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

Spoor, B.E.P.

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]

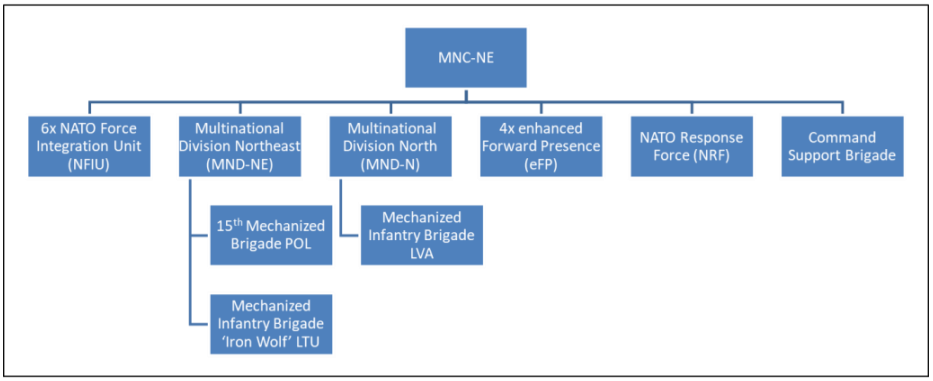

Figure 8: Peacetime organisation of MNC NE.[580]

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.