. This makes sense for tactical units in case of war, but it also impairs getting

knowledge during peace conditions. Furthermore, the respondents signalled the value of outside knowledge because, regardless of peace time, organic intelligence missed expertise on various topics. In order to not become too complex itself by trying to cover a broad and diverse set of information requirements, an organisation must seek answers from partners instead.[602]

Overall, while acknowledging some diversity, the respondents considered the extent of different ways of thinking too limited. A clear example is the staff's limited experience with social media, that was considered a very important source (see section 7.1.2). The respondent's observation of too little diversity, or not actively managing the present diversity, is in line with an important prerequisite for the law of requisite variety. The law does not mean that an equal variety is of itself an effective response, but it is necessary. The different states of the system that come from its variety must still generate effective responses that match against the environmental conditions.[603]

Diversity was only managed insofar as there was the opportunity given other tasks and only concerned functional diversity. This is in line with other empirical findings on diversity in a military setting.[604] Diversity management proper however is concerned with leveraging the qualities and capacities, not job title, of different individuals.[605] In lacking all this, the intelligence staff's ability to address the variety and complexity in MNC NE's operational environment was severely strained.

8.4.2 Sensemaking

The second design property for organisations to address complexity is sensemaking. As for MNC NE, many instances of sensemaking were observed. Informal mechanisms to conduct sensemaking consisted of discussion amongst colleagues on

---

[602] S. Rietjens, "The Future of NLD DISS: A Complex Perspective," *Militaire Spectator* 191, no. 9 (2022): 16.

[603] Bar-Yam, "Multiscale Variety in Complex Systems," 37.

[604] Femke Bosman, "Uniformed Diversity: A Multifaceted Approach Towards the Diversity Climate in the Netherlands Defence Organisation." (University of Tilburg / Netherlands Defence Academy, 2008); Fleur Ter Meulen, "Diversiteit in Inlichtingenorganisaties" (Netherlands Defence Academy, 2022).

[605] Andri Georgiadou, Maria Alejandra Gonzalez-Perez, and Miguel R. Olivas-Luján, "Diversity within Diversity: Equality and Managing Diversity," in *Diversity within Diversity Management*, Advanced Series in Management (Emerald Publishing Limited, 2019).

(the quality of) intelligence products. These took place frequently, but mostly occurred within one branch only. Cross-disciplinary discussions between members of different branches were rare. Another informal mechanism was the establishment of small communities to reflect and discuss intelligence related topics. Formally, the coordination boards and meetings were designed to facilitate collective sensemaking. However, as section 6.3 outlined, there was little room for discussion and intelligence fusion.

The level of sensemaking depended on several issues. First of all, the diversity of the staff, both culturally and cognitive, see sections 6.2.3 & 7.2.3. Second, the amount of slack resources, i.e. buffer capacity. Many staff had a unique background and position in the intelligence production process. This implied that when one staff member was inactive due to leave or illness, there was often no replacement. This hampered the (sustainment of the) intelligence process. Third, while several respondents stated that they were open to new insights and different analytical frames, others were less responsive. When a staff member in Adazi introduced the highly relevant theoretical concept 'reflexive control' to assess the Russian way of warfare, only few colleagues were open to discuss and reflect on this concept.[606] Finally, the lack of interoperable ICT systems (see section 7.3) hampered the quick exchange of different viewpoints amongst the staff.

The little sensemaking effort there is, besides the issues mentioned so far, is often geared towards the interpretation of available intelligence by comparing and aligning assessments. However, Weick states interpretation is a component of sensemaking but is not the same.[607] While interpretation often relates to a product or some end state, sensemaking is about a process or an activity. Furthermore, interpretation implies that there is something to be discovered or approximated, whereas sensemaking *'is less about discovery than it is about invention'*.[608] *'Sensemaking is about the ways people generate what they interpret.'*[609] In other words *'sensemaking thus involves not merely interpretation and meaning production but the active authoring of the situations in which reflexive actors are embedded and*

[606] Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (2004).

[607] Weick, *Sensemaking in Organizations*, 7.

[608] Ibid., 13.

[609] Ibid.

are attempting to comprehend."[610] This is reminiscent of the comment from the first chapter that instead of describing the world as it is, intelligence analysis 'actively creates' the world.[611]

Using a sensemaking lens finds that while efforts are made to align intelligence perspectives in the corps they are far from being a constant and reflexive process about inventing the dots.

8.4.3 Organisational learning

The third design property is organisational learning. Learning is present when actors within an organisation reflect on major challenges or problems that may arise and take corrective actions to adjust organisational behaviour. From organisational learning literature a helpful concept in analysing MNC NE's efforts is single/double/triple-loop learning. Whereas single loop learning refers to actors making simple adaptations and taking corrective actions, double loop learning involves reframing and seeing things in novel ways. Triple loop learning entails actors developing new processes or methodologies for arriving at such re-framings.[612]

At the individual and unit levels, single loop learning happened through working groups, briefings and presentations. Often, however, there were no formal procedures to codify experiences or lessons learned. While some staffs and units recorded their experiences and lessons, often in self-developed formats and reports, most paid no attention to this. This led to fragmentation and hampered structural comparison and analysis of the lessons learned. And, although during exercises NATO's Lessons Learned system was applied (see section 6.2.2), this did not lead to many corrective actions.

At the level of double loop learning, i.e. of reframing, one saw a debate what strategy to follow: preparing for a future Article 5 situation or addressing current grey zone threats. This had many implications such as the intensity and frequency of exercises, and the focus of the intelligence efforts. Also, the intelligence efforts were directed

---

[610] Andrew D. Brown, Ian Colville, and Annie Pye, "Making Sense of Sensemaking in Organization Studies," *Organization studies* (2015): 267.

[611] Fry and Hochstein, "Epistemic Communities: Intelligence Studies and International Relations," 25.

[612] A Georges L Romme and Arjen Van Witteloostuijn, "Circular Organizing and Triple Loop Learning," *Journal of organizational change management* 12, no. 5 (1999).

at conventional land forces and emphasised tangible issues such as the forces' disposition, their capabilities, and leadership. Air and naval issues as well as less tangible aspects including morale of the troops and their mode of operation were, however, often not addressed (see section 7.1.1). Although many individual respondents recognised the importance of these, MNC NE was not able to embed this at an organisational level, because of the larger organisational design of military command hierarchy. In other words, the organisation was geared towards solving puzzles according to the traditional intelligence paradigm, with individuals questioning the validity of this.

Finally, triple loop learning seeks to enhance the fullness and depth of learning about complex issues and dilemmas.[613] To this end, actors link together in an overall learning infrastructure, but also develop new processes and methods to use this infrastructure. Within MNC NE, linking the different actors inside and outside the organisation happened to a limited extent as section 7.3 on alignment illustrates. In terms of new processes and methods, the use of open sources is particularly challenging. Although many respondents considered open sources of great importance, MNC NE was not able to establish an effective process to optimise the OSINT process. The analysis showed many different challenges, including technical access, the absence of specific open source collection tools, the staff's limited knowledge of and experience with conducting OSINT, language capabilities, circular reporting and information overload. The same goes for the integration of data science and quantitative methods. Until now the corps mainly experiences the challenges of the information revolution and none of its benefits (see section 3.3.2). MNC NE could significantly benefit from improving its OSINT process, and incorporating more qualitative methods.

8.5 Conclusion: How do military intelligence organisations deal with their complex operational environment?

The research data show the perception of the intelligence cycle and which intelligence theory the respondents adhere to, clearly fall in the ordered domains of Cynefin. The codes directly relating to Cynefin however, show the most data in the complex domain. This is because this data is about the need for more complexity

[613] de Waard et al., "Learning in Complex Public Systems: The Case of Minusma's Intelligence Organization."

awareness and not the actual presence of this awareness. This is in line with the institutional dynamics and the moderate operational complexity perceived by the respondents in the previous chapter. This makes that MNC NE and its intelligence organisation do not cope well with its, even moderately experienced, complex operational environment. The environment is only partially recognised as complex, and only at the individual level. Meanwhile the organisation is modelled on clear and complicated problems and standard solutions, even though a large number of respondents experience difficulties because of this misalignment.

In conclusion, this misalignment means the schemata used by the intelligence organisation of the corps do not fit its complex environment; broader organisation and operational environment. There is in fact little actual dealing with, or adapting to, the complexity of the environment. As such, there is no sufficient co-evolution between the intelligence organisation and its environment. Only the environment poses an influence and the organisation merely reacts but does not evolve to, in its turn, influence its environment. Here as well, the habitus is crooked as the theory of practice does not fit the environment. This underlines the conclusion of Chapters 2 and 3 regarding the contrast between a complex environment and an intelligence system built for clear and complicated problems. This is a far-reaching conclusion given the overlap between NATO and national intelligence doctrine and procedures – collectively seen as the Western intelligence system.

This misalignment between the intelligence organisation of the corps and its environment is further examined with the design properties of requisite variety, sensemaking, and organisational learning. All three properties are minimally present. There are some initiatives for improvement that fit the category but these only exist locally or temporarily. The design properties make clear why the corps is hindered to show more complex behaviour. This logically means the same properties, among other concepts, can provide opportunities to improve. This will be the subject of the final, concluding chapter.

9. Conclusion, Reflection, Recommendations

This final chapter consist of three sections. The first section provides the conclusion of this research. The second section serves as a reflection on the research. Finally, the last section suggest recommendations for expanding the complexity-intelligence nexus.

9.1 Conclusion: How can complexity science advance intelligence transformation?

This research aims to contribute to the study of intelligence, not complexity science. Overall it shows how complexity thinking and methods relate to intelligence and how these can help advance its transformation, to adopt to an increasingly complex world.

To this aim, the problem statement *How can complexity science advance intelligence transformation?* is supported by four research questions:

1. *What is the status of intelligence transformation?*
2. *How did the intelligence habitus evolve?*
3. *How does complexity science relate to intelligence*?
4. *How do military intelligence organisations deal with their complex operational environment?*

Before answering the main research question this section starts with a summary of the preceding chapters and their answers to the four research questions.

Chapter 1 sketches the research puzzle: The security environment is increasingly complex, yet intelligence does not incorporate knowledge from complexity science. That provides the problem statement: *How can complexity science advance intelligence transformation?* Intelligence transformation is a fundamental change, a paradigm shift.

Chapter 2 examines the first research question *What is the status of intelligence transformation?* To establish a baseline on intelligence transformation the chapter investigates three focal points of fundamental change: a growing critique on the intelligence cycle model, a diversification of theories, and a debate about a paradigm shift. In the literature these are often described with complexity-related

terminology. The chapter finds that there is an early paradigm shift in so far that there are deep cracks in the traditional paradigm. These cannot be explained with, or incorporated in, existing explanations of intelligence. The increased complexity of the operational environment and security context, studied in a fragmented debate, result in much ambiguity on the form and role of intelligence. Intelligence is in a postmodern condition where different interpretations of intelligence exist simultaneously.

Chapter 3 looks at the second research question *How did the intelligence habitus evolve?* The purpose is to examine how the critique on the intelligence cycle, theoretical diversification, and a possible paradigm shift – including their complexity connotations – relate to broader developments influencing intelligence. It shows how great power politics, technological developments and formative events (external drivers) – as the practical dimensions of the intelligence habitus – constitute increased complexity while the theoretical dimensions of debate and institutionalisation (internal drivers) are lagging behind in response. This also connects back to Chapter 2 and the complexity-related critique on the cycle, intelligence theory, and paradigm debate.

Chapter 4 expands on the intelligence-complexity nexus in answering the third research question *How does complexity science relate to intelligence*? It finds that the nexus between intelligence and complexity is understudied. It identifies Cynefin, the puzzles/mysteries/complexities typology, Jominian and Clausewitzian understandings of intelligence, Rumsfeld matrix, and a β-approach as complexity lenses for intelligence. In addition, the four complexity characteristics self-organisation, emergence, non-linearity, and adaptation are adopted into the research method – as well as the design properties requisite variety, sensemaking, and organisational learning.

Chapter 5 presents the methodology of the case study research into the intelligence organisation of MNC NE. This research uses a qualitative method in a single-case study. It is based on empirical data about how intelligence practitioners comprehend and handle their complex environment. The description of the data initially keeps close to the wording and worldview expressed by the respondents. In a second stage the data is analysed with concepts and ideas from Chapters 2, 3, and 4. These act as a lens to examine the empirical data with.

Chapters 6 to 8 examine the fourth, and last, research question *How do military intelligence organisations deal with their complex operational environment?* After

introducing the intelligence organisation of MNC NE, Chapter 6 describes its environment in the terms used by the respondents: *peacetime, hybrid, or Article 5?*, *exercise mode versus real life*, and *national versus NATO interests*. The chapter finds that the respondents talk about the broader NATO organisation and the operational environment as interconnected and external factors. These are seen as the origin of many challenges that exist within the corps' intelligence organisation. Remarkably, empirical data contained more on problems within NATO than about Russia or other threats. This *'self-imposed complexity'* frustrates much of the intelligence work. Then the analysis of the data on the environment is done using the four complexity characteristics of self-organisation, emergence, non-linearity, and adaptation. The cumulative conclusion of these characteristics is that the respondents experienced moderate environmental complexity. This contrasts with general consensus in professional and academic literature regarding the increased complexity of the military operational environment. Two factors are fundamental in this. First is the tendency to make all problems simple. This is intuitive and by training, as well as enforced because the methods and processes of the intelligence organisation are designed for simple problems. Second, knowledge on complexity, and its methods, was lacking among the respondents.

Chapter 7 describes the organisation of intelligence within MNC NE in respondent terms. This is reflected in the three sections of the chapter: the intelligence cycle, reflections on practice, and issues of alignment. The respondents mainly have problems with the intelligence cycle because it is not functioning as it should do, according to doctrine, within the corps The products and methods form the intelligence practice for observing and measuring of reality, or collection and processing in an intelligence context. Any deficiencies in this are seen as the result of a lack of resources, mandate or otherwise practical circumstances and conditions. With regard to alignment, internally this is primarily frustrated because of the mismatch between force and command structure that in its turn impacts command and control. There is almost no outreach outside of the chain of command to peer units or non-military partners.

Chapter 8 presents the analysis of the intelligence organisation of the corps. In general the respondents are proceduralists and do not think outside the intelligence cycle. It can be seen as a cybernetic feedback loop where only a change of direction input can lead to any adaptation. This is in stark contrast with critical perspectives and academic literature that problematise this traditional understanding of intelligence as a command-driven cycle, applicable in any circumstance and

environment. This forms another dimension in the gap between the practical dimensions of intelligence and intelligence theory.

With regard to theory the overall stance of the respondents is a positivist one and nuances exist few and far between. The larger implication of this is that the military intelligence workforce employs a worldview, and methods, that are increasingly out of touch with the complexity of the practical dimensions of intelligence

When analysing the raw data and earlier conclusions with Cynefin most data points fall in the complex domain. This is in contrast to the intelligence cycle and theory that fall in the ordered domains of clear and complicated. The reason is that most data is about the organisational and operational environment of the intelligence organisation. It is about the problem of complex phenomena within an organisation that is not necessarily suited to deal with complexity. This also underlines earlier conclusions on the gap between an intelligence organisation that is not suited to address the complexity of its environment. The case study confirms the theory from Chapters 2 and 3. The intelligence organisation of MNC NE operates according to schemata that do not fit its organisational and operational environments. The lack of successful co-evolution with its complex environment results in an adaptation failure. This is examined further with the three design properties of requisite variety, sensemaking, and organisational learning. The minimal presence of each property within the corps shows why it is hindered to show more complex behaviour.

The research questions are sufficiently addressed to answer the problem statement. Furthermore, throughout the chapters, two intelligence paradigms appear; a traditional intelligence paradigm for ordered problems and an intelligence paradigm that is tailored towards complex problems. Table 16 juxtaposes both paradigms at the end of this section. While these paradigms are extremes, many in-between modes of intelligence exist.

The traditional paradigm has a worldview that the intelligence environment is knowable and measurable, as long as sufficient resources are available. In this, it is a positivist persuasion. It is also linear, meaning cause and effect are observable. As a result, logical reasoning will usually get a long way, and prediction – to a degree – is possible. Hereby, intelligence problems are seen as puzzles: The problem is finite and an answer or solution exists. It is a sort of formula that needs data, or in other words, a puzzle consisting of puzzle pieces. The more pieces the better, but if one is missing, its meaning can probably be derived from other, surrounding, pieces. The guiding idea is to eliminate uncertainty through effective collection and analysis. More

information and intelligence means more precise assessments. Any remaining uncertainty is the result of a faulty process, not because of the process itself. It is a very Jominian view on intelligence.

The model of traditional intelligence is the intelligence cycle. It is a cybernetic feedback loop that positions intelligence as the feedback from, and to, policy and decision-making. Within this model there are clearly separated and specialist roles within intelligence (stovepipes), and work is mostly done in a standardised way with procedures and protocols to maximise efficiency (the Fordist intelligence factory). The intelligence function itself has little room to adapt the model. The organisation is primarily based on uniformity, diversity is seen as having different functional areas.

The organisation is steered by decision-making, this process is command-led, very planned and deliberate, and problem structuring is often a onetime occasion at the beginning of the operational process. Any adjustments come down to adhering, repairing, or improving to existing processes (single loop learning) while there is little reframing of problems and seeing things in a different way (double loop learning).

The relation between intelligence and policy or decisionmakers is about telling truth to power. Intelligence, ideally, is objective and at a distance from policy or decision-making. In practice this means many intelligence requirements are answered by a one-time, static pull product.

The method, or practice, of this model is geared to find known unknowns. Identified pieces of intelligence that are missing to fulfil the puzzle are broken down to collectable items in an intelligence collection plan. In other words, the intelligence problem is first analysed, or reduced, to understandable and solvable parts. Second, it is put back together again to understand the whole. The analysis happens through logic and analytic techniques, and is mainly done by humans, supported by software. The analysis is either descriptive, explanatory or prognostic and aimed at proving causal connections. Stated differently, it follows scientific logic by reducing the α, the chance of incorrectly concluding a relation between phenomena exists (Type I error, or false positive).

Next to the traditional intelligence paradigm there also appears an intelligence paradigm that is geared towards complex problems. The worldview of this system is postmodern, meaning reality is unknowable, and measurement is mere interpretation. This is because with complexity cause and effect are non-linear, meaning causality is unclear and leads to unexpected major outcomes. Perhaps

causality can be established in hindsight, but beforehand correlation is the best possible outcome. Complex intelligence phenomena are about problem structuring. Because the problem is unclear and changes, structuring the problem requires constant adjustment. Because of this shifting phenomenon, information on it is often contradictory, false, and uncertain. While this is inherent to information to some degree, the problem is significantly worse with regard to complexity. The goal then is to assess the uncertainty, not solve it. Because of inherent uncertainty, single-point predictions are inaccurate and therefore better analysis should point to more possible outcomes (Clausewitzian intelligence).

The model accompanying this complex worldview resembles a complex system itself. It is an open system with explicit feedback loops. This allows it to adapt and incorporate new perspectives, knowledge and collection methods. As the case study research shows this incorporation is severely impaired in traditional intelligence. Ideally, as with the original OODA-loop, the form of intelligence follows its function: The intelligence problem at hand dictates how the model looks like, instead of a single model being the solution to all intelligence problems. The model most allow for collaboration because alleviation of the problem is only possible through improvisation and innovation. In traditional intelligence practice there are too many stovepipes for this to occur.

The organisation is not only diverse in functional areas or collection assets but, more importantly to understand the environment, it is also cognitive diverse. This enables better variety to deal with the environment. The organisation is steered through sensemaking in a collaborative, iterative, and continuous process of problem structuring. Adjustments to the organisation happens through mature double loop learning or to full triple loop adaptation.

This means the relation between intelligence and policy is one of involvement. The relation is close, continuous, and mutually influencing to enable maximum sensemaking of the problem.

Methods in this model look for unknown unknowns. Instead of breaking down the problem and disregarding intelligence that does not fit the chosen analysis path, synthesising all available intelligence is necessary not to miss a threat and discover unknown unknowns. To enable this, and guard against an overload, a data-driven approach is needed in addition to qualitative methods. An example of this is Activity

Based Intelligence (ABI).[614] This method *'uses a large volume of data from a variety of intelligence sources to enable data correlations that, among other things, drive discovery of weak signatures and patterns in a noisy data environment'*. It allows analysts to *'correlate activities, detect anomalies, and discover links between objects'*.[615] This would mean a severe increase in data software and computing power to enable human-machine teaming in intelligence analysis. The ideal is to use foresight and anticipatory methods to identify more possible outcomes instead of narrowing down to a most likely and most dangerous scenario as is staple among military intelligence. To not miss a threat and discover unknown unknowns the model should allow for a β chance (Type 2 error, false negative) approach.

Traditional intelligence paradigm	**Complexity intelligence paradigm**
Worldview	
Positivist (world is knowable).	Postmodern (interpretation).
Linear, causality observable.	Non-linear, correlation at best.
Puzzle solving (problem is finite, solvable).	Problem structuring (problem is unclear, changing).
More information = more precision.	Information is contradictory, false, uncertain.
Jominian intelligence.	Clausewitzian intelligence.
Model	
Cybernetic intelligence cycle.	Adaptive system.

[614] See also: Patrick Biltgen and Stephen Ryan, Activity-Based Intelligence, (Norwood: Artech House, 2015); Lawrence, "Activity-Based Intelligence: Coping with the" Unknown Unknowns" in Complex and Chaotic Environments."; Gregory Treverton, "Creatively Disrupting the Intelligence Paradigm," *ISN Security Watch* (2014).

[615] Chandler P. Atwood, "Activity-Based Intelligence: Revolutionizing Military Intelligence Analysis," *Joint Force Quarterly: JFQ*, no. 77 (2015): 26.

Stovepiped and specialised (Fordist intelligence factory).	Collaborative.
Standardisation.	Improvisation/innovation.
Organisation	
Uniformity, functional diversity.	Requisite variety, cognitive diversity.
Decision-making, command-led, planned, one-time problem structuring.	Sensemaking, collaborative, iterative, continuous problem structuring.
Single & double loop learning.	Double & triple loop learning.
Relation with policy	
Objective, separate (Telling truth).	Involved.
Static pull product for Commander.	Continuous sensemaking.
Method	
Known unknowns (intelligence collection plan).	Unknown unknowns.
Analysis / reductionism.	Synthesis.
Analytic techniques and logical reasoning.	Data-driven (activity-based intelligence).
Processing by humans.	Processing by human-machine teaming.
Descriptive, explanatory, prognostic (forecast).	Foresight, anticipatory.
Reduce α chance, Type 1 error, false positive.	Reduce β chance, Type 2 error, false negative.

Table 16: Traditional versus complexity intelligence paradigms.[616]

[616] Compiled by author.

The answers to the four research questions, combined with Table 16 that contrasts the traditional paradigm with a complexity paradigm, enable to address the problem statement *How can complexity science advance intelligence transformation?*

Complexity science can advance intelligence transformation by providing alternative insights, tested in broader military sciences and other related fields, to improve its performance. This research shows how complexity, first of all, has a lot in common with intelligence. Both fields are concerned with how a system can understand its environment and how it processes information to do so.

The research finds intelligence is failing to adapt to a complex environment. Meanwhile the field has missed the complexity turn, a broader social science adoption of the ideas and methods of complexity science. This research shows how the external drivers, or practical dimensions, of great power politics, technology, and events constitute an increasingly complex world. However, this is not reflected by debate and institutionalisation as internal, theoretical drivers of intelligence. Neither is it reflected by the empirical data. Plotted in Cynefin the data shows an organisation designed for clear and complicated problems, struggling with moderate complex phenomena. This design failure is exemplified by the US Army Field Manual 2.0 *Intelligence* (2023). In the introduction it states: '*Providing effective intelligence is becoming more challenging as operations become more complicated. The current operational environment (OE) is dynamic, complex, and shaped by the intersection of worldwide trends driven by globalization, technology, climate change, shifting geopolitics, and varying stages of conflict and resolution.*'[617] Without realising the writers point out the problem of intelligence, as concluded in this research: conducting complicated operations in a complex environment. This doctrinal publication is a very practical example of missing the complexity turn in intelligence.

Still, several anomalies appear. The critique on the intelligence cycle, the diversification of theory, paradigm issues, and initiatives by respondents that go against traditional intelligence all resonate some form of complexity thinking. In doing so, they form cracks in the traditional intelligence paradigm but it is still far away from any complexity turn.

Complexity science offers a language and understanding to further examine these anomalies – just as it does for examining the gap between a complex environment and an intelligence paradigm meant for solving puzzles. With complexity a new

[617] "Field Manual 2.0 Intelligence," (US Army 2023).

intelligence paradigm is formulated, and contrasted to the traditional intelligence paradigm. The three design properties (requisite variety, sensemaking, and organisational learning) show how concepts from complexity can help to move from the traditional to the new, complexity paradigm.

With these insights this research adds to the debate around the intelligence cycle by explicitly framing it as a cybernetic feedback loop, something that is new even to the latest research on the intelligence cycle.[618] It also adds a voice to a growing volume of post-positivist intelligence theory. This research continues the paradigm debate past the non-state actor turn and formulates a new, complexity paradigm. Another theoretical contribution is the development of intelligence in the framework of Buzan and Hansen, that links intelligence studies to related fields such as security studies and international relations. More theoretical contribution is made by comparing intelligence to broader military science and the study of war and warfare. This research makes a contributions to research practice; it shows the role of military security and secrecy in scientific fieldwork, something which is rarely addressed in a practical manner.[619] Lastly, this research provides some insight into NATO – which is very relevant considering the developments on the alliance's eastern border.

9.2 Reflection

This section on reflection consists of three parts: theoretical, methodological, and personal. Regarding theory, while the nexus on intelligence and complexity in literature is small in volume, this research shows the usefulness and value of using complexity science to examine intelligence. It showed how intelligence missed the complexity turn in social sciences while there is a general agreement that the modern operational environment is complex. It also showed how characteristics and design properties of complexity shed new light, and offer novel solutions, on intelligence problems. Especially the Cynefin framework enables an application of complexity thinking to organisational problems. Besides the intelligence-complexity

[618] Daniel Tallat Rønn Shakoor, "The Intelligence Cycle in Denmark: Unwinding and Reconceptualising the Process of Formulating Intelligence Requirements Surrounding the Middle East in the Danish Defence Intelligence Service" (University of Southern Denmark, 2021).

[619] Sjøgren et al., "Military Security and Research Ethics: Using Principles of Research Ethics to Navigate Military Security Dilemmas," 36.

nexus this research connects theory from security studies, international relations, and broader military sciences.

The most striking theoretical feature of this research is the contradictory need for intelligence organisations to simultaneously be centralised to coordinate all different functionalities, and be decentralised to quickly adapt to emergent issues. This is based on Rovner and Long in section 3.6.2, and emphasised by De Waard et al. in section 4.1.1.[620] This poses a conundrum without an ideal solution, and calls for attention towards the study of the adaptation mechanisms of intelligence systems.

In general, when regarding the role of theory in this research, it was expected the abstraction level of complexity would take some heavy conceptual struggling before it could be sufficiently mastered to apply it to intelligence. While it was by no means easy, in the end, this was not the case. While there is no shortage on abstract, theoretical publications, the literature on complexity also has authors that connect to real world issues in accessible language.[621] Especially Cynefin showed value in understanding complexity, and even more so in analysing the empirical data. Other inroads into complexity were found in broader military science literature, that showed how complexity was adopted into (the study) warfare. This literature, by nature, is closely related to intelligence studies.

The last theoretical reflection is on the Western intelligence system as mentioned in Chapter 5. There it states that the intelligence system under examination in this research can be seen as being valid for all Western, and NATO states. This is based on a unifying effect of shared, or comparable, doctrine within NATO but with more Western partners as well. This in turn is a manifestation of a general desire for military interoperability among Western partners given the international missions of the last decades. This does not mean this Western intelligence system is normative, or exactly the same everywhere. Within the term Western is a variety of intelligence cultures with different histories, threat perceptions, and ideas on intelligence.[622]

---

[620] Rovner and Long, "The Perils of Shallow Theory: Intelligence Reform and the 9/11 Commission," 627; de Waard et al., "Learning in Complex Public Systems: The Case of Minusma's Intelligence Organization."

[621] e.g. Johnson, *Simply Complexity: A Clear Guide to Complexity Theory*; Mitchell, *Complexity: A Guided Tour*; S Page, *The Diversity Bonus* (Princeton: Princeton University Press, 2017).

[622] e.g. Bob de Graaff, James M. Nyce, and Chelsea Locke, eds., *Handbook of European Intelligence Cultures* (Lanham, MD: Rowman & Littlefield, 2016).

There is however enough common ground found regarding the topics examined in this research to call it a Western intelligence system.

When reflecting on the research method, two issues stand out. The first one is the interplay between the empirical data and its analysis. Because the interviews were semi-structured, and the goal was to stay close to the worldview of the respondents, the planned analysis process had to be adjusted as the interviews progressed to fit the analysis to the data instead of vice versa. Initially, the Cynefin framework was used to operationalise questions. Specifically, the type of constraint, practice and action per domain of the framework were transformed into questions regarding the intelligence environment. However, this proved too abstract for the first few respondents. It required too much immediate reflection and thinking on their part. Therefore the adjustment was made to use the idea of a paradigm for the analysis of the interview data and Cynefin was used to draw inferences from.

Another interplay between data and analysis concerns the alignment terms from Chapter 7 and the design properties that followed from it in Chapters 8 and 9. Initially the idea was that any topics on the coordination of intelligence effort and exchange of intelligence products would fit in the original question set. However, the volume of data on alignment issues called for a section of its own. This realisation, after the first round of data collection, led to the decision to make the alignment issues explicit and specific. This meant formulating extra theory to operationalise questions from and to analyse the data with.

The second methodological issue that stands out is the role of secrecy in doing research into intelligence practice. As described in section 5.2.1, secrecy permeates the entire research. It plays a role in getting access, the possibility of research topics, and storing data. Not mentioned in section 5.2.1, and attesting to the professionalism of the corps' intelligence organisation, is that during the field visits the research team was approached by counter-intelligence officers on two occasions. In a conversation these officers merely wanted to double-check on research agreements made by others for which they were responsible in case of any security issues. Another safeguard was a review by several officers of the corps headquarters. Not only does secrecy limit research opportunities, measures to safeguard it can be time consuming.

These methodological issues lead to the significant question how the case study research method influenced the overall research results, which in turn ties in with issues of validity regarding a single case study (see section 5.2.4). First, the first four

theoretical chapters were written before any serious in-depth exploration of a specific case study. In this sense, as well as the amount of chapters, there is balance. In volume, the theoretical chapters even take up two third of the total wordcount. Second, the conclusion of the case study confirmed the theoretical conclusions to a large degree. Third, the semi-structured form of the interviews, as well as the Gioia method, provide enough space for the respondents to communicate their worldview in their own words, without the data leading to a constant re-evaluation of the theory preceding it. Fourth, the research can be repeated on a different unit of analysis, be it a national intelligence service, deployed military intelligence unit, or private sector intelligence. There is no requirement to change the research method or to delete any case study specific elements in it.

Furthermore, the validity of the research was tested on multiple occasions. The theoretical and case study parts of the research have been presented, separately, and in combination, at (scientific) conferences, in professional military education, and on working floor level. A driving force was the yearly International Studies Association conference. This led to contact and ideas with scholars and ultimately to three publications that tested some of the research conclusions.[623] Regarding education, the research results are integrated into lectures that are part of the curriculum of military cadets, analysts of both Dutch civilian and military intelligence services, and military intelligence officers in the Dutch Armed Forces. On occasion lectures were given at e.g. the Dutch Army headquarters staff, Dutch Special Operations Command, Royal Military College Saint-Jean (Canada), and Mercyhurst University (United States). All these occasions provided the opportunity to get feedback on research insights and results. The lectures were not only a transfer of knowledge, but on several instances led to the adoption of complexity insights and applications. Anecdotally, after a lecture, the commanding colonel of a project team to review the Dutch military intelligence system vowed to *'embrace uncertainty'* in thinking about a renewed system.

[623] Spoor, "Intelligence Adaptation; Insights from Complexity Science and the Need for Analytic Cognitive Diversity." in "Innovations in International Affairs" book series volume, edited by Effie Charalampaki, Czesław Mesjasz and Luis Tomé (Routledge 2025), forthcoming; Spoor and de Werd, "Complexity in Military Intelligence."; Spoor and Rothman, "On the Critical Utility of Complexity Theory in Intelligence Studies."

The last reflection is on the role of the researcher. Being a soldier with experience in intelligence is an integral aspect of this research. Anecdotally, when the researcher was confronted with the scientific term 'unit of analysis' the connotation of 'unit' and 'analysis' was purely military. Also, the term 'informant', that in many research literature is used to mean people to be interviewed by the researcher, had a different connotation entirely. To avoid any conflation with the term being used in matters regarding covert human intelligence sources this research prefers the term 'respondent' instead.

Being an insider of some sorts influenced the conduct of the case study research with regard to getting access and gaining the trust of the respondents, as described in section 5.2.1. Being a soldier with intelligence experience also had challenges. When communicating about, and writing on, the research many intelligence content had to be explained without using too much terminology and insider-speak. For a field that exists largely outside the public eye, and that is rife with abbreviations and acronyms, this was a trying process. Another challenge was when respondents started sharing stories that could be classified, or sensitive otherwise. This meant the ethical restriction on the side of the researcher not to record or use this data.

Still, being a soldier still meant being surprised when finding out a lot of foundational concepts of modern day warfare are based on complexity thinking. This is never addressed during personal professional military education. It provided conceptual linkages that helped to understand complexity and how to apply it to intelligence. This is exemplary for how the research left the familiar terrain of intelligence practice and an international relations master and transitioned into unfamiliar terrain such as, next to complexity science and military sciences, security studies, postmodern philosophy, and organisation theory. This meant both a broadening of perspective and a sharpening of understanding each individual field.

9.3 Recommendations

This section first provides recommendations for the intelligence organisation of MNC NE. Several of those will resonate with general intelligence challenges from broader practice; NATO-wide, national intelligence services, and military units and commands. Second, the section suggests recommendations for further research.

9.3.1 Recommendations for practice

Overall, the respondents are unanimous in concluding that NATO's internal organisational dynamics exacerbate the problem. Particularly the notion that many military issues are interconnected with politics and national interests complicates performance within NATO structures. However, in order to make the outcome of the present study actionable, the recommendations will focus on areas of interest that can actually be influenced by NATO and/or MNC NE on a military level. Therefore, the recommendations will not debate NATO's peacetime mandate and organisational characteristics because these are given political facts. However, it must be stated that, to some degree, these things cannot be separated. The hybridity that Russia employs against NATO and its member states is designed to exploit the current situation without escalating to a level of more direct and open (military) confrontation.

It is important to emphasise that at the military level the issues brought forward in the interviews are interconnected as well. For example, without a prominent role for agreed upon intelligence requirements, current events tend to get most attention, making intelligence collection prone to emergence. Consequently, a self-enforcing collection cycle develops wherein current affairs and open source reporting start dominating the intelligence products. On top of that, the corps has no dedicated capacity to produce usable OSINT. As a result, there is the danger of becoming too reliant on non-validated open source information for decision-making, but also the contamination of key data bases with large volumes of doubtful raw information. Consequently, issues like circular reporting and insufficient source grading pervasively infect the outcome of the intelligence process.

Due to the interconnectedness of factors influencing the intelligence process, the recommendations for the intelligence organisation of MNC NE are divided in two parts. First, referring to requisite variety, organisational learning, and sensemaking as key design properties of complex systems, a comprehensive, yet more fundamental, view on the functioning of MNC NE will be provided. These design properties are operationalised using the case study, but they show how intelligence organisations of all kinds can benefit from insights from complexity science.[624] Second, more practical and easier to address suggestions for improvement will be given for intervening at specific points in the institutional context, and the intelligence cycle and its issues of alignment.

[624] See also: Rietjens, "The Future of NLD DISS: A Complex Perspective."

First, the principle of requisite variety requires attention. Within MNC NE a dual picture emerges. On the one hand, the multi-national composition of the corps creates a base of human resources that is culturally quite diverse, where staff with different historical and societal backgrounds work closely together and share knowledge. On the other hand, the corps' rather traditional deterrence role within the overarching military strategy of NATO has placed the performance focus on manoeuvre warfare. As a result, cognitively the staff is far less diverse. Apart from military knowledge on major combat scenarios, insights and skills are needed to identify and interpret security conundrums that remain below the threshold of war. However, required expertise in for example social media dynamics, cyber tactics, public order, and security challenges, but also in languages, religions, and global micro-regions, is so diverse that structural incorporation within MNC NE seems impossible. Still, it is recommendable to invest in better managing the diversity that is already in place, but also in ways and networks to consciously attract specialised non-military knowledge when needed. Regarding the former, increasing cognitive diversity and/or better managing existing diversity is a recommendation for intelligence in general; NATO-wide, national intelligence services, and military units and commands. Regarding the latter, one could think of creating liaison positions to set up and maintain external relations and establishing formalised relationships with NATO centres of excellence, military academies, and civilian knowledge institutions (e.g. think tanks and universities).

The second property entails the trinity of single, double, and triple-loop learning. It could be argued that within MNC NE single loop learning dominates. However, this learning ability appears local and informal, mainly taking place at the individual and team level without codifying the learning experiences for others to take advantage of. MNC NE's ability for double loop learning (i.e. changing goals or decision-making frames based on experiences) is strained because the formal military deterrence role it has to fulfil does not comply with the equivocal hybrid and grey zone threats the corps is currently facing. Triple loop learning is about actors linking together in a learning structure that generates new frames, methods and processes. The study identifies OSINT as the centre of gravity for fuelling triple loop learning, that as second order effect could help to improve the double loop learning process. In short, if the collection, analysis, and dissemination of open source information is professionalised, relevant societal knowledge impulses can be fed into the ruling military-focused intelligence process, making it possible to combine a military combat focus with a threat assessment of environmental dynamics taking place below the threshold of war. There is however a significant legal issue with regards to

OSINT mandate for military and intelligence organisations in peace-time conditions. This, again, points to problems being interwoven between political and military levels and without sufficient mediation of the issues will continue the usefulness of OSINT and be a handicap for intelligence in the information age.

One level of learning lower, a professionalised OSINT process supports the mitigation of circular reporting and source grading. A low hanging fruit solution for improving OSINT is to start with providing better OSINT training before people actually start working in the J2 branch. A more fundamental consideration is, of course, how to professionalise the entire OSINT process. It evokes additional questions like: What kind of and how many subject matter experts do we need? Do we need in-house staff or can we attract the required specialists trough networking? How do we establish an ample human resource base to safeguard sustainable staffing of OSINT positions?

Sensemaking is about the ability the continuously re-evaluate situational awareness. Currently, within MNC-NE, sensemaking is problematic, because pressing deadlines, daily routines, formalised processes, and personnel shortage, leave hardly any room for people to contemplate and have discussions with colleagues from other J2 sections or MNC NE branches. An important recommendation is, thus, to set-up new or improve existing consultation committees specifically aimed at facilitating the exchange of knowledge and learning experiences between people. Institutionalising the potential of workers to actively and mutually scrutinise existing modus operandi could help to create an atmosphere of continuous improvement.

A second issue that affects sensemaking concerns the disconnect between the functioning of MNC NE during exercises and under regular conditions. The two enactment realities seem to alternate, which causes feelings of confusion among staff. Especially, after Russia had invaded Ukraine the traditional distinction between the two worlds was deemed artificial and even out of place. The fact that most exercises followed a traditional manoeuvre scenario, particularly in comparison to the intricate mixture of overt and covert hostilities actually taking place in Ukraine, further increased these feelings. Respondents stressed repeatedly that the staff does not live up to the key military paradigm of 'train as you fight', disqualifying the enactment logic and patterns of exercises for being obsolete.

Interestingly, however, at the same time many respondents hailed the exercise mode for making it possible to break out of daily routines and transcend ruling stovepiped work relationships. When an exercise had ended people missed the

mutual adjustment dynamics that organically took place during exercises. Knowing that MNC NE has already scaled down its contributions to exercises not directly benefitting its mission, the present study shows that investing even more effort in bringing the two worlds closer together could offer major performance gains. Developing realistic scenarios and preparing the corps in different exercises for a variety of task settings is one of the most promising measures to take. For intelligence units especially, the closer the scenario is to reality, the better it can be trained for the hybrid complexities of today. After all, when the depth, richness, and vastness of real-life information clouds are captured in scenarios, intel specialists are actively challenged to dissect such conundrums into viable and military relevant intelligence products. Another, perhaps more difficult path to travel, is to try and mimic the behavioural interaction patterns of exercises in the regular working routines of MNC-NE.

Next to these suggestions based on design properties, the following four practical avenues for improvement are suggested. First, the IRM&CM functionality needs a revival to improve the horizontal and vertical alignment of the intelligence process. Deliberately managing the operationalisation of intelligence requirements could offer a shared intelligence mind-set that facilitates cooperation between the different J2 sections and that synchronises the key echelons in the intelligence chain. In addition, an initial quick win would be to use the doctrinal terms of 'planned' and 'emerging' intelligence requirements to differentiate between the requirements from the Intelligence Collection Plan and those derived from current events. This helps to manage and balance effort and resources. To some degree at least, as emergent issues are inescapable in a complex world. Furthermore, the perspective of the analysts also determines if something is considered emergent or not.

Second, two intel collection issues need consideration. To start with, making collection requirements explicit could help to streamline demand-supply relationships within the intelligence chain, also improving internal accountability. Next, the use and knowledge of relevant databases varies considerably between the individual respondents. Preparatory training could easily address this problem.

Third, concentrating on intelligence processing, the problems with transforming open source information into relevant and reliable intelligence stand out most. Apart from the fundamental changes discussed earlier, a more concrete improvement would be to provide training in structured analytic techniques. This would offer analysts a proven and standardised method of working.

Fourth, dissemination appears to be push-oriented with MNC NE's commander as the sole consumer. A revived IRM&CM framework could guide the dissemination of intelligence to a broader audience and familiarise other sections with the existing portfolio of intelligence products.

9.3.2 Recommendations for further research

This last part of this section, and research, suggests recommendations for further research. The obvious recommendation is to call for more research on the intelligence-complexity nexus. As this research shows, applications of complexity science to intelligence are sparse. This research aims to address this but can only scratch the surface. Because complexity science offers a broad research agenda for intelligence, future research could elaborate on many things from applying computational methods to literature on planning and management in complexity, and from spatial/geographic complexity to complexity in political science. This call for more research on the nexus is directed towards intelligence, and complexity related fields and disciplines from outside the intelligence sphere.

A pertinent issue for more complexity research into intelligence, as mentioned in the section on reflection, is the issue of design. How to create an organisation that is suited to the task at hand but at the same time is quick to adapt to any new circumstances? This research does not mean to portray traditional intelligence as simple or easy, it is still difficult. More important, it is still relevant – only not for all intelligence problems. However, it is not about one system being better than the other, it is about using the right one for the problem at hand. It is about adaptation to changing circumstances. In reality, both traditional and complexity intelligence systems would be the extremes and the intelligence problems distributed along ranges between these extremes. Not all intelligence problems are either clear or complex. Furthermore clear problems can have complex aspects, and vice versa. Another interesting thought is offered by De Werd who states *'the problem typology of puzzles, mysteries and complexities should be seen more as a matryoshka doll: puzzles are workable simplifications but never excuse analysts from reflexivism'*.[625] This brings us back to the question how an organisation can be designed to adapt between both intelligence paradigms.

Getting perspectives on how this adaptation can look like, are helpful in designing other intelligence systems. A starting point can be derived from Hammond's article

[625] Peter de Werd, "Reflexive Intelligence and Converging Knowledge Regimes," *Intelligence and National Security* 36, no. 4 (2021): 513.

'Intelligence Organizations and the Organization of Intelligence'.[626] In his article Hammond shows that Cold War intelligence saw discussions on how to organise along two contradictions. The first contradiction is the need for centralised command to coordinate the many aspects of intelligence versus the need for decentralisation to be more adaptable for complex situations. The second contradiction is if intelligence should be organised geographically or thematically? However, Hammond also concludes that during these Cold War discussions no scholar *'provided a method for determining the circumstances in which one structural design might be better than another'*.[627]

Another possible starting point is Volberda's idea of organisational flexibility.[628] This is a two-dimensional concept. It is about a managerial task, or control capacity, on one side. The other side is about the organisational design task, or the controllability of the organisation. Both tasks need to be fit for the environment. The managerial task is to know how to harness which capabilities of the organisation sufficiently to deal with changes in the environment, called the 'sufficiency of flexibility mix'. In addition Volberda states an organisation needs to actively study this sufficiency of flexibility to learn from it. The design task is to realise an organisation that is responsive to the flexibility mix. The organisation should create conditions that foster flexibility, called 'adequacy of organizational design'.[629] While there is no room here to go into details, both Hammond and Volberda offer promising concepts to examine how intelligence adaptation can look like.

Other recommendations for further research concern the intelligence cycle. The cycle in the traditional intelligence system is intended for major combat operations, but as the case study shows, has severe shortcomings in a hybrid context. This brings up the question if, and when, and what shortcomings manifest? Research into the boundaries of the cycle – when is it (no longer) useful? – as well as the search for an

---

[626] Hammond, "Intelligence Organizations and the Organization of Intelligence."

[627] Ibid., 703.

[628] Henk W Volberda, "Toward the Flexible Form: How to Remain Vital in Hypercompetitive Environments," *Organization science* 7, no. 4 (1996); Henk W. Volberda, *The Flexible Firm. How to Remain Competitive* (Oxford: Oxford University Press, 1998).

[629] See also: Amaia Sopelana, Martin Kunc, and Olga Rivera Hernáez, "Organizational Flexibility: A Dynamic Evaluation of Volberda's Theory" (paper presented at the 28th International Conference of the System Dynamics Society, 2010).

alternative (model) are much needed in stimulating a critical reflection on the archetypical model of intelligence.

Expanding non-positivist intelligence theory, and further defining intelligence paradigms is a recommendation to stimulate scholarly reflection as well as the theoretical development of intelligence. On top of that, well thought-out paradigm formulations, offer insights for changing intelligence practice.

Lastly, research on NATO intelligence is encouraged, as well as empirical research into how different intelligence organisations, make sense of their complex environment. It would be especially interesting to examine intelligence organisations outside the western space.

Bibliography

Agrell, Wilhelm. "Intelligence Analysis after the Cold War." In *National Intelligence Systems: Current Research and Future Prospects*, edited by Gregory F. Treverton and Wilhelm Agrell, 93-117. New York, NY: Cambridge University Press, 2009.

———. "The Next 100 Years?: Reflections on the Future of Intelligence." In *The Future of Intelligence*, edited by Isabelle Duyvesteyn, Ben De Jong and Joop Van Reijn, 133-48. London: Routledge, 2014.

Agrell, Wilhelm, and Gregory F. Treverton. *National Intelligence and Science : Beyond the Great Divide in Analysis and Policy.* Oxford ; New York: Oxford University Press, 2015.

Aid, Matthew. "Us Humint and Comint in the Korean War: From the Approach of War to the Chinese Intervention." *Intelligence and National Security* 14, no. 4 (1999): 17-63.

Alberts, David S, and Thomas J Czerwinski. "Complexity, Global Politics, and National Security." Washington D.C.: National Defense University, 1997.

Aldrich, Richard J. "Beyond the Vigilant State: Globalisation and Intelligence." *Review of International Studies* 35, no. 4 (2009): 889-902.

Allison, Roy. "Russian 'Deniable' Intervention in Ukraine: How and Why Russia Broke the Rules." *International Affairs* 90, no. 6 (2014): 1255-97.

Almäng, Jan. "War, Vagueness and Hybrid War." *Defence Studies* 19, no. 2 (2019/04/03 2019): 189-204.

Anderson, P. W. "More Is Different." *Science* 177, no. 4047 (1972): 393-96.

Andrew, Christopher. "Intelligence, International Relations and 'under-Theorisation'." *Intelligence and National Security* 19, no. 2 (2004): 170-84.

———. *The Secret World: A History of Intelligence.* Yale: Yale University Press, 2018.

Andrew, Christopher, and David Dilks. *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century.* London: Macmillan 1984.

Andrus, D. Calvin. "The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community." Washington DC: Central Intelligence Agency, 2005.

Aradau, Claudia, and Mc Cluskey. "Critical Security and Intelligence Studies." In *A Research Agenda for Intelligence Studies and Government*, edited by Robert Dover, Huw Dylan and Michael S Goodman, 2-21. Cheltenham: Edward Elgar, 2022.

Australian Army Headquarters. "Army's Future Land Operating Concept: Adaptive Campaigning." Canberra 2009.

Artner, Stephen J., Richard. Girven, and James B. Bruce. "Assessing the Value of Structured Analytic Techniques in the Us Intelligence Community." Rand Corporation, 2016.

Ashby, W. Ross. *An Introduction to Cybernetics.* 4 ed. London: Chapman & Hall Ltd, 1961.

Atwood, Chandler P. "Activity-Based Intelligence: Revolutionizing Military Intelligence Analysis." *Joint Force Quarterly : JFQ*, no. 77 (2015): 24-29.

Bak, Per, Chao Tang, and Kurt Wiesenfeld. "Self-Organized Criticality: An Explanation of the 1/F Noise." *Physical review letters* 59, no. 4 (1987): 381.

Bang, Martin. "Pitfalls in Military Quantitative Intelligence Analysis: Incident Reporting in a Low Intensity Conflict." *Intelligence & National Security* 31, no. 1 (2016): 49.

Bar-Joseph, Uri. "Intelligence Intervention in the Politics of Democratic States: The United States." *Israel, and Britain (University Park: Pennsylvania State Press, 1995)* (1995).

Bar-Joseph, Uri, and Rose McDermott. *Intelligence Success and Failure : The Human Factor.* Oxford University Press, 2017.

Bar-Yam, Yaneer. "Complexity of Military Conflict: Multiscale Complex Systems Analysis of Littoral Warfare." New England Complex Systems Institute, 2003.

———. *Making Things Work: Solving Complex Problems in a Complex World.* Cambridge, MA: Knowledge Press, 2004.

Bar-Yam, Yaneer. "Multiscale Variety in Complex Systems." *Complexity* 9, no. 4 (2004): 37-45.

Baranowski, Michał, Linas Kojala, Toms Rostoks, and Kalev Stoicescu. "What Next for Nato? Views from the North-East Flank on Alliance Adaptation." Tallinn: International Centre for Defence and Security, 2020.

Barbrook-Johnson, Pete, and Jayne Carrick. "Combining Complexity-Framed Research Methods for Social Research." *International Journal of Social Research Methodology* 25, no. 6 (2021): 835-48.

Barger, Deborah G. "Toward a Revolution in Intelligence Affairs." Santa Monica, CA: RAND Corporation, 2005.

Barrie, Douglas, Nick Childs, Yohann Michel, Ester Sabatino, and Ben Schreer. "Northern Europe, the Arctic and the Baltic: The ISR Gap." London: The International Institute for Strategic Studies, 2022.

Baudet, Floribert, Eleni Braat, J. T. W. H. van Woensel, and Aad Wever. "Military Intelligence: From Telling Truth to Power to Bewilderment?". In *Perspectives on Military Intelligence from the First World War to Mali : Between Learning and Law*, edited by Floribert Baudet, Eleni Braat, Jeoffrey van Woensel and Aad Wever, 1-22. The Hague: T.M.C. Asser Press, 2017.

Bay, Sebastian. "Intelligence Theories: A Literary Overview." *Lund, Sweden: Lund University* (2009).

Bean, Hamilton. "Intelligence Theory from the Margins: Questions Ignored and Debates Not Had." *Intelligence & National Security* 33, no. 4 (2018): 527-40.

———. "Privatizing Intelligence." In *Routledge Handbook of Private Security Studies*, 79-88: Routledge, 2015.

———. "Rhetorical and Critical/Cultural Intelligence Studies." *Intelligence and National Security* 28, no. 4 (2013): 495-519.

Bean, Hamilton, Peter de Werd, and Cristina Ivan. "Critical Intelligence Studies: Introduction to the Special Issue." *Intelligence and National Security* 36, no. 4 (2021/06/07 2021): 467-75.

Bean, Hamilton, and Mia Fischer. "Queering Intelligence Studies." *Intelligence and National Security* 36, no. 4 (2021/06/07 2021): 584-98.

Beebe, Sarah Miller, and George S. Beebe. "Understanding the Non-Linear Event: A Framework for Complex Systems Analysis." *International Journal of Intelligence and Counterintelligence* 25, no. 3 (2012): 508-28.

Belcher, Oliver. "Sensing, Territory, Population: Computation, Embodied Sensors, and Hamlet Control in the Vietnam War." *Security Dialogue* 50, no. 5 (2019).

Ben Jaffel, Hager, Alvina Hoffmann, Oliver Kearns, and Sebastian Larsson. "Collective Discussion: Toward Critical Approaches to Intelligence as a Social Phenomenon." *International Political Sociology* 14, no. 3 (2020): 323-44.

Bernstein, Steven, Richard Ned Lebow, Janice Gross Stein, and Steven Weber. "God Gave Physics the Easy Problems: Adapting Social Science to an Unpredictable World." *European Journal of International Relations* 6, no. 1 (2000): 43-76.

Betts, Richard K. "Two Faces of Intelligence Failure: September 11 and Iraq's Missing WMD." *Political Science Quarterly* 122, no. 4 (2008): 585-606.

Beyerchen, Alan D. "Clausewitz and the Non-Linear Nature of Warfare: Systems of Organized Complexity." In *Clausewitz in the Twenty-First Century* edited by Hew Strachan and Andreas Herberg-Rothe, 21-23. Oxford: Oxford University Press, 2007.

———. "Clausewitz, Nonlinearity, and the Unpredictability of War." *International Security* 17, no. 3 (1992): 59-90.

Bill, McKelvey, and Boisot Max. "Redefining Strategic Foresight: 'Fast' and 'Far' Sight Via Complexity Science." In *Handbook of Research on Strategy and Foresight*, 576-76: Edward Elgar Publishing, 2009.

Biltgen, Patrick, and Stephen Ryan. *Activity-Based Intelligence*. Norwood: Artech House, 2015.

Blake, Amy K. "From Intelligence Analysis to Medical Education: Using Structured Tools to Manage Bias." *Medical Education* 52, no. 3 (2018): 244-45.

Blignaut, Sonja. "Introduction." In *Cynefin: Weaving Sense-Making into the Fabric of Our World*, edited by R. Greenberg and B. Bertsch. Singapore: Cognitive Edge Pte Ltd, 2021.

Boelens, Minne. "The Revolution in Intelligence Affairs: Problem Solved?". Chap. 6 In *Perspectives on Military Intelligence from the First World War to Mali: Between*

Learning and Law, edited by Floribert Baudet, Eleni Braat, Jeoffrey van Woensel and Aad Wever, 119-43. The Hague, The Netherlands: T.M.C. Asser Press, 2017.

Boisot, Max, and Bill McKelvey. "Complexity and Organization-Environment Relations: Revisiting Ashby's Law of Requisite Variety." In *The Sage Handbook of Complexity and Management*, edited by Peter Allen, Steve Maguire and Bill McKelvey. Los Angeles, CA: SAGE, 2011.

Borch, Fred L. "Comparing Pearl Harbor and "9/11": Intelligence Failure? American Unpreparedness? Military Responsibility?". *The Journal of Military History* 67, no. 3 (2003): 845.

Bornio, Jakub. "20 Years of NATO's Flagship Multinational Corps Northeast: An Interview with Lieutenant General Sławomir Wojciechowski." *New Eastern Europe* 3, no. 41 (2020): 107-13.

Bosma, Esmé, Marieke de Goede, and Polly Pallister-Wilkins. "Introduction: Navigating Secrecy in Security Research." In *Secrecy and Methods in Security Research*, edited by Marieke De Goede, Esmé Bosma and Polly Pallister-Wilkins, 1-27: Routledge, 2020.

Bosman, Femke. "Uniformed Diversity: A Multifaceted Approach Towards the Diversity Climate in the Netherlands Defence Organisation.", University of Tilburg / Netherlands Defence Academy, 2008.

Bourdieu, Pierre. *Esquisse D'une Théorie De La Pratique, Précédé De Trois Études D'ethnologie Kabyle.* Genève: Librairie Droz, 1972.

———. *In Other Words: Essays Towards a Reflexive Sociology.* Cambridge: Polity, 1990.

———. *Outline of a Theory of Practice.* Cambridge: Cambridge University Press, 1977.

Bousquet, Antoine, and Simon Curtis. "Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations." *Cambridge Review of International Affairs* 24, no. 1 (2011): 43.

Bousquet, Antoine J. "Complexity Theory and the War on Terror: Understanding the Self-Organising Dynamics of Leaderless Jihad." [In Engels]. *Journal of international relations and development* (2012).

———. *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity.* London: Hurst & Company, 2009.

Bouwmeester, A. J. H. "Lo and Behold: Let the Truth Be Told -- Russian Deception Warfare in Crimea and Ukraine and the Return of 'Maskirovka' and 'Reflexive Control Theory'." In *Winning without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, edited by Paul A.L. Ducheine and Frans P.B. Osinga. The Hague: T.M.C. Asser Press, 2017.

Bozeman, Adda. "Political Intelligence in Non-Western Societies: Suggestions for Comparative Research." In *Comparing Foreign Intelligence: The Us, the Ussr, the Uk & the Third World*, edited by Roy Godson. Washington, DC: National Strategy Information Center, 1981.

Breakspear, Alan. "A New Definition of Intelligence." *Intelligence & National Security* 28, no. 5 (2013): 678.

Broekema, Wout. "When Does the Phoenix Rise? Factors and Mechanisms That Influence Crisis-Induced Learning by Public Organizations." Leiden, 2018.

Brown, Andrew D., Ian Colville, and Annie Pye. "Making Sense of Sensemaking in Organization Studies." *Organization studies* (2015).

Brown, Eddie J. "Conveying the Complex: Updating U.S. Joint Systems Analysis Doctrine with Complexity Theory." edited by School of Advanced Military Studies and United States Army Command and General Staff College. Fort Leavenworth, KS 2013.

Brown, Eddie J., and Tomas D. Pike. "Complex Intelligence Preparation of the Battlefield." In *International Studies Association Conference*. Baltimore, MD 2017.

Brown, Zachary T. "Intelligence Isn't Just for Commanders Anymore." *The Cipher Brief* (2022). https://www.thecipherbrief.com/intelligence-isnt-just-for-commanders-anymore.

Bruce, James B. "Dynamic Adaptation: A Twenty-First Century Intelligence Paradigm." 2004.

Brusset, Emery, Cedric De Coning, and Bryn Hughes. *Complexity Thinking for Peacebuilding Practice and Evaluation.* Springer, 2016.

Bryman, Alan. *Social Research Methods.* Fifth edition. ed. Oxford: Oxford University Press, 2016.

Buzan, Barry, and Lene Hansen. "Beyond the Evolution of International Security Studies?". *Security Dialogue* 41, no. 6 (2010): 659-67.

———. *The Evolution of International Security Studies.* Cambridge: Cambridge University Press, 2016.

Byrne, David, and Gillian Callaghan. *Complexity Theory and the Social Sciences: The State of the Art.* New York, NY: Routledge, 2014.

———. *Complexity Theory and the Social Sciences: The State of the Art.* New York: Routledge, 2013.

Caceres-Rodriguez, Rick, and Michael Landon-Murray. "Charting a Research Agenda for Intelligence Studies Using Public Administration and Organization Theory Scholarship." In *Researching National Security Intelligence: Multidisciplinary Approaches*, edited by Stephen Coulthart, Michael Landon-Murray and Damien Van Puyvelde. Washington, D.C.: Georgetown University Press, 2019.

Caddell, Joseph. "Discovering Soviet Missiles in Cuba: How Intelligence Collection Relates to Analysis and Policy." https://warontherocks.com/2017/10/discovering-soviet-missiles-in-cuba-intelligence-collection-and-its-relationship-with-analysis-and-policy/.

Capra, Fritjof. *The Web of Life : A New Synthesis of Mind and Matter.* London: Flamingo, 1997.

Capra, Fritjof, and Pier Luigi Luisi. *The Systems View of Life: A Unifying Vision.* Cambridge University Press, 2014.

Carter, Donald P. "Clouds or Clocks: The Limitations of Intelligence Preparation of the Battlefield in a Complex World." *Military Review* 96, no. 2 (2016): 36-41.

Casti, J. L. *Would-Be Worlds : How Simulation Is Changing the Frontiers of Science.* New York: J. Wiley, 1997.

Cetina, Karin Knorr. "Complex Global Microstructures: The New Terrorist Societies." *Theory, Culture & Society* 22, no. 5 (2005).

Chang, Welton, Elissabeth Berdini, David R. Mandel, and Philip E. Tetlock. "Restructuring Structured Analytic Techniques in Intelligence." *Intelligence and National Security* 33, no. 3 (2018): 337-56.

Chenoy, Anuradha M., and Rajan Kumar. *Re-Emerging Russia : Structures, Institutions and Processes.* Singapore: Palgrave Macmillan, 2017. doi:10.1007/978-981-10-5299-6.

Chesterman, S. "'We Can't Spy... If We Can't Buy!': The Privatization of Intelligence and the Limits of Outsourcing 'Inherently Governmental Functions'." *European Journal of International Law* 19, no. 5 (2008): 1055-74.

Chin, William Y. "Diversity in the Age of Terror: How Racial and Ethnic Diversity in the Us Intelligence Community Enhances National Security." *Fla. A & M UL Rev.* 6 (2010): 49.

Chiru, Irena, Cristina Ivan, and Ruben Arcos. "Diversity in Intelligence: Organizations, Processes, and People." *International Journal of Intelligence and CounterIntelligence* (2022): 1-14.

Cilliers, Paul. *Complexity and Postmodernism: Understanding Complex Systems.* London: Routledge, 1998.

Clark, Robert M. *Intelligence Analysis: A Target-Centric Approach.* 5 ed. Los Angeles, CA: Sage, 2016.

Clark, Timothy, and Robert Johnson, eds. *The World Information War: Western Resilience, Campaigning, and Cognitive Effects*. London: Routledge, 2021.

Clauset, Aaron. "Trends and Fluctuations in the Severity of Interstate Wars." *Science advances* 4, no. 2 (2018).

Clausewitz, Carl von. *On War.* Edited by Michael Howard and Peter Paret. New York, NY: Alfred A. Knopf (Random House), 1993.

Cobb, Adam. "Intelligence Adaptation." *The RUSI Journal* 156, no. 4 (2011): 54-62.

Committee on a Decadal Survey of Social and Behavioral Sciences for Applications to National Security. "A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis." Washington, D.C.: National Academies of Sciences, Engineering, Medicine, 2019.

Cooper, Jeffrey R. "Curing Analytic Pathologies." Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2005.

Copeland, Thomas E. *Fool Me Twice : Intelligence Failure and Mass Casualty Terrorism.* Leiden ;: Martinus Nijhoff, 2007. doi:10.1163/ej.9789004158450.i-292.

———. "Intelligence Failure Theory." In *Oxford Research Encyclopedia of International Studies*, 2010.

Coping with Complexity in the Euro-Atlantic Community and Beyond. Edited by Andris Sprūds and Diāna Potjomkina, Riga Conference: Latvian Institute of International Affairs, 2016.

Coulthart, Stephen. "What's the Problem? Frameworks and Methods from Policy Analysis for Analyzing Complex Problems." *Intelligence and National Security* 32, no. 5 (2017/07/29 2017): 636-48.

Coulthart, Stephen J. "An Evidence-Based Evaluation of 12 Core Structured Analytic Techniques." *The International Journal of Intelligence and Counter Intelligence* 30, no. 2 (2017): 368.

Coulthart, Stephen, Michael Landon-Murray, and Damien Van Puyvelde. "Introduction: A Pluralistic Approach to Intelligence Sholarship." In *Researching National Security Intelligence: Multidisciplinary Approaches*, edited by Stephen Coulthart, Michael Landon-Murray and Damien Van Puyvelde, 1-11. Washington, D.C.: Georgetown University Press, 2019.

———, eds. *Researching National Security Intelligence: Multidisciplinary Approaches*: Georgetown University Press, 2019.

Coulthart, Stephen, and Abebe Rorissa. "Growth, Diversification, and Disconnection: An Analysis of 70 Years of Intelligence Scholarship (1950-2020)." *Intelligence and National Security* (2023): 1-17.

Cradock, Percy. *Know Your Enemy : How the Joint Intelligence Committee Saw the World.* London: John Murray, 2002.

Cullen, Patrick. "Hybrid Threats as a New 'Wicked Problem' for Early Warning." Helsinki: Hybrid Center of Excellence, 2018.

Dahl, Erik J. *Intelligence and Surprise Attack : Failure and Success from Pearl Harbor to 9/11 and Beyond.* Washington, DC: Georgetown University Press, 2013.

Dalsjö, Robert, Michael Jonsson, and Johan Norberg. "A Brutal Examination: Russian Military Capability in Light of the Ukraine War." *Survival* 64, no. 3 (2022): 7-28.

Danchev, Alex. "The Reckoning: Official Inquiries and the Iraq War." *Intelligence & National Security* 19, no. 3 (2004): 436-66.

Danner, Lukas K. *China's Grand Strategy : Contradictory Foreign Policy?* Cham, Switzerland: Palgrave MacMillan, 2018.

Dao, T., J. Patterson, and P. Roberts. "Diversity and Inclusion: A Mission Imperative for the Intelligence Community." In *Intelligence after Next*: Mitre Centre for Technology and National Security, 2021.

Davies, Philip. "A Critical Look at Britain's Spy Machinery'." *Studies in Intelligence* 49, no. 4 (2005): 41-54.

Davies, Philip H. J. "Ideas of Intelligence." *Harvard International Review* 24, no. 3 (2002): 62-66.

Davies, Philip H. J., Kristian Gustafson, and Ian Rigden. "The Intelligence Cycle Is Dead, Long Live the Intelligence Cycle: Rethinking Intelligence Fundamentals for a New Intelligence Doctrine." In *Understanding the Intelligence Cycle*, edited by Mark Phythian, 56-76. Milton Park, Abingdon, Oxon: Routledge, 2013.

Davies, Philip HJ. "Theory and Intelligence Reconsidered." In *Intelligence Theory: Key Questions and Debate*, edited by Peter Gill, Stephen Marrin and Mark Phythian, 200-21. New York, NY: Routledge, 2009.

Davis, Jack. "The Kent-Kendall Debate of 1949." *Studies in Intelligence* 35, no. 2 (1992).

Day, Adam, and Charles T. Hunt. "A Perturbed Peace: Applying Complexity Theory to Un Peacekeeping." *International Peacekeeping* 30, no. 1 (2023): 1-23.

de Coning, Cedric, Rui Saraiva, and Ako Muto. *Adaptive Peacebuilding: A New Approach to Sustaining Peace in the 21st Century.* Springer Nature, 2023.

de Waard, Erik J, Sebastiaan Rietjens, A Georges L Romme, and Paul C van Fenema. "Learning in Complex Public Systems: The Case of Minusma's Intelligence Organization." *Public Management Review* (2021): 1-20.

de Werd, Peter. "Reflexive Intelligence and Converging Knowledge Regimes." *Intelligence and National Security* 36, no. 4 (2021): 512-26.

Der Derian, James. *Antidiplomacy: Spies, Terror, Speed, and War.* Cambridge, MA: Blackwell, 1992.

DeWeerd, Harvey A. "Strategic Surprise in the Korean War." Santa Monica, CA: Rand Corporation, 1962.

Dhami, Mandeep K., Ian K. Belton, and David R. Mandel. "The "Analysis of Competing Hypotheses" in Intelligence Analysis." *Applied Cognitive Psychology* 33, no. 6 (2019): 1080-90.

Donkersloot, E. H. F. "Hybrid Threats from the East ; the Gerasimov Doctrine and Intelligence Challenges for NATO." *Militaire spectator : tijdschrift voor het Nederlandsche leger* 186, no. 9 (2017). https://www.militairespectator.nl/sites/default/files/uitgaven/inhoudsopgave/Militaire%20Spectator%209-2017%20Donkersloot.pdf.

Dougherty, Christopher. "Strange Debacle: Misadventures in Assessing Russian Military Power." *War on the Rocks* 2022. https://warontherocks.com/2022/06/strange-debacle-misadventures-in-assessing-russian-military-power/

Dover, Robert, Huw Dylan, and Michael S Goodman. "Introduction to a Research Agenda for Intelligence Studies and Government." *A Research Agenda for Intelligence Studies and Government* (2022): 1-6.

Dunn Cavelty, Myriam, and Jennifer Giroux. "The Good, the Bad, and the Sometimes Ugly. Complexity as Both Threat and Oppertunity in National Security.". In *World Politics at the Edge of Chaos: Reflections on Complexity and Global Life*, edited by Emilian Kavalski. New York, NY: State University of New York Press, 2015.

Dunn Cavelty, Myriam, and Victor Mauer. "Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence." *Security Dialogue* 40, no. 2 (2009): 123-44.

Duvenage, Magdalena Adriana. "Intelligence: Lessons from Knowledge Management." In *International Studies Association*. San Francisco, 2013.

Eftimiades, Nicholas. "On the Question of Chinese Espionage." *Brown J. World Aff.* 26 (2019): 125.

Eikmeier, Dale C. "Simplicity: A Tool for Working with Complexity and Chaos." *Joint Force Quarterly : JFQ*, no. 92 (2019): 30-35.

Eisenhardt, Kathleen M. "Building Theories from Case Study Research." *Academy of management review* 14, no. 4 (1989): 532-50.

Engelen, Dick. "Mars Door De Tijd Van Een Institutie: Beknopte Geschiedenis Van De Aivd." In *Inlichtingen-En Veiligheidsdiensten*, edited by B.A. de Graaf, E.R. Muller and J.A. Reijn, 59-70. Alphen aan den Rijn: Kluwer, 2010.

Eriksson, Gunilla. *Swedish Military Intelligence : Producing Knowledge*. Edinburgh: Edinburgh University Press, 2016.

Evaluatiecommissie Wet op de inlichtingen- en veiligheidsdiensten 2002. "Evaluatie Wet Op De Inlichtingen-En Veiligheidsdiensten 2002: Naar Een Nieuwe Balans Tussen Bevoegdheden En Waarborgen." 2013.

Evans, Geraint. "Rethinking Military Intelligence Failure – Putting the Wheels Back on the Intelligence Cycle." *Defence Studies* 9, no. 1 (2009): 22-46.

Fägersten, Björn. "Forward Resilience in the Age of Hybrid Threats: The Role of European Intelligence." *Forward Resilience: Protecting Society in an Interconnected World* (2017): 113-26.

Ferguson, M.E., C. Harper, and R.D. Hooker. "NATO Joint Intelligence, Surveillance, and Reconnaissance in the Baltic Sea Region." The Scowcroft Center for Strategy and Security, 2019.

Ferris, John. "Netcentric Warfare, C4ISR and Information Operations: Towards a Revolution in Military Intelligence?". *Intelligence and National Security* 19, no. 2 (2004): 199-225.

"Field Manual 2.0 Intelligence." edited by Headquarters Department of the Army. Washington, DC 2023.

"Field Manual 3-24: Counterinsurgency." edited by Headquarters Department of the Army and Headquarters Department of the Navy. Washington, DC 2006.

Finney, Nathan, and "AR". "Human Terrain Team Handbook." Fort Leavenworth, KS.: Human Terrain System program, 2008.

Fishbein, Warren, and Gregory F. Treverton. "Making Sense of Transnational Threats." *Sherman Kent Center Occasional Papers* 3, no. 1 (2004).

Flynn, Michael T., Matt Pottinger, and Paul Batchelor. "Fixing Intel : A Blueprint for Making Intelligence Relevant in Afghanistan." Washington, DC: Center for a New American Security, 2010.

Folker, Robert D. *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods.* Washington, D.C: Joint Military Intelligence College, 2000.

Frank, Aaron. "Computational Social Science and Intelligence Analysis." *Intelligence & National Security* 32, no. 5 (2017): 579-99.

Freedman, Lawrence. "'Powerful Intelligence'." *Intelligence and National Security* 12, no. 2 (1997): 198.

Freeman, Richard. "Epistemological Bricolage: How Practitioners Make Sense of Learning." *Administration & society* 39, no. 4 (2007): 476-96.

Friedman, Thomas L. *The World Is Flat: The Globalized World in the Twenty-First Century.* New York, NY: Farrar, Straus and Giroux, 2005.

Fry, Michael G., and Miles Hochstein. "Epistemic Communities: Intelligence Studies and International Relations." *Intelligence and National Security* 8, no. 3 (1993): 14-28.

Galeotti, Mark. "The 'Gerasimov Doctrine'and Russian Non-Linear War." In *Moscow's Shadows*, 2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

———. "Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?". *Small Wars & Insurgencies* 27, no. 2 (2016): 282.

———. "I'm Sorry for Creating the 'Gerasimov Doctrine'." *Foreign Policy* 5 (2018): 2018.

———. "The Mythical 'Gerasimov Doctrine' and the Language of Threat." *Critical Studies on Security* 7, no. 2 (2019): 157-61.

Galster, Kjeld. *The Face of the Foe: Pitfalls and Perspectives of Military Intelligence.* Kingston, ON: Legacy Book Press, 2015.

Gans, Ben. "The Complexity of Peacekeeping Intelligence." *Journal of European and American Intelligence Studies* 1, no. 1 (2018): 35-60.

Gareis, Sven Bernhard, and Ulrich vom Hagen. "The Difficult Practice of Military Multinationaly: The Multinational Corps Northeast in Szczecin." In *The European Armed Forces in Transition : A Comparative Analysis*, edited by Franz Kernic, Paul Klein and Karl W. Haltiner, 157-76. New York: Peter Lang, 2005.

Gareis, Sven Bernhard, Ulrich Vom Hagen, Per Bach, Torben Andreasen, Ivan Doulgerof, Adam Kolodziejczyk, and Mariusz Wachowicz. "Conditions of Military Multinationality the Multinational Corps Northeast in Szczecin ; Report of the Trinational Research Team Strausberg, Copenhagen, Warsaw." [In Engels]. *Forum International* 24 (2003).

Gell-Mann, Murray. "Let's Call It Plectics.". *Complexity Journal* 1, no. 5 (1996): 3-6.

———. *The Quark and the Jaguar: Adventures in the Simple and the Complex.* New York, NY: Freeman and Company, 1994.

Gentry, John A. "Intelligence in War: How Important Is It? How Do We Know?". *Intelligence and National Security* 34, no. 6 (2019): 833-50.

———. "Intelligence Learning and Adaptation: Lessons from Counterinsurgency Wars." *Intelligence and National Security* 25, no. 1 (2010): 50-75.

Gentry, John A. "Demographic Diversity in U.S. Intelligence Personnel: Is It Functionally Useful?". *International Journal of Intelligence and CounterIntelligence* 36, no. 2 (2023/04/03 2023): 564-96.

George, Roger Z. "Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm." *Studies in Intelligence* 51, no. 3 (2007).

Georgiadou, Andri, Maria Alejandra Gonzalez-Perez, and Miguel R. Olivas-Luján. "Diversity within Diversity: Equality and Managing Diversity." In *Diversity within Diversity Management*. Advanced Series in Management, 1-16: Emerald Publishing Limited, 2019.

Gerasimov, Valery. "The Value of Science in Prediction." *Military-Industrial Courier* 476, no. 8 (2013).

Gill, P., and M. Phythian. "What Is Intelligence Studies?". *The International Journal of Intelligence, Security, and Public Affairs* 18, no. 1 (2016): 5-19.

Gill, Peter. "Intelligence, Threat, Risk and the Challenge of Oversight." *Intelligence & National Security* 27, no. 2 (2012): 206.

———. "Knowing the Self, Knowing the Other." In *Handbook of Intelligence Studies*, edited by Loch K. johnson, 82: Routledge, 2009.

———. "Theories of Intelligence." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson, 43-58. New York, NY: Oxford University Press, 2010.

———. "Theories of Intelligence Where Are We, Where Should We Go and How Might We Proceed?". In *Intelligence Theory: Key Questions and Debates*, edited by Peter Gill, Stephen Marrin and Mark Phythian, 208-26: Routledge, 2009.

Gill, Peter, Stephen Marrin, and Mark Phythian, eds. *Intelligence Theory: Key Questions and Debates*. London: Routledge, 2009.

Gill, Peter, and Mark Phythian. "From Intelligence Cycle to Web of Intelligence: Complexity and the Conceptualisation of Intelligence." In *Understanding the Intelligence Cycle*, 35-56: Routledge, 2013.

———. *Intelligence in an Insecure World.* 3 ed. Cambridge, UK Polity Press, 2018.

Gioia, Dennis A., Kevin G. Corley, and Aimee L. Hamilton. "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology." *Organizational research methods* 16, no. 1 (2013): 15-31.

Gioia, Dennis A., and Evelyn Pitre. "Multiparadigm Perspectives on Theory Building." *The Academy of Management Review* 15, no. 4 (1990): 584-602.

Glass, Robert Rigby, and Phillip B. Davidson. *Intelligence Is for Commanders.* Harrisburg, PA: Military Service Publishing Company, 1948.

Gleick, James. *Chaos : Making a New Science*. New York, N.Y.: Open Road Integrated Media, 2011.

Goldstein, Jeffrey. "Emergence as a Construct: History and Issues." *Emergence* 1, no. 1 (1999): 49-72.

Graaff, Bob de. *Data En Dreiging : Stap in De Wereld Van Intelligence.* Amsterdam: Boom, 2019.

———. "Intelligence and Intelligence Studies. Time for a Divorce?". *Romanian Intelligence Studies Review*, no. 21 (2019): 5-30.

Graaff, Bob de, James M. Nyce, and Chelsea Locke, eds. *Handbook of European Intelligence Cultures*. Lanham, MD: Rowman & Littlefield, 2016.

Graaff, Bob de, and Cees Wiebes. *Villa Maarheeze : De Geschiedenis Van De Inlichtingendienst Buitenland* [in Nederlands] Den Haag: Sdu Uitgevers, 1999.

Graham, Thomas, Jr., and Keith A. Hansen. *Spy Satellites : And Other Intelligence Technologies That Changed History.* Seattle: University of Washington Press, 2007.

Greenberg, R., and B. Bertsch, eds. *Cynefin: Weaving Sense-Making into the Fabric of Our World*. Singapore: Cognitive Edge Pte Ltd, 2021.

Gustafson, Kristian. "Complex Threats." *The RUSI Journal* 155, no. 1 (2010): 72-78.

Hackman, JR, SM Kosslyn, and AW Woolley. "The Design and Leadership of Intelligence Analysis Teams." *Unpublished Technical Report* 11 (2008).

Hammond, Thomas H. "Intelligence Organizations and the Organization of Intelligence." *The International Journal of Intelligence and Counter Intelligence* 23, no. 4 (2010): 680.

Hannas, William C., James C. Mulvenon, and Anna B. Puglisi. *Chinese Industrial Espionage : Technology Acquisition and Military Modernization.* London: Routledge, 2013.

Hansen, James H. "Soviet Deception in the Cuban Missile Crisis." *Studies in Intelligence* 46, no. 1 (2002).

Hansen, Morten. "Intelligence Contracting: On the Motivations, Interests, and Capabilities of Core Personnel Contractors in the Us Intelligence Community." *Intelligence & National Security* 29, no. 1 (2014): 58.

Herman, Michael. *Intelligence Power in Peace and War.* Cambridge: Cambridge University Press, 1996.

Heuer, Richards J., and Randolph H. Pherson. *Structured Analytic Techniques for Intelligence Analysis.* [in Engels] Second edition. ed. Washington, DC: CQ Press, 2015.

Heylighen, Francis, and Cliff Joslyn. "Cybernetics and Second-Order Cybernetics." In *Encyclopedia of physical science & technology*, edited by R.A. Meyers, 155-70. New York, NY: Academic Press, 2001.

Hillebrand, Claudia, and R. Gerald Hughes. "The Quest for a Theory of Intelligence." In *The Palgrave Handbook of Security, Risk and Intelligence*, edited by Robert Dover, Huw Dylan and Michael S. Goodman, 1-24. London: Palgrave Macmillan, 2017.

Hilsman, Roger. "Intelligence and Policy-Making in Foreign Affairs." *World Politics* 5, no. 1 (1952): 1-45.

Hindrén, Rasmus, and Hanna Smith. "Understanding and Countering Hybrid Threats through a Comprehensive and Multinational Approach." In *The Academic-Practitioner Divide in Intelligence Studies*, edited by Rubén Arcos, Nicole K. Drumhiller and M.ark Phythian. Lanham, MD: Rowman & Littlefield, 2022.

Hoffman, Frank G. "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges." *Prism* 7, no. 4 (2018): 30-47.

Hoffman, Frank G. *Conflict in the 21st Century : The Rise of Hybrid Wars.* [in Engels] Arlington, VA: Potomac Institute for Policy Studies, 2007.

Hogendoorn, Michelle, Bram Spoor, and Sebastiaan Rietjens. "Caught by Surprise: Warning for Russia's Invasion of Ukraine." In *Reflections on the Russia-Ukraine War*, edited by Maarten Rothman, Lonneke Peperkamp and Sebastiaan Rietjens, 41-56. Leiden: Leiden University Press, 2024.

Holland, John H. *Complexity : A Very Short Introduction.* First edition. ed. Oxford: Oxford University Press, 2014.

———. *Emergence: From Chaos to Order.* Oxford University Press, 2010.

———. *Hidden Order : How Adaptation Builds Complexity.* Helix Books. Reading, MA: Perseus, 1996.

Hoogstrate, André J. "The Effect of Big Data and Ai on Forecasting in Defence and Military Applications." In *Towards a Data-Driven Military. A Multidisciplinary Perspective.*, edited by Peter B.M.J. Pijpers, Mark Voskuijl and Robert M. Beeres. Netherlands Annual Review of Military Science, 145-61. Leiden: Leiden University Press, 2022.

Horlings, Tess. "Dealing with Data: Coming to Grips with the Information Age in Intelligence Studies Journals." *Intelligence and National Security* 38, no. 3 (2023): 447-69.

Horlings, Tess, Roy Lindelauf, and Sebastiaan Rietjens. "Battling Information Overload in Military Intelligence & Security Organisations." In *Towards a Data-Driven Military. A Multidisciplinary Perspective.*, edited by Peter B.M.J. Pijpers, Mark Voskuijl and Robert M. Beeres. Netherlands Annual Review of Military Science, 221-37. Leiden: Leiden University Press, 2022.

Huber, George P. "Organizational Learning: The Contributing Processes and the Literatures." *Organization Science* 2, no. 1 (1991): 88-115. doi:10.1287/orsc.2.1.88.

Hughes-Wilson, John. *On Intelligence.* [in Engels] London: Constable, 2017.

Hughes, Patrick M. "On Convergence, Emergence, and Complexity." *Military Review* 96, no. 2 (2016): 42-46.

Hughes, Thomas L. "The Fate of Facts in the World of Men." Paper presented at the Proceedings of the American Society of International Law at its annual meeting, 1969.

Hulnick, Arthur S. "The Intelligence Producer–Policy Consumer Linkage: A Theoretical Approach." *Intelligence and National Security* 1, no. 2 (1986): 212-33.

Hulnick, Arthur S. "Controlling Intelligence Estimates." In *Controlling Intelligence*, edited by Glenn Hastedt, 81-96. London: Frank Cass, 1991.

———. "The Future of the Intelligence Process: The End of the Intelligence Cycle." In *The Future of Intelligence: Challenges in the 21st Century*, edited by Isabelle Duyvesteyn, Ben de Jong and Joop van Reijn, 47. New York, NY: Routledge, 2014.

———. "Indications and Warning for Homeland Security: Seeking a New Paradigm." *International Journal of Intelligence and CounterIntelligence* 18, no. 4 (2005): 593-608.

———. "What's Wrong with the Intelligence Cycle." *Intelligence and National Security* 21, no. 6 (2006): 959-79.

Ikani, Nikki, Christoph O. Meyer, Eva Michaels, and Aviva Guttmann. "Expectations from Estimative Intelligence and Anticipatory Foreign Policy: A Realistic Appraisal." In *Estimative Intelligence in European Foreign Policymaking: Learning Lessons from*

an Era of Surprise, edited by Christoph O. Meyer, Eva Michaels, Nikki Ikani, Aviva Guttmann and Michael S. Goodman, 27-68. Edinburgh: Edinburgh University Press, 2022.

Ilachinski, Andrew. "Land Warfare and Complexity, Part Ii: An Assessment of the Applicability of Nonlinear Dynamics and Complex Systems Theory to the Study of Land Warfare." Alexandria, VA: Center for Naval Analyses 1996.

Irak, Commissie van Onderzoek Besluitvorming. "Rapport Commissie Van Onderzoek Besluitvorming Irak." Amsterdam: Boom, 2010.

James, Dorough-Lewis. "Investing in Uncertainty : Applying Social Science to Military Operations." In *Social Science Goes to War : The Human Terrain System in Iraq and Afghanistan*: Oxford University Press, 2015.

Javorsek, Daniel, and John G. Schwitz. "Probing Uncertainty, Complexity, and Human Agency in Intelligence." *Intelligence & National Security* 29, no. 5 (2014): 639.

Jeffreys-Jones, Rhodri. "The Rise and Fall of the Cia." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson. New York, NY: Oxford University Press, 2010.

Jehl, Douglas. "C.I.A. Nominee Wary of Budget Cuts." *New York Times*, 3 February 1993.

Jenkins, Richard. *Pierre Bourdieu.* London: Routledge, 1992.

Jervis, Robert. "Reports, Politics, and Intelligence Failures: The Case of Iraq." *Journal of Strategic Studies* 29, no. 1 (2006): 3-52.

———. *System Effects: Complexity in Political and Social Life.* Princeton, NJ: Princeton University Press, 1997.

———. *Why Intelligence Fails : Lessons from the Iranian Revolution and the Iraq War.* Ithaca, NY: Cornell University Press, 2010.

Johnson, Loch K, and James J Wirtz. *Intelligence: The Secret World of Spies: An Anthology.* 3 ed.: Oxford University Press, 2011.

Johnson, Loch K. "The Development of Intelligence Studies." In *Routledge Companion to Intelligence Studies*, 21-40: Routledge, 2013.

Johnson, Neil F. *Simply Complexity: A Clear Guide to Complexity Theory.* London: Oneworld Publications, 2012.

Johnston, Judith Meister, and Rob Johnston. "Testing the Intelligence Cycle through Systems Modeling and Simulation." In *Analytic Culture in the Us Intelligence Community: An Ethnographic Study* 45-56. Washington, DC: Center for the Study of Intelligence, CIA, 2005.

Jones, Morgan D. *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving.* Crown Business, 1998.

Kalyvas, Stathis N., and Matthew Adam Kocher. "The Dynamics of Violence in Vietnam: An Analysis of the Hamlet Evaluation System (Hes)." *Journal of Peace Research* 46, no. 3 (2009): 335.

Kamphuis, C. "Reflexive Control: The Relevance of a 50-Year-Old Russian Theory Regarding Perception Control." *Militaire Spectator* 187, no. 6 (2018): 324-39.

Kandrik, Matej. "Rethinking Russian Hybrid Warfare." *Perspectives*, no. 7 (2023).

Karlsen, Geir Hågen. "Tools of Russian Influence: Information and Propaganda." In *Ukraine and Beyond : Russia's Strategic Security Challenge to Europe*, edited by Janne Haaland Matlary and Tormod Heier, 181-208: Palgrave Macmillan, 2016.

Kavalski, Emilian, ed. *World Politics at the Edge of Chaos: Reflections on Complexity and Global Life*. New York, NY: State University of New York Press, 2015.

Keefe, Patrick R. "Privatized Spying: The Emerging Intelligence Industry." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. johnson. New York, NY: Oxford University Press, 2010.

Keegan, John. *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda.* Random House, 2004.

Kendall, Willmoore. "The Function of Intelligence." *World Politics* 1, no. 4 (1949): 542-52.

Kent, Sherman. "Prospects for the National Intelligence Service." *The Yale review* 36 (1946).

———. *Strategic Intelligence for American World Policy.* Princeton, N.J.: Princeton University Press, 1949.

Kerbel, Josh. "Lost for Words: The Intelligence Community's Struggle to Find Its Voice." *Parameters* 38, no. 2 (2008): 102-12.

———. "The Us Talks a Lot About Strategic Complexity. Too Bad It's Mostly Just Talk." https://www.defenseone.com/ideas/2021/03/us-talks-lot-about-strategic-complexity-too-bad-its-mostly-just-talk/172549/.

Kirwan, Cyril. *Making Sense of Organizational Learning : Putting Theory into Practice.* London: Routledge, 2016.

Klein, G., B. Moon, and R. R. Hoffman. "Making Sense of Sensemaking 1: Alternative Perspectives." *IEEE Intelligent Systems* 21, no. 4 (2006): 70-73.

Knorr, Klaus Eugen. "Foreign Intelligence and the Social Sciences." Center of International Studies, Princeton University, 1964.

Kramer, E. H., B. van Bezooijen, and R. Delahaij. "Sensemaking During Operations and Incidents." In *Managing Military Organizations : Theory and Practice*, edited by J. Soeters, Paul C. van Fenema and Robert Beeres. London: Routledge, 2010.

Kreienkamp, Julia, and Tom Pegram. "Governing Complexity: Design Principles for the Governance of Complex Global Catastrophic Risks." *International Studies Review* (2019).

Kreuter, Nate. "The Us Intelligence Community's Mathematical Ideology of Technical Communication." *Technical Communication Quarterly* 24, no. 3 (2015): 217-34.

Kriebel, David W. "Anthropological Theory and Intelligence." *Global Security and Intelligence Studies* 1, no. 1 (2015): 6.

Krieger, Wolfgang. "The German Bundesnachrichtendienst (Bnd): Evolution and Current Policy Issues." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. johnson. New York, NY: Oxford University Press, 2010.

Kritz, David. "Coming Together: Strengthening the Intelligence Community through Cognitive Diversity." *Global Security & Intelligence Studies* 7, no. 1 (2022): 25-48.

Kuhn, Thomas S. *The Structure of Scientific Revolutions.* Fourth edition. ed. Chicago: The University of Chicago Press, 2012.

Kuhns, Woodrow J. "Intelligence Failures: Forecasting and the Lessons of Epistemology." In *Paradoxes of Strategic Intelligence*, edited by Richard K. Betts and Thomas Mahnken, 90-109. London: Routledge, 2003.

Kurtz, Cynthia F, and David J. Snowden. "The New Dynamics of Strategy: Sense-Making in a Complex and Complicated World." *IBM systems journal* 42, no. 3 (2003): 462-83.

Kwa, Chong Guan. "Postmodern Intelligence: Strategic Warning and Crisis Management." Chap. 5 In *Perspectives on Military Intelligence from the First World War to Mali: Between Learning and Law*, edited by Floribert Baudet, Eleni Braat, Jeoffrey van Woensel and Aad Wever, 97-118. The Hague, The Netherlands: T.M.C. Asser Press, 2017.

Ladyman, James, and Karoline Wiesner. *What Is a Complex System?* New Haven, CT: Yale University Press, 2020.

Lahneman, William J. *Keeping U.S. Intelligence Effective: The Need for a Revolution in Intelligence Affairs.* Lanham, Md.: Scarecrow Press, 2011.

———. *National Intelligence Agencies and Transnational Threats: The Need for a New Intelligence Paradigm*. College Park, MD: Center for International & Security Studies, U. Maryland, 2008.

Lamanna, Lawrence J. "Documenting the Differences between American and British Intelligence Reports." *International Journal of Intelligence and CounterIntelligence* 20, no. 4 (2007): 602-28.

Lanoszka, Alexander, and Michael A. Hunzeker. "Evaluating the Enhanced Forward Presence after Five Years." *The RUSI Journal* (2023): 1-10.

Laqueur, Walter. *World of Secrets: The Uses and Limits of Intelligence.* London: Weidenfeld and Nicolson, 1985.

Lawrence, James L. "Activity-Based Intelligence: Coping with the" Unknown Unknowns" in Complex and Chaotic Environments." *American Intelligence Journal* 33, no. 1 (2016): 17-25.

Lawson, Sean T. *Nonlinear Science and Warfare: Chaos, Complexity and the U.S. Military in the Information Age.* Milton Park, Abingdon, Oxon: Routledge, 2014.

Lebovic, James H. "Perception and Politics in Intelligence Assessment: U.S. Estimates of the Soviet and “Rogue-State” Nuclear Threats." *International Studies Perspectives* 10, no. 4 (2009): 394-412.

Liaropoulos, Andrew. "A (R)Evolution in Intelligence Affairs? In Search of a New Paradigm." Athens: Research Institute for European and American Studies, 2006.

Libiseller, Chiara. "'Hybrid Warfare' as an Academic Fashion." *Journal of Strategic Studies* (2023): 1-23.

Lillbacka, Ralf. "An Outline of a Clausewitzian Theory of Intelligence." *International Journal of Intelligence and Counter Intelligence* 32, no. 3 (2019): 494.

Lillbacka, Ralf G. V. "Realism, Constructivism, and Intelligence Analysis." *International Journal of Intelligence and Counterintelligence* 26, no. 2 (2013): 304-31.

Lorenz, Edward. "Predictability: Does the Flap of a Butterfly's Wing in Brazil Set Off a Tornado in Texas?" Paper presented at the American Association for the Advancement of Science, Cambridge, MA, 1972.

Lowenthal, Mark M. *The Future of Intelligence.* Cambridge: Polity Press, 2018.

———. *Intelligence: From Secrets to Policy.* 5 ed. Washington, DC: CQ Press, 2012.

Luft, Joseph, and Harry Ingham. "The Johari Window, a Graphic Model of Interpersonal Awareness." *Proceedings of the western training laboratory in group development* 246 (1955): 2014-03.

Luttwak, Edward. *The Rise of China Vs. The Logic of Strategy.* Cambridge, MA: Belknap Press of Harvard University Press, 2012. doi:10.4159/harvard.9780674067936.

Lyotard, Jean François. *The Postmodern Condition : A Report on Knowledge.* Manchester: Manchester University Press, 1986.

Manjikian, Mary. "Positivism, Post-Positivism, and Intelligence Analysis." *International Journal of Intelligence and Counterintelligence* 26, no. 3 (2013): 563-82.

Mann, Steven R. "Chaos Theory and Strategic Thought." *Parameters* 22 (1992): 54-68.

Marrin. "Analytic Objectivity and Science: Evaluating the Us Intelligence Community's Approach to Applied Epistemology." *Intelligence and National Security* 35, no. 3 (2020): 350-66.

Marrin, Stephen. "Evaluating Intelligence Theories: Current State of Play." *Intelligence and National Security* 33, no. 4 (2018): 479-90.

———. *Improving Intelligence Analysis : Bridging the Gap between Scholarship and Practice.* Milton Park, Abingdon, Oxon: Routledge, 2012.

———. "Improving Intelligence Studies as an Academic Discipline." *Intelligence and National Security* 31, no. 2 (2016): 266-79.

———. "Intelligence Analysis and Decision-Making: Methodological Challenges." In *Intelligence Theory: Key Questions and Debates*, edited by Peter Gill, Stephen Marrin and Mark Phythian, 145-64: Routledge, 2009.

———. "Intelligence Analysis Theory: Explaining and Predicting Analytic Responsibilities." *Intelligence and National Security* 22, no. 6 (2007): 821-46.

———. "Is Intelligence Analysis an Art or a Science?". *International Journal of Intelligence and CounterIntelligence* 25, no. 3 (2012): 529-45.

———. "Modeling Intelligence Analysis on the Social Sciences." In *Handbook of Intelligence Studies*, edited by loch K. Johnson: Routledge, 2009.

———. "Understanding and Improving Intelligence Analysis by Learning from Other Disciplines." *Intelligence and National Security* 32, no. 5 (2017/07/29 2017): 539-47.

Marrin, Stephen, and Jonathan D. Clemente. "Modeling an Intelligence Analysis Profession on Medicine." *International Journal of Intelligence and CounterIntelligence* 19, no. 4 (2006/12/01 2006): 642-65.

Marrin, Stephen, and Efren Torres. "Improving How to Think in Intelligence Analysis and Medicine." *Intelligence and National Security* 32, no. 5 (2017/07/29 2017): 649-62.

Marsick, V.J., and K.E. Watkins. "Learning Organization." In *International Encyclopedia of Adult Education*, edited by L.M. English, 355–60. London: Palgrave, 2005.

Martelloni, Gianluca, Francesca Di Patti, and Ugo Bardi. "Pattern Analysis of World Conflicts over the Past 600 Years." (2018).

Mattis, Peter. "A Guide to Chinese Intelligence Operations." War on the Rocks, https://warontherocks.com/2015/08/a-guide-to-chinese-intelligence-operations/.

Mattis, Peter, and Matthew Brazil. *Chinese Communist Espionage: An Intelligence Primer.* Naval Institute Press, 2019.

Maturana, Humberto R, and Francisco J Varela. *Autopoiesis and Cognition: The Realization of the Living.* Springer Science & Business Media, 1991.

Medar, Sergiu. "Intelligence in Hybrid Warfare." In *Countering Hybrid Threats: Lessons Learned from Ukraine*, edited by Niculae Iancu, Andrei Fortuna, Cristian Barna and Mihaela Teodor. NATO Science for Peace and Security Series. Amsterdam: IOS Press, 2016.

Mendosa, Julie. "Expanding Mental Models in Intelligence through Diverse Perspectives." *International Journal of Intelligence and CounterIntelligence* 35, no. 4 (2022/10/02 2022): 621-36.

Menkveld, Christiaan. "Understanding the Complexity of Intelligence Problems." *Intelligence and National Security* 36, no. 5 (2021): 621-41.

Mercier, Denis. "NATO's Adaptation in an Age of Complexity." *PRISM* 7, no. 4 (2018): 2-11.

Mesjasz, Czeslaw. "Complex Systems Studies and Terrorism." *Conflict and complexity: Countering terrorism, insurgency, ethnic and regional violence* (2015): 35-71.

Meyer, Christoph O., and Nikki Ikani. "The Case of the Ukraine-Russia Undeclared War 2013/2014: Lessons for the Eu's Estimative Intelligence." In *Estimative Intelligence in European Foreign Policymaking: Learning Lessons from an Era of Surprise*, edited by Christoph O. Meyer, Eva Michaels, Nikki Ikani, Aviva Guttmann and Michael S. Goodman, 129-59. Edinburgh: Edinburgh University Press, 2022.

Michael, Kobi, and Aaron Kornbluth. "The Academization of Intelligence: A Comparative Overview of Intelligence Studies in the West." *Cyber, Intelligence, and Security* 3 (2019).

Miller, John H., and Scott E. Page. *Complex Adaptive Systems : An Introduction to Computational Models of Social Life.* Princeton, N.J.: Princeton University Press, 2007.

Miller, Steven E. "The Hegemonic Illusion? Traditional Strategic Studies in Context." *Security Dialogue* 41, no. 6 (2010): 639-48.

Mitchell, Melanie. *Complexity: A Guided Tour.* New York, NY: Oxford University Press, 2009.

Mitelman, Lawrence T. "Preface to a Theory of Intelligence." *Studies in Intelligence* 18, no. 3 (1974): 19-22.

Mitleton-Kelly, E. V. E. "A Complexity Approach to Co-Creating an Innovative Environment." *World Futures: The Journal of General Evolution* 62, no. 3 (2006): 223-39.

MIT Technology Review. "Data Mining Adds Evidence That War Is Baked into the Structure of Society."
https://www.technologyreview.com/2019/01/04/137950/data-mining-adds-evidence-that-war-is-baked-into-the-structure-of-society/.

Moffat, James. *Complexity Theory and Network Centric Warfare.* Washington, DC: CCRP Publication Series, 2003.

Moore, D. T., E. Moore, S. Cantey, and R. R. Hoffman. "Sensemaking for 21st Century Intelligence." *Journal of Intelligence History* (2020).

Moore, David T, and Robert R Hoffman. "Data-Frame Theory of Sensemaking as a Best Model for Intelligence." *American Intelligence Journal* 29, no. 2 (2011): 145-58.

Moore, David T. *Sensemaking : A Structure for an Intelligence Revolution.* Washington, DC: National Defense Intelligence College Press, 2011.

Morris, Victor R. "Complex Intelligence Preparation of the Battlefield in Ukrainian Antiterrorism Operations." *Military Review* 97, no. 1 (2017): 58-65.

Mountcastle, Clay. "The Myth of the New Complexity." *Military Review* 96, no. 2 (2016): 47-53.

Mumford, Andrew, and Pascal Carlucci. "Hybrid Warfare: The Continuation of Ambiguity by Other Means." *European Journal of International Security* 8, no. 2 (2023): 192-206.

Nag, Rajiv, and Dennis A. Gioia. "From Common to Uncommon Knowledge: Foundations of Firm-Specific Use of Knowledge as a Resource." *The Academy of Management Journal* 55, no. 2 (2012): 421-57.

National commission on terrorist attacks upon the United States. "The 9/11 Commission Report." 2004.

Newbery, Samantha, and Christian Kaunert. "Critical Intelligence Studies: A New Framework for Analysis." *Intelligence and National Security* (2023): 1-19.

Nicander, Lars D. "Understanding Intelligence Community Innovation in the Post-9/11 World." *International Journal of Intelligence and Counter Intelligence* 24, no. 3 (2011): 534-68.

Nolan, Bridget Rose. "From the “Lavender Scare” to “out and Equal”: Lgbtqia+ Diversity in the U.S. Intelligence Community." *International Journal of Intelligence and CounterIntelligence* 35, no. 4 (2022/10/02 2022): 713-25.

Nye, Joseph S. "Peering into the Future." *Foreign Affairs* 73, no. 4 (1994): 82.

Olcott, Anthony. "Revisiting the Legacy: Sherman Kent, Willmoore Kendall, and George Pettee–Strategic Intelligence in the Digital Age." *Studies in intelligence* 53, no. 2 (2009): 21-32.

Omand, David. "The Cycle of Intelligence." In *Routledge Companion to Intelligence Studies*, edited by Robert Dover, Michael S. Goodman and Claudia Hillebrand, 59-71. Abingdon, Oxfordshire: Routledge, 2015.

———. "The Future of Intelligence: What Are the Threats, the Challenges and the Opportunities?". In *The Future of Intelligence*, edited by Isabelle Duyvesteyn, Ben De Jong and Joop Van Reijn, 14-26. London: Routledge, 2014.

———. "Is It Time to Move Beyond the Intelligence Cycle? A Uk Practitioner Perspective." In *Understanding the Intelligence Cycle*, edited by Mark Phythian, 134-49. Milton Park, Abingdon, Oxon: Routledge, 2013.

———. *Securing the State.* London: C. Hurst & Co, 2010.

Osinga, Frans P. B. "Organizing for Insecurity and Chaos: Resilience and Modern Military Theory." In *Netherlands Annual Review of Military Studies 2016 : Organizing for Safety and Security in Military Organizations*, edited by Robert Beeres, Gwendolyn Bakx, Erik de Waard and Sebastiaan Rietjens, 43-73. The Hague: T.M.C. Asser Press, 2016.

———. *Science, Strategy and War: The Strategic Theory of John Boyd.* Routledge, 2007.

Otte, Paul. *Grayisms. And Other Thoughts on Leadership from General Al Gray, Usmc (Retired) 29th Commandant of the Marine Corps.* Arlington, VA: Potomac Institute Press, 2015.

Paananen, Soili, Alisa Puustinen, Harri Raisio, and Harri Jalonen. "Embracing Dynamic Tensions: Peacekeeping as a Balancing Act of Complexity." *Public Administration Review* 82, no. 6 (2022): 1168-78.

Page, S. *The Diversity Bonus.* Princeton: Princeton University Press, 2017.

Page, Scott E. *Diversity and Complexity.* Princeton, NJ: Princeton University Press, 2011.

Patrick, Rus. "Exploring Unknown Unknowns in Intelligence Analysis." *Romanian Intelligence Studies Review*, no. 19-20 (2018): 5-14.

Pellerin, Cheryl. "Project Maven to Deploy Computer Algorithms to War Zone by Year's End." US Department of Defense, https://www.defense.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/.

Perrow, Charles. *Normal Accidents : Living with High-Risk Technologies.* [in Engels] Princeton Paperbacks. Princeton, N.J.: Princeton University Press, 1999.

Pfützenreuter, Ulrich. "20 Years of Multinational Corps Northeast – from Political Symbol to Regional Responsibility." *Baltic Amber magazine* 2020.

Phythian, Mark. "Framing the Challenges and Oppertunities of Intelligence Studies Research." In *Researching National Security Intelligence: Multidisciplinary Approaches*, edited by Stephen Coulthart, Michael Landon-Murray and Damien Van Puyvelde, 11-29. Washington, D.C.: Georgetown University Press, 2019.

———. "Intelligence Theory and Theories of International Relations Shared World or Separate Worlds?". In *Intelligence Theory : Key Questions and Debates*, edited by Peter Gill, Stephen Marrin and Mark Phythian, 54-72: Routledge, 2009.

———. "The Perfect Intelligence Failure? U.S. Pre-War Intelligence on Iraqi Weapons of Mass Destruction." *Politics & Policy* 34, no. 2 (2006): 400-24.

———, ed. *Understanding the Intelligence Cycle*. Edited by Mark Phythian, Studies in Intelligence. Milton Park, Abingdon, Oxon: Routledge, 2013.

Pike, Thomas D., and Eddie J. Brown. "Complex Ipb." Small Wars Journal, https://smallwarsjournal.com/jrnl/art/complex-ipb (accessed 16-3-2019).

Pillar, Paul R. "Adapting Intelligence to Changing Issues." *Handbook of intelligence studies* (2007): 148.

Platt, Washington. *Strategic Intelligence Production: Basic Principles.* Praeger, 1957.

Prigogine, Ilya, and Isabelle Stengers. *Order out of Chaos: Man's New Dialogue with Nature.* London: Flamingo, 1985.

"Quick Wins for Busy Analysts." edited by Defence Intelligence. London: United Kingdom Ministry of Defence, 2013.

Quiggin, Thomas. *Seeing the Invisible: National Security Intelligence in an Uncertain Age.* World Scientific, 2007.

Raisio, Harri, Alisa Puustinen, and Jaakko Jäntti. ""“The Security Environment Has Always Been Complex!”: The Views of Finnish Military Officers on Complexity." *Defence Studies* 20, no. 4 (2020): 390-411.

Rathmell, Andrew. "Towards Postmodern Intelligence." *Intelligence and National Security* 17, no. 3 (2002): 87-104.

Renz, Bettina. "Russia and ‘Hybrid Warfare’." *Contemporary Politics* 22, no. 3 (2016/07/02 2016): 283-300.

Reuters. "Finland, Norway Bridle at Migrant Flows from Russia." 2016.

Richards, Julian. *The Art and Science of Intelligence Analysis.* [in Engels] Oxford ;: Oxford University Press, 2010.

———. "Intelligence Studies, Academia and Professionalization." *The International Journal of Intelligence, Security, and Public Affairs* 18, no. 1 (2016/01/02 2016): 20-33.

———. "Pedalling Hard: Further Questions About the Intelligence Cycle in the Contemporary Era." In *Understanding the Intelligence Cycle*, edited by Mark Phythian, 57-69. Milton Park, Abingdon, Oxon: Routledge, 2013.

Richardson, Kurt, and Paul Cilliers. "What Is Complexity Science? A View from Different Directions." (2001).

Riedel, Bruce O. *Jfk's Forgotten Crisis : Tibet, the Cia, and Sino-Indian War.* Washington, D.C.: Brookings Institution Press, 2015.

Rietjens, Sebastiaan. "The Future of NLD DISS: A Complex Perspective." *Militaire Spectator* 191, no. 9 (2022): 12-23.

———. "Intelligence in Defence Organizations: A Tour De Force." *Intelligence and National Security* 35, no. 5 (2020): 717-33.

———. *A Warning System for Hybrid Threats-Is It Possible?* : European centre of excellence for countering hybrid threats, 2020.

Rietjens, Sebastiaan, and Peter De Werd. "Intelligence and the Military: Introduction." 1-6: Taylor & Francis, 2023.

Rittel, Horst W. J., and Melvin M. Webber. "Dilemmas in a General Theory of Planning." *Policy Sciences* 4, no. 2 (1973).

Rodriguez, Ismael R. . "Uncertain About Uncertainty: Improving the Understanding of Uncertainty in Mi Doctrine." *Military Intelligence Professional Bulletin* 37, no. 2 (2011).

Rogg, Jeff. "Military–Intelligence Relations: Explaining the Oxymoron." *International Journal of Intelligence and CounterIntelligence* (2023): 1-18.

Romme, A Georges L, and Arjen Van Witteloostuijn. "Circular Organizing and Triple Loop Learning." *Journal of organizational change management* 12, no. 5 (1999): 439-54.

Rønn, Kira Vrist, and Simon Høffding. "The Epistemic Status of Intelligence: An Epistemological Contribution to the Understanding of Intelligence." *Intelligence & National Security* 28, no. 5 (2013): 694.

Rothman, Maarten. "On the Instrumentality of Soft Power; or Putin against Democracy Promotion." [In Engels]. *Winning without killing: the strategic and operational utility of non-kinetic capabilities in crises* (2017).

Rothman, Maarten, and Th B. F. M. Brinkel. "Of Snoops and Pirates : Competing Discourses of Cyber Security." *Cyber warfare: critical perspectives* (2012).

Rovner, Joshua, and Austin Long. "The Perils of Shallow Theory: Intelligence Reform and the 9/11 Commission." *International Journal of Intelligence and Counterintelligence* 18, no. 4 (2005): 609-37.

Ruffa, Chiara, and Joseph Soeters. "Cross-National Research in the Military: Comparing Operational Styles." In *Routledge Handbook of Research Methods in Military Studies*, edited by Joseph Soeters, Patricia M Shields and Sebastiaan Rietjens, 236-47: Routledge, 2014.

Rumsfeld, Donald. *Known and Unknown : A Memoir.* New York: Sentinel, 2011.

Sæther, Tobias. "War of Broken Fraternity: Competing Explanations for the Outbreak of War in Ukraine in 2014." *The Journal of Slavic Military Studies* 36, no. 1 (2023/01/02 2023): 28-56.

Sageman, Marc. *Leaderless Jihad: Terror Networks in the Twenty-First Century.* Philadelphia, PA: University of Pennsylvania Press, 2008.

Sari, Aurel. "Instrumentalized Migration and the Belarus Crisis: Strategies of Legal Coercion." In *Hybrid CoE Paper 7*: The European Centre of Excellence for Countering Hybrid Threats, 2023.

Scheffler, Alessandro, and Jan-Hendrik Dietrich. "Military Intelligence: Ill-Defined and Understudied." *International Journal of Intelligence and CounterIntelligence* (2023): 1-20.

Schlesinger, James R. "A Review of the Intelligence Community." edited by Office of Management and Budget, 1971.

Scott, Len. "British Strategic Intelligence and the Cold War." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. johnson. New York, NY: Oxford University Press, 2010.

Scott, Len, and Peter Jackson. "The Study of Intelligence in Theory and Practice." *Intelligence & National Security* 19, no. 2 (2004): 139-69.

Seymen, Oya Aytemiz. "The Cultural Diversity Phenomenon in Organisations and Different Approaches for Effective Cultural Diversity Management: A Literary Review." *Cross Cultural Management: An International Journal* 13, no. 4 (2006): 296-315.

Shahan, Jess. "“Don’t Keep Mum”: Critical Approaches to the Narratives of Women Intelligence Professionals." *Intelligence and National Security* 36, no. 4 (2021/06/07 2021): 569-83.

Shakoor, Daniel Tallat Rønn. "The Intelligence Cycle in Denmark: Unwinding and Reconceptualising the Process of Formulating Intelligence Requirements Surrounding the Middle East in the Danish Defence Intelligence Service." University of Southern Denmark, 2021.

Shapira, Itai. "Strategic Intelligence as an Art and a Science: Creating and Using Conceptual Frameworks." *Intelligence and National Security* 35, no. 2 (2020): 283-99.

Shea, Jamie. "NATO in the Era of Global Complexity." *New Perspectives on Shared Security: NATO’s Next 70 Years* (2019): 19-23.

Sierzputowska, Kamila. "NATO Institutions in the Territory of Poland." Paper presented at the Security Forum, Banská Bystrica, Slovakia, 2018.

Sims, Jennifer. "The Theory and Philosophy of Intelligence." In *Routledge Companion to Intelligence Studies*, edited by Robert Dover, Michael S. Goodman and Claudia Hillebrand, 42-50: Routledge, 2015.

Singer, J. David. "Threat-Perception and the Armament-Tension Dilemma." *The Journal of Conflict Resolution (pre-1986)* 2, no. 1 (1958): 90.

Sjøgren, Søren, Jakob Clod Asmund, Maya Mynster Christensen, Karina Mayland, and Thomas Randrup Pedersen. "Military Security and Research Ethics: Using Principles

of Research Ethics to Navigate Military Security Dilemmas." *Scandinavian Journal of Military Studies* 7, no. 1 (2024): 34-47.

Smith, Rupert. *The Utility of Force: The Art of War in the Modern World.* New York, NY: Vintage, 2008.

Snetselaar, David. "Dreams Lab: Assembling Knowledge Security in Sino-Dutch Research Collaborations." *European Security* 32, no. 2 (2023): 233-51.

Snowden, David. "Complex Acts of Knowing: Paradox and Descriptive Self-Awareness." *The journal of knowledge management* 6, no. 2 (2002): 100-11.

———. "Cynefin: A Tale That Grew in the Telling." In *Cynefin: Weaving Sense-Making into the Fabric of Our World*, edited by R. Greenberg and B. Bertsch, 31-58. Singapore: Cognitive Edge Pte Ltd, 2021.

———. "What Cynefin Is in Brief." In *Cynefin: Weaving Sense-Making into the Fabric of Our World*, edited by R. Greenberg and B. Bertsch, 58-62. Singapore: Cognitive Edge Pte Ltd, 2021.

Snowden, Dave, and Alessandro Rancati. "Managing Complexity (and Chaos) in Times of Crisis." Luxembourg: Publications Office of the European Union, 2021.

Snowden, David J, and Mary E Boone. "A Leader's Framework for Decision Making." *Harvard business review* 85, no. 11 (2007): 68.

Soeters, Joseph. "Organizational Cultures in the Military." In *Handbook of the Sociology of the Military*, edited by Giuseppe Caforio and M. Nuciari, 251-72. Cham, Switzerland: Springer, 2018.

Solvit, Samuel. *Dimensions of War: Understanding War as a Complex Adaptive System.* Paris: L'Harmattan, 2012.

Sopelana, Amaia, Martin Kunc, and Olga Rivera Hernáez. "Organizational Flexibility: A Dynamic Evaluation of Volberda's Theory." Paper presented at the 28th International Conference of the System Dynamics Society, 2010.

Spoor, Bram. "Intelligence Adaptation; Insights from Complexity Science and the Need for Analytic Cognitive Diversity." In "Innovations in International Affairs" book series volume, edited by Effie Charalampaki, Czesław Mesjasz, and Luis Tomé (Routledge 2025), forthcoming.

Spoor, Bram, and Peter de Werd. "Complexity in Military Intelligence." *International Journal of Intelligence and CounterIntelligence* 36, no. 4 (2023): 1122-42.

Spoor, Bram, and Maarten Rothman. "On the Critical Utility of Complexity Theory in Intelligence Studies." *Intelligence & National Security* 36, no. 4 (2021): 555-68.

Standish, Reid. "For Finland and Norway, the Refugee Crisis Heats up Along the Russian Arctic." *Foreign Policy* 26 (2016): 2016.

Stoker, Donald, and Craig Whiteside. "Blurred Lines: Gray-Zone Conflict and Hybrid War-Two Failures of American Strategic Thinking." *Naval War College Review* 73, no. 1 (2020): 12-48.

Sulick, Michael J. "Intelligence in the Cold War." In *Guide to the Study of Intelligence*, edited by Peter C. Olseson, 127-37. Falls Church, VA: Association of Former Intelligence Officers, 2016.

Szymański, Piotr, Piotr Żochowski, and Witold Rodkiewicz. "Enforced Cooperation: The Finnish-Russian Migration Crisis." In *OSW Analyses*: Centre for Eastern Studies, 2016.

Ter Meulen, Fleur. "Diversiteit in Inlichtingenorganisaties." Netherlands Defence Academy, 2022.

Thomas, Timothy. "Russia's Reflexive Control Theory and the Military." *Journal of Slavic Military Studies* 17, no. 2 (2004): 237-56.

"A Tradecraft Primer : Structured Analytic Techniques for Improving Intelligence Analysis." edited by Center for the Study of Intelligence. Washington, D.C.: Central Intelligence Agency, 2009.

Treverton, Gregory F, Andrew Thvedt, Alicia R Chen, Kathy Lee, and Madeline McCue. "Addressing Hybrid Threats." 1-92: Swedish Defence University, 2018.

Treverton, Gregory F. "Addressing “Complexities” in Homeland Security." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson, 343-58. New York, NY: Oxford University Press, 2010.

———. "Creatively Disrupting the Intelligence Paradigm." *ISN Security Watch* (2014).

———. "The Intelligence Challenges of Hybrid Threats: Focus on Cyber and Virtual Realm." Swedish Defence University, 2018.

———. *Intelligence for an Age of Terror.* Cambridge: Cambridge University Press, 2009.

———. *Reshaping National Intelligence for an Age of Information.* New York City, NY: Cambridge University Press, 2003.

Treverton, Gregory F., Seth G. Jones, Steven Boraz, and Philip Lipscy. "Toward a Theory of Intelligence : Workshop Report." 2006.

Troy, Thomas F. "The "Correct" Definition of Intelligence." *International Journal of Intelligence and CounterIntelligence* 5, no. 4 (1991): 433-54.

Tucker, Patrick. "Spies Like Ai: The Future of Artificial Intelligence for the Us Intelligence Community." Defense One, https://www.defenseone.com/technology/2020/01/spies-ai-future-artificial-intelligence-us-intelligence-community/162673/?oref=d1-related-article.

Urry, John. "The Global Complexities of September 11th." *Theory, Culture and Society* 19, no. 4 (2002): 57-69.

U.S. Army Training and Doctrine Command. "The U.S. Army Operating Concept: Win in a Complex World.", 525-3. Fort Eustis, VA: United States Army Headquarters, 2014.

Valk, Giliam de. "Case Studies into the Unknown - Logic & Tooling." *Romanian Intelligence Studies Review*, no. 21 (2019): 243-68.

Valk, Giliam de, and Onno Goldbach. "Towards a Robust B Research Design: On Reasoning and Different Classes of Unknowns." *Journal of Intelligence History* 20, no. 1 (2021): 72-87.

Van Puyvelde, Damien. *Outsourcing Us Intelligence : Contractors and Government Accountability*. Edinburgh: Edinburgh University Press, 2019.

———. "The Why, Who and How of Using Qualitative Interviews to Research Intelligence Practices." In *Researching National Security Intelligence: Multidisciplinary Approaches*, edited by Stephen Coulthart, Michael Landon-Murray and Damien Van Puyvelde, 47-63. Washington, D.C.: Georgetown University Press, 2019.

———. "Women and Black Employees at the Central Intelligence Agency: From Fair Employment to Diversity Management." *Cambridge Review of International Affairs* 34, no. 5 (2021): 673-703.

Varzhanskyi, Illia. "Reflexive Control as a Risk Factor for Using Osint: Insights from the Russia–Ukraine Conflict." *International Journal of Intelligence and CounterIntelligence* (2023): 1-31.

Voelz, Glenn J. "Contractors and Intelligence: The Private Sector in the Intelligence Community." *International Journal of Intelligence and CounterIntelligence* 22, no. 4 (2009): 586-613.

Vogel, Kathleen M. "The Impact of Technology on Intelligence Analysis." In *A Research Agenda for Intelligence Studies and Government*, edited by Robert Dover, Huw Dylan and Michael S Goodman, 113-27. Cheltenham: Edward Elgar, 2022.

Volberda, Henk W. "Toward the Flexible Form: How to Remain Vital in Hypercompetitive Environments." *Organization science* 7, no. 4 (1996): 359-74.

Volberda, Henk W. *The Flexible Firm. How to Remain Competitive.* Oxford: Oxford University Press, 1998.

Vorm, van der Martijn. "War's Didactics a Theoretical Exploration on How Militaries Learn from Conflict." Breda: Faculty of Military Sciences; Netherlands Defence Academy, 2021.

Walby, Sylvia. "Complexity Theory, Systems Theory, and Multiple Intersecting Social Inequalities." *Philosophy of the Social Sciences* 37, no. 4 (2007): 449.

Waldrop, Mitchell M. *Complexity: The Emerging Science at the Edge of Order and Chaos.* New York, NY: Simon and Schuster, 1992.

Waltz, Edward. *Quantitative Intelligence Analysis: Applied Analytic Models, Simulations, and Games.* London: Rowman & Littlefield, 2014.

Warner, Michael. "Intelligence and Reflexivity: An Invitation to a Dialogue." *Intelligence & National Security* 27, no. 2 (2012).

———. *The Rise and Fall of Intelligence: An International Security History.* Washington: Georgetown University Press, 2014.

———. "The Rise of the Us Intelligence System, 1917–1977." In *The Oxford Handbook of National Security Intelligence*, edited by Loch K. Johnson. New York, NY: Oxford University Press, 2010.

———. "Theories of Intelligence: The State of Play." In *Routledge Companion to Intelligence Studies*, edited by Robert Dover, Michael S. Goodman and Claudia Hillebrand, 25-33: Routledge, 2015.

———. "Wanted: A Definition of Intelligence." *Studies in Intelligence* 46, no. 3 (2002): 15-22.

Weaver, Warren. "Science and Complexity." *American Scientist* 36, no. 4 (1948): 536-44.

Webb, Jen, Tony Schirato, and Geoff Danaher. *Understanding Bourdieu.* London SAGE Publications, 2002.

Weick, Karl E. *Sensemaking in Organizations.* Thousand Oaks, CA: Sage Publications, 1995.

Weisgerber, Marcus. "The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt Isis." Defense One, https://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis/137833/.

Werd, Peter de. "Critical Intelligence Studies? A Contribution." *Journal of European and American Intelligence Studies* 1, no. 1 (2018): 109-48.

———. "Critical Intelligence: Analysis by Contrasting Narratives : Identifying and Analyzing the Most Relevant Truths." PhD, Utrecht University, 2018.

Wheaton, K. J., and M. T. Beerbower. "Towards a New Definition of Intelligence." *Stanford law & policy review.* 17, no. 2 (2006): 319-30.

Williams, Michael C. "The Public, the Private and the Evolution of Security Studies." *Security Dialogue* 41, no. 6 (2010): 623-30.

Wilson, Andrew. "Ukraine's Orange Revolution, Ngos and the Role of the West*." *Cambridge Review of International Affairs* 19, no. 1 (2006): 21-32.

Wirtz, James J. "Life in the "Gray Zone": Observations for Contemporary Strategists." *Defense & Security Analysis* 33, no. 2 (2017): 106-14.

———. "The American Approach to Intelligence Studies." In *Handbook of Intelligence Studies*, edited by Loch K. Johnson, 46-56: Routledge, 2009.

———. "DéJà Vu?: Comparing Pearl Harbor and September 11." *Harvard International Review* 24, no. 3 (2002): 73-77.

———. *The Tet Offensive : Intelligence Failure in War.* [in Engels] Ithaca, NY: Cornell University Press, 1991.

Wiuff Moe, Louise , and Markus-Michael Müller, eds. *Reconfiguring Intervention : Complexity, Resilience and the 'Local Turn' in Counterinsurgent Warfare*. London: Palgrave Macmillan, 2017.

WMD Commission. "Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction." *Washington, DC: US Government Printing Office* (2005).

Wolfram, Stephen. *A New Kind of Science.* Champaign, IL: Wolfram media 2002.

Wrigley, Cara, Genevieve Mosely, and Michael Mosely. "Defining Military Design Thinking: An Extensive, Critical Literature Review." *She Ji: The Journal of Design, Economics, and Innovation* 7, no. 1 (2021): 104-43.

Ydstebø, Palle. "Russian Operations: Continuity, Novelties and Adaptation." In *Ukraine and Beyond : Russia's Strategic Security Challenge to Europe*, edited by Janne Haaland Matlary and Tormod Heier: Palgrave Macmillan, 2016.

Yin, Robert K. *Case Study Research: Design and Methods.* Applied Social Research Methods Series ; Vol. 5. 4th ed., 4th print. ed. Los Angeles: SAGE Publications, 2009.

Zegart, Amy B. "Spies, Lies, and Algorithms." In *Spies, Lies, and Algorithms*. Princeton: Princeton University Press, 2022.

Zegart, Amy B. "The Cuban Missile Crisis as Intelligence Failure." *Policy Review*, no. 175 (2012): 23-39.

———. *Spying Blind : The Cia, the Fbi, and the Origins of 9/11.* Princeton, N.J.: Princeton University Press, 2007.

Zweibelson, Ben. "An Awkward Tango: Pairing Traditional Military Planning to Design and Why It Currently Fails to Work." *Journal of military and strategic studies* 16, no. 1 (2015): 11-41.

———. "'Design' Goes Dutch: Army Considerations for Unconventional Planning and Sensemaking." *Atlantisch perspectief* 39, no. 6 (2015): 31-36.

———. *Understanding the Military Design Movement: War, Change and Innovation.* Taylor & Francis, 2023.

Annex A: Case study protocol

This protocol provides more detail on the data collection of the case study. The protocol consists of four parts. First it operationalises theory to interview questions. Second, the interview questions are listed. The third part explains how the data is managed.

A1. From theory to questions

As mentioned in Chapter 5 the interview questions consist of two sets. Set 1 consists of questions regarding the complex intelligence environment as experienced by military intelligence professionals. This environment, or rather the entities that shape it, is examined with the characteristics of self-organisation, emergence, non-linearity and adaptation. The second set of questions is on how intelligence is organised within MNC NE, represented by the intelligence cycle and intelligence theory.

To formulate questions based on these theoretical concepts, they need to be operationalised. The questions regarding the operational environment (set 1) are operationalised and formulated based on the four characteristics of complexity and is grounded in Chapter 4. Self-organisation is operationalised with the concept of the edge of chaos as explained by Waldrop: a stable, yet temporary, position 'where the components of a system never quite lock into place, and yet never quite dissolve into turbulence, either'.[630] Emergence is about phenomena that constitute radical novelty; they never occurred before, nor are they predicted. These characteristics of emergence, borrowed from Page[631] and Goldstein[632], form the question on emergence. Non-linearity means a small change in input can create large effects. Furthermore, simple interactions can lead to complex patterns and vice versa. As a result, exact predictions are impossible. These properties of non-linearity, described by Capra and Luisi, form the basis for the questions on non-linearity. [633] Lastly, adaptation is operationalised with schemata (as introduced by Gell-Mann); mental

[630] Waldrop, *Complexity: The Emerging Science at the Edge of Order and Chaos*, 12.

[631] Page, *Diversity and Complexity*, 25.

[632] Goldstein, "Emergence as a Construct: History and Issues."

[633] Capra and Luisi, *The Systems View of Life: A Unifying Vision*, 105.

frameworks that organise data to understand the world.[634] These mental frameworks develop through co-evolution, a good concept to explain adaptation as an active process and not as a single and isolated cause and effect.

The second set of questions addresses the intelligence cycle and intelligence theory. To operationalise these questions Chapter 2 is re-visited. Questions about the intelligence cycle draw from the debate on the cycle. The questions are formulated along the main point of critique; the sequential and linear nature of the cycle. Regarding the topic of intelligence theory, respondents are asked questions on how they see intelligence. Is it about objectively and independently ascertaining the world of threats where causality can be observed, or if they emphasise interpretation, bias, context and uncertainty in trying to understand the environment. In other words, if they adhere to the positivist dominance of 'telling truth to power' or show postmodern features regarding the relativity of truth. Combining both sets of questions will reveal if the gap from Chapter 3 between an increasingly complex environment and an intelligence system that is lagging behind in adaptation is reflected in the case study as well.

The first few interviews revealed many alignment problems internally in the intelligence organisation and externally between the intelligence organisation and the corps and NATO. The respondents, while talking about many different topics, indicated that alignment problems were a big concern. This volume of data on alignment issues was too large to ignore and therefore the data collection was expanded by adding questions on this topic.

A2. List with interview questions

The interview questions are listed in the following sections. The list consists of the questions derived from theory, with the addition of a general introductory question for both sets of questions. Within brackets the related operationalisation concepts are mentioned. A more complete overview of how the conceptual design is operationalised to case questions is presented in Annex B.

For administrative and introductory purposes the first question was always directed at current working position, background, experience, and national culture. Such as

[634] Gell-Mann, *The Quark and the Jaguar: Adventures in the Simple and the Complex*, 25.

broad question was on purpose and served to probe the respondent's way of thinking. The other questions were about the research direction, and are listed below:

Set 1: Questions on operational environment

1. Could you describe operational environment and the challenges in understanding it? Please reflect on what the intelligence problem/requirement in this environment is.
    - *AOR & AIR/AII*
    - *(f)actors, driving forces*
    - *Warfighting domains*
2. Was your operational environment in stable condition or constantly changing? [self-organisation]
    - *If it is constantly changing, are there temporary balances or is it changing all the time?*
3. Did you experience any surprise events, i.e. events that could not have been foreseen whatsoever, in your operational environment? [emergence]
    - *Black swan/grey rhino.*
4. To what extent were you able to establish cause and effect relations, and what challenges did arise in doing this? [non-linearity]
5. To what extent did the main actors in your AO changed their behaviour as a consequence of changes in the environment? [adaptation]
    - *(Russian, or other) armed forces/government/population.*

Set 2: Questions on the organisation of intelligence

6. Could you describe how your unit organises for intelligence and what the challenges are?

7. To what extent does the intelligence cycle represent the intelligence process in your organisation?

8. Is it a linear and sequential process or are there feedback loops and more interconnections? [main points of critique from debate]

    - *Is direction a one-time occurrence for an intelligence requirement or constant examination/discussion?*

    - *How much room for interpretation of the intelligence requirements is there?*

    - *What are the partners - military, civilian or otherwise - you cooperate with outside of the cycle?*

9. What possibilities are there to make adjustments and changes in the intelligence cycle? [intelligence cycle as cybernetic feedback loop without adaptation]

    - *Can the collection scope (type of sensors, sources and thematic focus) sufficiently cover all aspects of the intelligence problem?*

    - *Is there room to adjust the collection package?*

    - *Is there enough expert analytic knowledge to understand all aspects of the environment and data on it.*

    - *What are the challenges in adjusting to emerging intelligence requirements next to the standing ones?*

10. To what extent do you think your intelligence organisation is able to generate an objective understanding of the environment? [intelligence theory; is there an objective reality (positivist) or only perception (postmodern)]

    - *Do you see your work as telling truth to power?*

    - *How much bias is involved?*

11. To what extent was your intelligence organisation able to understand and assess the operational environment? [intelligence theory]

- *To what extent was the organisation able to measure aspects of the operational environment by means of metric and tables?*
- *What frameworks do you use (intentions x capabilities x activities or ICA, joint intelligence preparation of the environment or JIPOE, etc.)*
- *To what extent was the organisation able to predict the future status of the operational environment?*
    - *Prognostic intelligence vs descriptive & explanatory*
    - *Indication &Warning, scenario's.*

12. Could you reflect upon the different cognitive and cultural perspectives present in your intelligence section or division? Do they cover all the needs? Are they being managed? [law of requisite variety]
13. Could you reflect on any collective effort across desks, branches and sections to come to an understanding of the environment? Competing perspectives? [sensemaking]
14. Could you reflect upon learning processes in your section? Evaluation, Lessons Identified/Lessons Learned system, after action reviews? [learning organisation]

A3. Data management

The data collection, analysis and storage are done only by the researcher. Data collection consists of interviews, informal conversations, observations, and (insight into) documents. The interviews, conversations, observations and insights into documents are documented on paper.

Raw data consists of these notes on paper and their transcribed, digital versions, and documents retrieved during field research. The written notes and other hardcopy documents are stored by the researcher in a private archive. The transcribed digital notes and documents are stored on an encrypted flash drive. Coded data is done, and stored, with NVIVO on a laptop. Digital documents and coded data are also stored on a flash drive for back-up storage.

To protect the identity of the correspondents, their names are not be included in any of these stored files. Instead, the only file with their identity is kept on the encrypted flash drive for the duration of the research, and deleted a year after completion.

Annex B: Operationalisation of questions

Table 17 represents how the idea of talking with intelligence practitioners about their operational environment, and how it relates to the workings of their intelligence organisation, is operationalised to actual questions. The first column, conceptual design, depicts the two sets of questions directed at the operational environment and the organisation of intelligence. The second column lists the characteristics of complexity and the organisation of intelligence that are used to focus the questions. The third column mentions the theoretical basis of the characteristics, and what their locations in the chapters are. The fourth and fifth columns list the interview questions and their number.

In order to show an understandable depiction of this process, details are left out. The characteristics of complexity (column 3) have a broader theoretical basis than what is mentioned, but these descriptions are the most concise. Also the questions contained much more detail. These were mostly topics to drive the conversation and give an example to a respondent of what was meant, or to get a more granular answer. The intelligence paradigm, originally meant to operationalise questions but was moved to the data analysis, as mentioned in section 9.2 – is left in. This is done so that annexes B and C line-up and show a complete overview from the operationalisation of questions to the data analysis.

Conceptual design	Characteristics	Theoretical basis / location in chapters	#	Questions
		Broad and open question to probe respondents' way of thinking.	1.	Could you describe operational environment and the challenges in understanding it Please reflect on what the intelligence problem/requirement in this environment is.
Operational environment	Self-organization	Edge of chaos: a stable, yet temporary, position 'where the components of a system never quite lock into place, and yet never quite dissolve into turbulence, either' (Waldrop, 1992). Section 4.3.1	2.	Was your operational environment in stable condition or constantly changing?
	Emergence	Phenomena cannot be deduced from their components, they exhibit radical novelty and are unpredictable (Page 2011 & Goldstein, 1999). Section 4.3.2	3.	Did you experience any surprise events, i.e. events that could not have been foreseen whatsoever, in your operational environment?
	Non-linearity	Small changes can create large effects, simple interactions can create complex patterns. Exact predictions are impossible (Capra & Luisi, 2014). Section 4.3.3	4.	To what extent were you able to establish cause and effect relations, and what challenges did arise in doing this?
	Adaptation	Schemata as frames of reference to understand and adapt to environment. Co-evolution as mutually influenced process (Gell-Mann, 1994). Section 4.3.4	5.	To what extent did the main actors in your AO changed their behaviour as a consequence of changes in the environment?
		Broad and open question to probe respondents' way of thinking.	6.	Could you describe how your unit organizes for intelligence and what the challenges are?
Organisation of intelligence	Intelligence cycle	Main critique debate: cycle linear & sequential. Section 2.2	7.	To what extent does the intelligence cycle represent the intelligence process in your organisation? What are the challenges?
			8.	Is it a linear and sequential process or are there feedback loops and more interconnections?
		Own critique: cycle lacks adaptation and is more of a cybernetic feedback loop. Section 2.2	9.	What possibilities are there to make adjustments and changes in the intelligence cycle?
	Intelligence theory	Positivist-postmodern dichotomy regarding objective reality. Section 2.3	10.	To what extent do you think your intelligence organisation is able to generate an objective understanding of the environment?
			11.	To what extent was your intelligence organization able to understand and assess the operational environment?
	Intelligence paradigm			
	Design properties	Requisite variety. For a system 'to be efficaciously adaptive, the variety of its internal order must match the variety of the environmental constraints' (McKelvey & Boisot, 2009). Section 4.4.1	12.	Could you reflect upon the different cognitive and cultural perspectives present in your intelligence section or division.
		Sensemaking. Structuring the unknown whereby attention is given to what is constructed, how and why this takes place, and what the effects are (Weick, 1995). Section 4.4.2	13.	Could you reflect on any collective effort across desks, branches and sections to come to an understanding of the environment?
		Organisational learning. The relation between acquiring new knowledge and the actions that follow from it (Freeman, 2007). Section 4.4.3	14.	Could you reflect upon learning processes in your section?

Table 17: Operationalisation of interview questions.

Annex C: Data analysis

Table 18 depicts the analysis of the empirical data according to the Gioia method. The first column represents the terms used by the respondents. The second column shows the themes the research used to confront the empirical data with the theory. The third column shows how the first and second order analysis tie back into the conceptual design.

Table 18 is more of an impression than a complete overview of the data analysis. As mentioned in Chapter 5, the data analysis is done in NVivo. Displaying all terms, themes, and the data they represent, is too much to present in an understandable manner here.

First order terms (respondent-centric)	Second order themes (knowledgable researcher)	Aggregate dimensions
Peacetime / grey zone / Article 5 Exercise mode versus reality. National versus NATO interests.	Self-organisation	Operational environment
	Emergence	
	Non-linearity	
	Adaptation	
Intelligence cycle (direction, collection, processing / analysis, dissemination)	Intelligence cycle as missing procedure. Proceduralist / conceptualist	Organisation of intelligence
Bias / different (cultural) perspectives Prediction / prognosis Products, methods	Positivist / postmodern Telling truth to power / objective reality Reflexive, metrics Relativity of knowledge	
Inference Known unknowns / unknown unknowns Feedback	Intelligence paradigm Clear, complicated, complex, chaos, confused.	
Alignment issues: Coordination, exchange of intelligence Interoperability (of communication systems) Direction and guidance,	Design properties (requisite variety, organisational learning, sensemaking)	

Table 18: Data analysis: terms, themes, and dimensions.

Summary

This study asserts that complexity science, the study of systems that are complex and adaptive, holds many promises for examining the threats in the operational environment as well as intelligence organisations themselves. While this may seem a logical deduction, the study of intelligence has yet to adopt the ideas and methods of complexity science. This is striking; There is general agreement on the increased complexity of threats and the security environment in general, however this is not addressed by taking a complexity turn and adapting intelligence to the changed circumstances. Therefore this study aims to seek insights from complexity science and to apply these to intelligence. In doing so it strives for a theoretical and also an empirical contribution to the study of intelligence. The empirical contribution is formed by case study research into how NATO's Multinational Corps Northeast (MNC NE) organises its intelligence. This is guided with the research question How can complexity science advance intelligence transformation?

The theoretical contribution, Chapters 2 to 4, examines intelligence studies and complexity science literature and finds that the nexus between the two fields is understudied. Next, a synthesis is offered with which to further study the nexus. Chapter 2 describes the status of intelligence transformation along three topics: a growing critique on the intelligence cycle model, a diversification of intelligence theories, and a debate about a paradigm shift in intelligence. It finds that the increased complexity of the operational environment and security context, studied in a fragmented debate, result in much ambiguity on the form and role of intelligence. Chapter 3 relates this to broader developments influencing intelligence. It borrows the five drivers-framework from Buzan and Hansen's Evolution of International Security Studies (2009) and shows how great power politics, technological developments and formative events (external drivers) constitute increased complexity while debate and institutionalisation (internal drivers) are lagging behind in response. Chapter 4 identifies several complexity lenses for intelligence that are already present in literature. In addition, the four complexity characteristics of self-organisation, emergence, non-linearity, and adaptation are adopted into the research method – as well as the design properties requisite variety, sensemaking, and organisational learning.

The empirical part of this research spans Chapters 5 to 8. It uses the intelligence cycle, intelligence theory, and a paradigm shift, in combination with the four

characteristics of complexity, and the three design properties. The object of analysis here is the intelligence organisation of Multinational Corps Northeast (MNC NE). The corps is the NATO tactical command for the defence of Poland, Estonia, Latvia, and Lithuania. The data collection took place by means of interviews with 56 (mainly) intelligence officers from 9 different corps units and commands, on how they make sense of their operational environment. As such, next to contributing to knowledge on military intelligence, this case study also contributes to the small volume of contemporary empirically-based research within intelligence studies.

The case study in Chapter 6 shows how the respondents talk about the broader NATO organisation and the operational environment as interconnected and external factors. These are seen as the origin of many challenges that exist within the corps' intelligence organisation. Remarkably, empirical data contains more on problems within NATO than about Russia or other threats. Next, the analysis is done using the four complexity characteristics: self-organisation, emergence, non-linearity, and adaptation. The cumulative conclusion of these characteristics is that the respondents experience moderate environmental complexity. This contrasts with general consensus in professional and academic literature regarding the increased complexity of the military operational environment.

Chapter 7 describes the organisation of intelligence within MNC NE in respondent terms. The respondents mainly have problems with the intelligence cycle because it is not functioning as it should do, according to doctrine, within the corps. The chapter also shows how the products and methods form the intelligence practice for observing and measuring of reality, or collection and processing in an intelligence context. Any deficiencies in this are seen as the result of a lack of resources, mandate or otherwise practical circumstances and conditions.

Chapter 8 presents the analysis of the intelligence organisation of the corps. In general the respondents are proceduralists and do not think outside the intelligence cycle. It can be seen as a cybernetic feedback loop where only a change of direction input can lead to any adaptation. This is in stark contrast with critical perspectives within intelligence literature. With regard to theory the overall stance of the respondents is a positivist one. The larger implication of this is that the military intelligence workforce employs a worldview, and methods, that are increasingly out of touch with the complexity of the practical dimensions of intelligence.

When analysing the raw data and earlier conclusions with the Cynefin framework most data points fall in the complex domain. This is in contrast to the intelligence

cycle and theory that fall in the ordered domains of clear and complicated. The reason is that most data is about the organisational and operational environment of the intelligence organisation. It is about the problem of complex phenomena within an organisation that is not necessarily suited to deal with complexity. This also underlines earlier conclusions on the gap between an intelligence organisation that is not suited to address the complexity of its environment. Overall, the case study confirms the theory from Chapters 2 and 3.

To answer the research question, complexity science can advance intelligence transformation by providing alternative insights, tested in broader military sciences and other related fields, to improve its performance. This research shows how complexity has a lot in common with intelligence. Both fields are concerned with how a system can understand its environment and how it processes information to do so. The critique on the intelligence cycle, the diversification of theory, paradigm issues, and initiatives by respondents that go against traditional intelligence all resonate some form of complexity thinking. In doing so, they form cracks in the traditional intelligence paradigm but it is still far away from any complexity turn.

Complexity science offers a language and understanding to further examine these cracks – just as it does for examining the gap between a complex environment and an intelligence paradigm meant for solving puzzles. With complexity a new intelligence paradigm is formulated, and contrasted to the traditional intelligence paradigm. The three design properties (requisite variety, sensemaking, and organisational learning) show how concepts from complexity can help to move from the traditional to the new, complexity paradigm.

With these insights this research adds to the debate around the intelligence cycle by explicitly framing it as a cybernetic feedback loop. It also adds a voice to a growing volume of post-positivist intelligence theory. This research continues the paradigm debate past the non-state actor turn and formulates a new, complexity paradigm. Another theoretical contribution is the connection laid between intelligence studies and related fields such as security studies and international relations. More theoretical contribution is made by comparing intelligence to broader military science and the study of war and warfare. This research also makes a contributions to research practice; it shows the role of military security and secrecy in scientific fieldwork, something which is rarely addressed in a practical manner. Lastly, this research provides some insight into NATO – which is very relevant considering the developments on the alliance's eastern border.

Samenvatting

Deze studie stelt dat complexiteitswetenschap, de studie van systemen die complex en adaptief zijn, veelbelovend is voor het onderzoeken van de dreigingen in de operationele omgeving en voor inlichtingenorganisaties zelf. Hoewel dit een logische gevolgtrekking lijkt, heeft het academische veld van inlichtingenstudies de ideeën en methoden van de complexiteitswetenschap nog niet overgenomen. Dit is opvallend; er is algemene overeenstemming over de toegenomen complexiteit van dreigingen en de veiligheidsomgeving in het algemeen, maar dit wordt niet gebruikt om een wending naar complexiteitsdenken te nemen en inlichtingen aan te passen aan de veranderde omstandigheden. Daarom is deze studie erop gericht om inzichten uit de complexiteitswetenschap toe te passen op inlichtingen. Daarbij wordt gestreefd naar een theoretische en empirische bijdrage aan de studie van inlichtingen. De empirische bijdrage wordt gevormd door case study onderzoek naar hoe het Multinational Corps Northeast (MNC NE) van de NAVO zijn inlichtingen organiseert. Dit wordt gestuurd door de onderzoeksvraag Hoe kan complexiteitswetenschap de transformatie van inlichtingen bevorderen?

In de theoretische bijdrage, hoofdstukken 2, 3 en 4, wordt de literatuur over inlichtingen- en complexiteitswetenschap onderzocht en wordt vastgesteld dat het verband tussen de twee gebieden onderbelicht is. Vervolgens wordt een synthese geboden waarmee dit verband verder kan worden bestudeerd. Hoofdstuk 2 beschrijft de status van inlichtingentransformatie aan de hand van drie onderwerpen: een groeiende kritiek op het model van de inlichtingencyclus, een diversificatie van inlichtingentheorieën, en een debat over een paradigmaverschuiving op het gebied van inlichtingen. Er wordt geconstateerd dat de toegenomen complexiteit van de operationele omgeving en de veiligheidscontext leiden tot veel onduidelijkheid over de vorm en de rol van inlichtingen. Hoofdstuk 3 brengt dit in verband met bredere ontwikkelingen die van invloed zijn op inlichtingen. Het leent het raamwerk van Buzan en Hansen's Evolution of International Security Studies (2009) en laat zien hoe machtspolitiek, technologische ontwikkelingen en bepalende gebeurtenissen (externe drivers) zorgen voor toegenomen complexiteit, terwijl debat en institutionalisering (interne drivers) achterblijven in reactie hierop. In het hoofdstuk worden verschillende complexiteitsperspectieven voor inlichtingen geïdentificeerd die al in de literatuur aanwezig zijn. Daarnaast worden de vier complexiteitskenmerken zelforganisatie, emergentie, non-lineariteit, en adaptatie overgenomen in de onderzoeksmethode - evenals de ontwerpeigenschappen requisite variety, sensemaking en organisational learning.

Het empirische deel van dit onderzoek beslaat de hoofdstukken 5 tot en met 8. Het maakt gebruik van de inlichtingencyclus, inlichtingentheorie, en een paradigmaverschuiving – in combinatie met de vier kenmerken van complexiteit en de drie ontwerpeigenschappen. Het object van analyse is hier de inlichtingenorganisatie van het Multinational Corps Northeast (MNC NE). Het korps is het tactische NAVO-commando voor de verdediging van Polen, Estland, Letland en Litouwen. De dataverzameling vond plaats door middel van interviews met 56 (voornamelijk) inlichtingenofficieren van 9 verschillende korpseenheden, over hoe zij hun operationele omgeving proberen te begrijpen. Als zodanig draagt deze case study niet alleen bij aan de kennis over militaire inlichtingen, maar ook aan de kleine hoeveelheid hedendaags empirisch onderbouwd onderzoek binnen inlichtingenstudies.

De casestudy in hoofdstuk 6 laat zien hoe de respondenten spreken over de bredere NAVO-organisatie en de operationele omgeving als onderling verbonden en externe factoren. Deze worden gezien als de oorsprong van veel uitdagingen binnen de inlichtingenorganisatie van het korps. Opvallend is dat de empirische data meer over problemen binnen de NAVO gingen dan over Rusland of andere dreigingen. Vervolgens wordt de analyse gedaan aan de hand van vier complexiteitskenmerken: zelforganisatie, opkomst, non-lineariteit en aanpassing. De cumulatieve conclusie hier is dat de respondenten een matige complexiteit van de omgeving ervaren. Dit staat in contrast met de algemene consensus in de professionele en academische literatuur over de toegenomen complexiteit van de militaire operationele omgeving.

Hoofdstuk 7 beschrijft de organisatie van inlichtingen binnen MNC NE in de woorden van de respondenten. Deze hebben vooral problemen met de inlichtingencyclus omdat deze binnen het korps niet functioneert zoals het volgens de doctrine zou moeten. Het hoofdstuk laat zien hoe de producten en methoden de inlichtingenpraktijk vormen voor het waarnemen en meten van de werkelijkheid, ofwel het verwerven en verwerken in een inlichtingencontext. Eventuele tekortkomingen hierin worden gezien als het gevolg van een gebrek aan middelen, mandaat of anderszins praktische omstandigheden.

Hoofdstuk 8 presenteert de analyse van de inlichtingenorganisatie van het korps. Over het algemeen zijn de respondenten proceduralisten en denken ze niet buiten de inlichtingencyclus. Deze kan worden gezien als een cybernetische feedback loop waarbij alleen een verandering van buiten inlichtingen kan leiden tot enige aanpassing. Dit staat in schril contrast met de kritische perspectieven binnen de inlichtingenliteratuur. Met betrekking tot theorie is de algemene houding van de

respondenten positivistisch. De grotere implicatie hiervan is dat de respondenten een wereldbeeld en methoden hanteren die steeds minder voeling hebben met de complexiteit van de inlichtingenpraktijk.

Bij het analyseren van de ruwe data en eerdere conclusies met het Cynefin raamwerk vallen de meeste datapunten in het complexe domein. Dit in tegenstelling tot de inlichtingencyclus en -theorie die in de geordende domeinen clear en complicated vallen. De reden hiervoor is dat de meeste data gaan over de organisatorische en operationele omgeving van de inlichtingenorganisatie. Het gaat over het probleem van complexe fenomenen binnen een organisatie die niet noodzakelijkerwijs geschikt is om met complexiteit om te gaan. Dit onderstreept ook eerdere conclusies over de kloof tussen een inlichtingenorganisatie die niet geschikt is om met de complexiteit van haar omgeving om te gaan.

Om de onderzoeksvraag te beantwoorden: complexiteitswetenschap kan de transformatie van inlichtingen bevorderen door alternatieve inzichten te bieden, die zijn getest in de bredere militaire wetenschappen en andere verwante vakgebieden, om de prestaties ervan te verbeteren. Dit onderzoek laat zien dat complexiteit veel gemeen heeft met inlichtingen. Beide gebieden houden zich bezig met de vraaghoe een systeem zijn omgeving kan begrijpen en hoe het informatie verwerkt om dat te doen. De kritiek op de iinlichtingencyclus, de diversificatie van theorie, paradigmakwesties, en initiatieven van respondenten die tegen traditionele inlichtingen ingaan, resoneren allemaal complexiteitsdenken. Daarmee vormen ze scheuren in het traditionele inlichtingenparadigma, maar het is nog ver verwijderd van een volledige wending naar complexiteit.

Complexiteitswetenschap biedt een taal en begrip om deze scheuren verder te onderzoeken – net zoals het dat doet voor het onderzoeken van de kloof tussen een complexe omgeving en een inlichtingenparadigma dat bedoeld is om puzzels op te lossen. Met complexiteit wordt een nieuw paradigma geformuleerd en afgezet tegen het traditionele intelligentieparadigma. De drie ontwerpeigenschappen (requisite variety, sensemaking en organisational learning) laten zien hoe complexiteitswetenschap kan helpen om van het traditionele naar het nieuwe, complexe paradigma te gaan.

Met deze inzichten draagt dit onderzoek bij aan het debat over de inlichtingencyclus door deze expliciet te beschrijven als een cybernetische feedback loop. Het voegt ook een stem toe aan de groeiende hoeveelheid post-positivistische inlichtingentheorieën. Een andere theoretische bijdrage is de verbinding die wordt

gelegd tussen inlichtingenstudies en verwante vakgebieden zoals internationale veiligheidsstudies en internationale betrekkingen. Een andere theoretische bijdrage wordt geleverd door inlichtingen te vergelijken met de bredere militaire wetenschap en de studie van oorlog en oorlogsvoering. Dit onderzoek levert ook een bijdrage aan de onderzoekspraktijk; het toont de rol van militaire veiligheid en geheimhouding in wetenschappelijk veldwerk, iets wat zelden op een praktische manier aan de orde komt. Tot slot geeft dit onderzoek enig inzicht in de NAVO - wat zeer relevant is gezien de ontwikkelingen aan de oostgrens van het bondgenootschap.

Acknowledgement

This PhD has been a transformative experience. It has changed all I knew about intelligence and the military. It brought me new philosophical and scientific perspectives, and I chased after a thousand others. That is why, naturally, my gratitude goes out to my supervisors prof.dr.ir. Bas Rietjens and dr. Maarten Rothman. They did their best to keep me from incorporating even more fields of knowledge. Even more, they strengthened this entire endeavour throughout with scientific guidance, and intellectual integrity and curiosity. Bas, thank you for always seeing opportunities, forcing me to improve my reasoning, and for picking restaurants in foreign countries. Maarten, thank you for always infusing any situation with a healthy dose of critical perspectives, showing my writing skills can still be improved, and talking about D&D and other nerdery to give my brain much needed breaks. I am also indebted to colonel Hans van Dalen and colonel Jos Brouns (retired) who gave me the opportunity to pursue this PhD – and to colonel Piotr, lieutenant-colonel Robert, and the soldiers of Multinational Corps Northeast who gave me the opportunity to do field research that is as relevant as it was exciting.

While doing a PhD can be a lonely process I never experienced this as such. I was lucky to have a group of fellow PhD travellers at the Faculty of Military Sciences from the Netherlands Defence Academy. Thank you for sparring, venting, and encouraging. A special thanks to Pepijn, Tess, and Paul for their support and humour through the pandemic. I would also like to thank the commanders and personnel of the Intelligence and Security Academy for providing a testing ground for my ideas and engaging with much that I threw at them.

This PhD adventure would not have been possible without the unwavering support of my parents, my sisters and their families, my friends, and Chantal. You all are the foundation of everything I have accomplished.

For this PhD, as with all cognitive endeavours, I owe everything and all to my brother Joost Vervoort. Our lifelong and relentless pursuit of knowledge, art, and dark spaces of the mind means everything to me. I am both curious and afraid where this left-hand path of life will take us.

Lastly, I want to thank my wonderful daughter. You truly are the light of my life and keep me sane. This PhD is dedicated to you. Always keep learning and make the world your own.

Curriculum Vitae

Bram Spoor studied International Relations at Utrecht University from 2006-2009, obtaining a Master of Arts degree. He then joined the Dutch Army and graduated from the Royal Military Academy's specialist track in 2009. Since then Bram serves as an officer in various positions, including several deployments. From 2018-2024 he wrote his dissertation at the War Studies department, Faculty of Military Sciences, Netherlands Defence Academy. Bram gives several courses and lectures on intelligence, ranging from intelligence basics for military cadets to complexity approaches for intelligence practitioners throughout the Dutch intelligence community. Bram has published on the nexus of intelligence and complexity science.

Intelligence is failing to keep up with the complex security challenges of the 21st century. It is sufficient to say that (the study of) intelligence missed the complexity turn in the social sciences. This research seeks to remedy this by infusing intelligence with complexity. It aims for a theoretical (complexity science) and an empirical (case study research) contribution to the study of intelligence. The case study research features NATO's Multinational Corps Northeast and is based on interviews with 56 (mainly) intelligence officers from nine different corps units and commands, on how they make sense of their operational environment.

9789493124417