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

Spoor, B.E.P.

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.