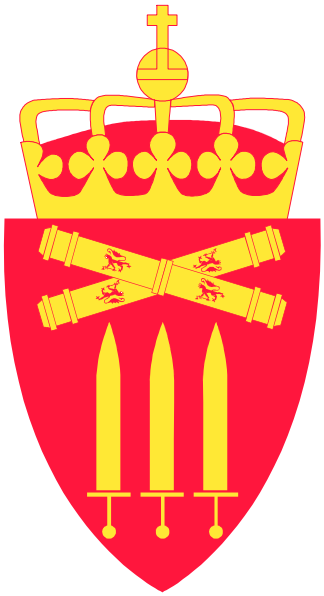

Norwegian Defence Command and Staff College

Spring 2010

Master thesis

Intelligence sharing with host nations in multinational operations:

Hurdles and dilemmas in Afghanistan

Helge Arnli

Abstract

This thesis explores a narrow but important aspect of the conflict in Afghanistan when it seeks to identify limitations on ISAF's ability for sharing intelligence with the Afghan National Security Forces. The case study is exploratory and utilizes a mixed methods approach where the initial qualitative phase aims to identify what ISAF intelligence officers recognize as hurdles for sharing. Data is collected through interviews, field observations and participation in partner meetings. The concurrent quantitative phase is based on a survey of all-source analysts and aims to expand on the qualitative research and also to identify how the analysts' perceptions influence ISAF's ability for intelligence sharing.

Even though ISAF has got the appropriate documentation and processes in place, a lack of education, training and open debate on moral dilemmas leave too much latitude and uncertainty in the hands of individuals. Missing quality control with the work of interpreters, the absence of universal standards for security markings, different national policies, procedures and caveats together with a mix of theatre-wide information systems are major obstacles for collaboration and limit ISAF's ability for sharing intelligence with the Afghan National Security Forces. Also the underdeveloped Afghan security standards add problems of legitimacy, and it degrades the important level of trust between the partners. The combined effect of these challenges seems to be less sharing, and at a higher security cost than probably intended.

Acknowledgements

This paper was completed as part of my master studies at the Norwegian Defence Command and Staff College during the autumn 2009 throughout the first half of 2010. To conduct unclassified research on intelligence matters during an ongoing operation is not straightforward, and was only made possible through the support and kind participation of dedicated intelligence professionals at various ISAF headquarters.

First of all, I would like to thank my advisers Torunn Laugen Haaland at the Norwegian Institute for Defence Studies in Oslo and Professor Michael Rainsborough at Kings College in London; Torunn for her extremely patient and professional guidance throughout this for me challenging but rewarding adventure; and Professor Rainsborough for his professional insights and enthusiastic comments during the difficult initial phases of the research. I would also like to thank intelligence leaders in ISAF Joint Command and Regional Command North, not only for receiving me and allowing me to carry out my research, but also for endorsing the project and for providing valuable assistance in a busy operational environment. My special thanks go to Jo Hatlemark and Tor Moe for their help with arranging the field studies; to those unnamed ISAF intelligence professionals that made themselves available for the research; and also to the Norwegian Contingent Commander and the Norwegian Support Element for their hospitality and administrative support. The excellent librarians at the Norwegian Defence University College deserves acknowledgement for their help and support throughout, and I have received invaluable linguistic assistance from a colleague. Last but not least I would like to thank my wife and sons for standing by me and supporting me through my shifting emotions over the last few months. You are as always my safe and secure home base…

Helge Arnli

Oslo, 25 May 2010

Table of contents

Figure list

1 Introduction

At the time of writing in early 2010 the Afghanistan conflict has entered its 9th running year and President Obama has announced another significant U.S. troop increase. The present thesis will look into a narrow but important aspect of this conflict. Its purpose is to identify limitations on the International Security Assistance Forces' (ISAF) ability to share intelligence with the Afghan National Security Forces (ANSF).

Why intelligence sharing? ISAF is authorized by the United Nations (2001) to render support to Afghan Authorities. In short its exit strategy is to make itself redundant through the development of, and eventual transfer of security responsibilities to, the ANSF. Anthony Cordesman has in a few words argued the central rationale for such a strategy (2009, p. ii):

> NATO/ISAF and U.S. forces cannot win this kind of military victory on their own. Their success will be determined in large part by how well and how quickly they build up a much larger and more effective Afghan National Security Forces (ANSF) first to support NATO/ISAF efforts, then take the lead, and eventually replace NATO/ISAF and US forces.

This strategy implies two distinct ISAF activities vis-à-vis the ANSF (UN, 2009): (1) to reform, enhance and expand their force structure; and (2) to partner with them in operations. The interdependence that stems from operational partnership rests on mutual situational awareness, something Michael Herman (2001) alludes to when he argues that common intelligence assessments are prerequisite for collective action by coalitions of the willing. In the present Afghanistan context the coalition must necessarily also embrace the host nation security forces. Dame Pauline Neville-Jones adds that "there have to be some generally accepted basic principles to which all forces involved in an operation sign up. The starting point has to be minimizing the risk of the forces involved while maximizing their effectiveness." (2003, p. ii). Both principles are dependent on good intelligence support, indicating that ISAF's force protection and ultimate success hinge on functioning intelligence collaboration with the ANSF. It is this partnering activity that forms the point of departure for the present thesis.

However, this kind of collaboration is not well described, either within the existing academic literature or in military doctrines. The American Joint Publication 3-24 on counterinsurgency operations (Joint Chiefs of Staff, 2009) has devoted less than half a page on the issue of intelligence integration with the host nation. The doctrine states that sharing is important, but counters this advice with a prudent reminder on the need for protecting sources and capacities as well as on the threat of infiltration.

The design of the present thesis is inspired by John W. Creswell's (2009) latest contribution to the field of social science research methodologies and processes. Its philosophical worldview is problem-centred and real-world oriented – a pragmatism that fits well with the author's professional background as a military officer. The study utilizes a mixed methods approach with a concurrent triangulation strategy that will be presented in greater detail in chapter 2. Chapter 3 will introduce an analytical framework comprising basic assumptions of factors that could limit intelligence sharing from a multinational force to the host nation in contexts like in Afghanistan. Chapter 4 aims to identify what ISAF intelligence officers recognize as hurdles for intelligence sharing with the ANSF, including how they understand the force' policy and how they practice such sharing. The empirical basis is five semi-structured interviews with centrally placed ISAF intelligence officers as well as field observations and participation in partner meetings. Chapter 5 aims to expand on the qualitative research and to identify how analysts' perceptions of the sharing environment influence ISAF's ability for intelligence sharing. The empirical basis is a survey of all-source analysts within "ISAF Joint Command" (IJC) and "Regional Command North" (RC (N)). Chapter 6 will summarize the findings and draw conclusions on those issues that limit ISAFs ability for sharing intelligence with the Afghan National Security Forces.

At this point it is prudent to inform about my personal experience from serving as chief of ISAF Headquarters Combined Joint Intelligence Planning Section (Chief CJ2 Plans) from December 2008 to June 2009. Intelligence sharing with our Afghan counterparts was already then regarded as important, and my section was deeply involved. The research question thus stems from being exposed to a real-world practical problem: *What limits ISAF's ability for sharing intelligence with the Afghan National Security Forces?*

Lacking proper intelligence theories or even a clear definition of intelligence itself (Treverton, Jones, Boraz, & Lipscy, 2006) the analytical framework of my research will start with a discussion of three basic models of the intelligence cycle. These rather plain models with their

step-by-step approach to intelligence production are central for understanding how intelligence organizations and national communities work, but they are not sufficient to explain how they interact and collaborate with foreign partners. Herman's model (1996), later discussed by Robert M. Clark (2007) and evolved by Sir David Omand (2009) will therefore be expanded in chapter 3 for the purpose of this study by the introduction of two central concepts: (1) *communication* per se; and (2) *circular reporting.* It will be argued that these two concepts comprise important interface hurdles for intelligence sharing. Communication with foreign partners is difficult because of the need for interpretation and because of cultural differences. Circular reporting, which means that shared intelligence is channelled back into the intelligence cycle as new information, is a hindrance towards sharing because the efforts to expose it soaks up scarce analytical resources.

Based on a review of central texts on intelligence and my personal experience as an intelligence officer, three additional factors have been added to the analytical model which will be used to focus the research. The combination of these three factors make up what this study refers to as the sharing environment. *Secrecy* (3) is the most distinctive feature of intelligence and is used as a means for protection of information about capacity, methods and sources (Herman, 1996). The need for secrecy is in itself a hindrance for sharing of all types of intelligence in all types of settings, but certain characteristics of the Afghan context make sharing even more demanding. The *multinationality* (4) of the force including multilateral frameworks for intelligence sharing is also likely to be a hindrance toward sharing because of interface hurdles and differences in national policy, procedures, processes and capacity. Finally, intelligence *ethics* (5) and moral dilemmas of those involved are likely to be a hindrance towards intelligence sharing because of the potential fatal consequences of sharing what should have been withheld, and conversely the same effects of not disseminating what should have been shared.

In a partnership like the one between ISAF and ANSF the sharing of information and intelligence is a two-way road. The exchange will become easier and more unrestricted further down in the chain of command with fewer countries involved (as the research demonstrates, these two issues are closely related). The present research is however focussed on identifying difficulties arising from the dynamics on a multinational level. In ISAF this narrows the scope to higher headquarters from the regional level up. Further, it is the ability of the multinational ISAF rather than the will or ability of the Afghans that will be investigated. The aim is therefore to identify what limits ISAF headquarters' ability for disseminating intelligence to the ANSF, and

not the other way around. In a setting characterized by secrecy, trust and personal responsibilities, the organizational ability for sharing is, however, affected by the willingness of single intelligence professionals to produce and share intelligence. This will is dependent on the analysts' knowledge of ISAF's policy, procedures and processes for intelligence sharing as well as their perceptions of the sharing environment to include their host nation partners, demanding this to be a major part of the research.

2 Research design

This research, which aims to identify limitations on ISAF's ability to share intelligence with the Afghan National Security Forces, will be conducted as an exploratory case study (Yin, 2003) utilizing a mixed methods approach with a concurrent triangulation strategy (Creswell, 2009). The exploratory nature comes as a consequence of limited existing studies on multinational intelligence collaboration in similar contexts. My rationale for choosing a combination of qualitative and quantitative methods is to enhance the reliability of the data on this relatively sensitive topic. Creswell (2009) suggests such mixed methods designs precisely when qualitative or quantitative methods alone seem inadequate for understanding the problem. He also proposes that "in a concurrent triangulation approach, the researcher collects both quantitative and qualitative data concurrently and then compares the two databases to determine if there is convergence, differences, or some combination." (p. 213).

The point of departure for my research will be some basic assumptions on factors that could limit intelligence sharing from a multinational force to the host nation in contexts such as Afghanistan. These assumptions will be developed through a literature review were Herman's (1996) seminal work "Intelligence power in peace and war" is central, but the work will also be informed by my own experiences. The assumptions are not hypotheses to be tested, but rather part of an analytical framework acting as focussing lenses for the research. During the field studies it was, however, important for me to keep an open mind to unexpected outcomes. One part of the framework is a modified model of the intelligence cycle. The model will be developed and presented in chapter 3 for use in this specific study, but it could potentially have wider and more general applications.

The case study is limited to examining how central ISAF intelligence professionals at a specific point in time consider the possibilities for intelligence sharing with their Afghan counterparts. Data was collected during my field trip to Afghanistan from 2 to 17 February 2010, only a few weeks after Major General Michael T. Flynn made public his "Blueprint for Making [American] Intelligence relevant in Afghanistan" (Flynn, Pottinger, & Batchelor, 2010). For the intelligence community this directive was epoch-making, and as significant as the recent developments in ISAF's command and headquarters structure.[1] To collect data so early in the implementation phase of both these processes could have influenced the results in various ways. To postpone the

[1] ISAF's organizational developments throughout the autumn 2009 are presented in more detail in paragraph 4.1.

field trip was, however, not a practical option. Both the interview guide (annex B) and the survey questionnaire (annex C) was developed in Norway and tested among experienced Afghanistan analysts on 20 January 2010. This test provided valuable inputs for a final calibration of these instruments.

The purpose of the qualitative interviews (chapter 4) was to identify what ISAF intelligence officers recognize as hurdles for intelligence sharing with the ANSF, including how they understand ISAF's policy and how they practice such sharing. The empirical base is five interviews; three with intelligence officers in IJC at Kabul International Airport; and two with similar personnel in RC (N) close to Masar-e Sharif. All five occupied central positions related to sharing, and most of them as senior all-source analysts. I selected these officers based on discussions with intelligence leaders in the two commands precisely for their experience and involvement in intelligence collaboration with the host nation. During my two weeks' stay in Afghanistan I also had the opportunity to observe work practices, to discuss with intelligence leaders and staff members, and to participate in collaborative partner meetings and official briefings.

The purpose of the quantitative research (chapter 5) is to expand on the qualitative research and to identify how analysts' perceptions of the sharing environment influence ISAF's ability for intelligence sharing.[2] The empirical data was collected through a survey of 19 all-source intelligence analysts from IJC and seven from RC (N), representing the majority of such personnel in the intelligence hubs of those commands.[3] Because of the inherent intelligence sensitivities, a cross-sectional self-administered questionnaire was chosen as the best vehicle for accessing this type of data. The questionnaire consists of 25 items, each presenting five alternative answers on a Likert scale. It also contains three open-ended questions. The demographic part of the questionnaire was developed with a view not to challenge general intelligence sensitivities, separating only military from civilian employees and establishing their intelligence experience with ISAF.

[2] As discussed in chapter 1, the term "sharing environment" in this study comprises of, and refers to, the three factors *secrecy*, *multinationality* and *ethics*.
[3] The applicable intelligence organizations of IJC and RC (N) are presented in more detail in the opening paragraphs of chapter 4.

The field trip was divided in two periods, with the first nine days spent in IJC and the rest in RC (N). The two first days in both commands were used for familiarization, introduction and more general discussions with intelligence leaders. The bulk of the time was then used for interviews, participation in meetings and briefings as well as for observations and conversations. With one exception the interviews were carried out in Norwegian establishments. The final action in both IJC and RC (N) was to conduct the survey. After a plenary introduction, this was carried out at each analyst's work place without my presence. Transcription of the interviews and sorting of survey data were completed in Afghanistan while I still had easy access to the respondents, while the actual analysis was done in Norway immediately after.

The reliability of the data could have been influenced by preconceptions and biases that stem from my background as an intelligence analyst and former ISAF employee. The fact that the research was welcomed by ISAF as both timely and relevant could similarly have influenced respondents to act and appear more involved and proactive than they genuinely were. It may also be that respondents with varied cultural and linguistic backgrounds understood questions and survey statements differently. To remove some of this potential ambiguity, tests of both the interview guide and survey questionnaire were conducted in advance. In order to obtain reliable data on sensitive topics it was important for me to guarantee the respondents' anonymity, even if this would make it harder for others to trace the research. The reliability could also have been affected by the fact that data was collected by an officer senior to many in the target group, and who benefited from recent operational experience. Sensitive about this, respondents could have been eager to impress with their own and ISAF's recent progress. Also security sensitivities could have influenced the reliability of especially the unclassified interviews. Instead of following their impulse not to discuss certain issues, respondents could have felt compelled to answer something or anything. Finally I would like to emphasize that an unclassified study on intelligence sharing can only hope to scratch the surface on some of the more sensitive topics. One such issue is how national policy on intelligence sharing and caveats differ between the ISAF troop-contributing nations.

When it comes to the internal validity of the study, it is worth mentioning that IJC was only a few months old at the time of data collection. The headquarters staff, which partly emanated from the old ISAF headquarters, was still in a run-in period and adapting to new realities. The increased emphasis on intelligence collaboration and associated documentation on policy and practices was equally fresh, while the operational tempo was as high as ever. To compensate for

such challenges the research covered two quite different headquarters, with RC (N) temporarily lesser marked by the new initiatives. Still, IJC and RC (N) count for only two of the altogether seven multinational ISAF headquarters at or above the regional level. The total number is even higher if the headquarters of the new NATO Training Command is included. The thesis therefore represents a snapshot of no more than roughly a quarter of the multinational headquarters at a very turbulent and hectic period for ISAF.

To counter these validity challenges the research utilizes three tools proposed by Creswell (2009): (1) triangulation between qualitative and quantitative methods; (2) rich and thick descriptions; and (3) detailed step-by-step explanations. Even if some scholars, and among them Helen Simons, find that "combining or mixing methods does not necessarily strengthen validity" (Simons, 2009, p. 130), I propose that parts of my research as well as the validity of certain findings were dependent on such an approach. Finally, Yin proposes "to have the draft report reviewed, not just by peers […] but also by the participants and informants in the case." (2003, p. 159). A last effort to improve the overall reliability and validity of the study was thus to give ISAF a chance to review a draft version of the paper. Even if the external validity of this confined case study is limited, it brings to light issues that would restrict intelligence sharing in similar contexts. As such, some of the findings could be transferrable.

3 Analytical framework

The purpose of this chapter is to introduce an analytical framework with basic assumptions of factors that could limit intelligence sharing from a multinational force to the host nation in contexts like the one in Afghanistan. To frame the discussions and for better appreciating the "elusiveness" of intelligence as a research area, it will open with a short review of the state of intelligence theory and definitions, emphasising how this relates to sharing. The discussion will then focus on three basic models of the intelligence cycle; their shortcomings related to sharing and consequently propose a modified model that is better suited to identify challenges for such sharing. *Communication* and *circular reporting* are two such challenges that will be illustrated in more detail in chapter 4 through the use of case specific examples. Finally, this chapter will introduce the three focussing factors or lenses that together form the sharing environment in this study: *secrecy*, *multinationality* and *ethics*.

3.1 Intelligence theory and how it relates to sharing

Intelligence as a phenomenon is complex and elusive, both in itself and even more so within the framework of international relations. To recognize aspects of this "specialness" is essential for appreciating the challenges associated with multinational intelligence sharing. A short review of the academic, political and military discourse related to intelligence theory and sharing will do much to accomplish this.

When, on 15 Jun 2005 the U.S. Office of the Director of National Intelligence and RAND Corporation gathered 40 practitioners, academics, and specialists from Europe and North America for a one-day workshop to discuss how theories underlie American intelligence work and how they could lead to a better understanding of intelligence, it became clear (Treverton, et al., 2006) that: (1) there is no uniquely, either American or any other theory of intelligence; (2) there is not even a common agreed definition of intelligence; and (3) there are also diverging views on the very essence of intelligence. Finally, in the context of different national practices, there is also a lack of academic agreement on the dividing lines between foreign and domestic intelligence, and between domestic intelligence and law enforcement.

In its conclusion the workshop report focuses on the observation that under the present security challenges even the strongest states becomes more coalition builders than unilateral "doers", and it singles out the importance of intelligence sharing (Treverton, et al., 2006, p. 32):

> Here, a theory of intelligence might help intelligence move beyond its *ad hoc* initiatives. Theory might help because moving intelligence back and forth to state and local partners, let alone non-friendly limited partners in the war on intelligence [terror], will take intelligence back to first principles: who needs what, when, and how? What is intelligence? What is classification and "need to know"?

This line of thought brings the report (p. 32) to rhetorically paraphrase and expand on questions earlier proposed by Michael Herman:

> Now, as the nature of states change, how far can their intelligence services become focal points for cooperation, even transparency? What are the limits of their potential to reach out, not just sharing choice tidbits with favoured partners, but engaging in joint problem-solving with corporations and NGOs, as well as states and local authorities and foreign partners?

It is evident from these discussions that even under the threat from international terrorism, states and agencies feel challenged when intelligence is proposed as a vehicle for cooperation. Herman (1996) suggests that security considerations limit the willingness of states to engage in intelligence collaboration and sharing. He further suggests that "every new foreign exchange is a new risk […]." (p. 207). This ingrained scepticism is part of the backdrop for any serious debate on intelligence sharing. Introverted risk considerations and self censoring leads to restraints that cause both international and inter-agency friction. This kind of "cultural isolation" in turn spurs articulated as well as latent differences in policy and execution, resulting in a rather motley and elusive baseline for those tasked with drawing up intelligence policy and practical procedures for a multinational force.

After 9/11 the political mood in many Western countries has turned towards more intelligence cooperation. The communities are, however, permeated with conservatism and they are for many reasons slow to react, even within national confines. After the failed 2009 Christmas Day terror plot to bring down a commercial jetliner en route to from Amsterdam to Detroit, New York Times journalists Jeff Zeleny and Helene Cooper cited White House officials eluding to the (still existing) domestic problem of sharing: "[…] The president was standing by his top national security advisers, including those whose agencies failed to communicate with one another." (Zeleny & Cooper, 2010, Jan 6).

The difficulties that were identified by Herman already in 1996 are evidently much the same after more than a decade of coalition operations from the Balkans via Afghanistan to Iraq. The latest American doctrine on counterinsurgency operations admits that "foreign disclosure guidelines could be a significant constraint to intelligence sharing with *allies* [my italics]" (Joint Chiefs of Staff, 2009, p. V3).[4] What then about sharing with unknown host nation partners? The doctrine continues: "This [sharing intelligence with coalition partners] is important in maintaining the integrity of a common holistic understanding of the OE [Operational Environment]." When discussing integration with the host nation, the doctrine simply asserts that "sharing intelligence with HN [host nation] security forces and government personnel is an important and effective means of supporting their COIN efforts." (p. V14). However, this is immediately followed by a caveat:

> When sharing intelligence with the HN, it is important to understand the level of infiltration by insurgents or foreign intelligence services. Insofar as possible, intelligence should be tailored so required intelligence still gets to HN consumers but does not give away information about sources and capabilities.

3.2 The intelligence cycle

A multinational force ability to share intelligence with the host nation depends inter alia on how that nation is aligned with, and adapted into the overall intelligence production cycle. Any new partner has to be treated both as a source of information and as a user of intelligence. As a source the partner will be judged by the timeliness, reliability and validity of the information it provides, and as a user by its ability to safeguard and not misuse the intelligence it receives. On this frontier of multilateral interaction are some general challenges for intelligence sharing: (1) to secure that written and verbal communication transcends language and cultural barriers with its contents and meaning intact; and (2) to safeguard against unchecked information backflows into the production cycle. Mechanisms for dealing with both these challenges will act as throttles on the multinational force ability to share intelligence. To visualize this it is necessary to stipulate a

[4] American National Disclosure Policy is described in some detail in Joint Publication 2-0: Joint and National Intelligence Support to Military Operations, Annex E (Joint Chiefs of Staff, 2004): "USG [United States Government] policy is to treat classified military information as a national security asset, which may be shared with foreign governments and international organizations only when there is a clearly defined advantage to the United States. […] in exceptional cases it will be in US interests to make information available to a foreign government before concluding an [security] agreement, even if the recipient government's safeguards appear inadequate."

model by how intelligence is produced in a multinational setting, including how a third party fits into the overall intelligence cycle.

3.2.1 Traditional models

In the midst of all controversies and discussions that surround intelligence definitions and theories, practitioners and scholars at least seem to agree on a few basics for a model of the intelligence process. Herman's (1996) basic version introduces three main stages: (1) collection with single-source outputs; (2) all-source analysis drawing from all available information; and (3) dissemination of intelligence reports to the policy and decision-makers. He also explains an intermediate stage between analysis and users where the broader intelligence community produces top level national assessments.[5] The problem with this and prospective models is that they create expectations of a fixed sequential process from collection via analysis to dissemination. The truth is, as Herman alludes to in his *fuller* intelligence process portrayed below (1996, p. 43), that intelligence and information is disseminated to the users from all stages in the process. Another of his findings is that "output of single-source collection incorporates substantial analysis and interpretation" (1996, p. 41), and that collection agencies function almost as stand-alone intelligence centres with single-source products going directly to users. Herman then turns our attention to the crucial division of responsibility between single-source communities as experts on techniques and all-source communities as experts on subjects.

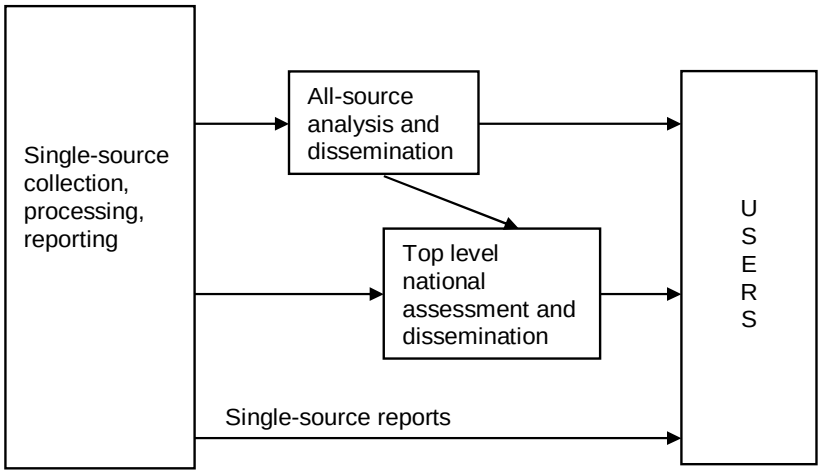

Figure 1: Herman's "Fuller intelligence process"

[5] In this study the term *assessment,* primarily a UK definition used for common intelligence products, is used to cover all finished forward-looking intelligence products, including the similar *estimate* used by the U.S. in inter-agency National Intelligence Estimates (NIE).

Before looking at other generic models it is important to notice that they all have a purely national perspective where intelligence – in principle – is produced bottom-up in a one-way stream from collectors to users with direction and tasking flowing the other way. In a multinational setting this is more complex. Here all-source analysts will receive and use a range of products from single-source outputs to finished intelligence products, much of it stemming from organizations and processes controlled by troop-contributing nations rather than by the multinational force they are supporting. How this influences intelligence sharing and how it may be incorporated in the models will be discussed later.

In Robert M. Clark's discussion of a target-centric approach to intelligence analysis he presents a traditional model of what he describes as "almost a theological concept" of an intelligence cycle (2007, p. 11). With six steps, this model may look somewhat different than Herman's, but the similarities are in fact bigger than the differences. The circular structure and arrows seem to emphasize a one-way cycle that according to Herman and many intelligence practitioners is misleading. This is exactly Clark's point, and he spends some time criticizing the model for its many flaws, among them also for constraining the flow of information. The reason for bringing forward Clark's *traditional* model rather than the one he proposes as an alternative is that it more closely resembles what nations teach in their doctrines and intelligence courses. The model that is presented in the American intelligence doctrine (Joint Chiefs of Staff, 2007) could act as an example, even if that variant is without arrows and has the mission included in the centre.

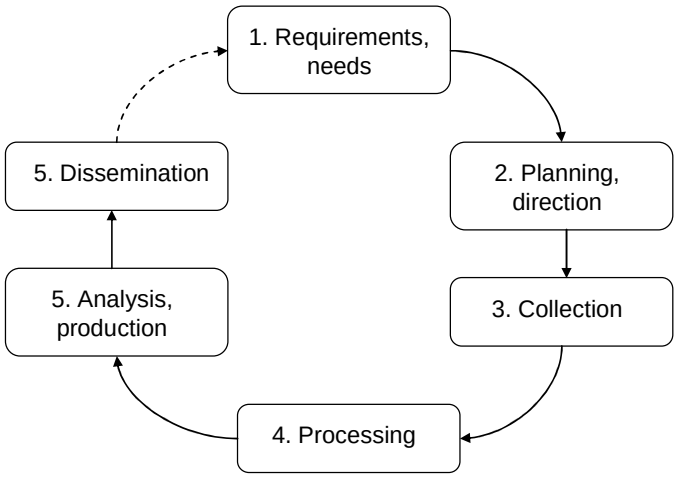

Figure 2: Clark's "Traditional Intelligence Cycle"

For our purpose the biggest difference between Herman and Clark is the isolation of the processing step from collection. This new step includes translation, decryption, validation and organization of the content into report formats. It however misses to explain that collector agencies or sections de facto execute their own dissemination to all-source agencies or sections as well as directly to intelligence users. A more thorough discussion of what it means to organize information into reports would hint to this. One formality is to include a proper security classification – something that no professional would forget. Another is to label it for release to foreign countries and/or organization(s), and a third and less frequently used is to annotate if further distribution is permitted. The last is admittedly less of a regular formality than a practical adaptation in the field. One example of how documents can be marked for further distribution is: "This report can be released to Afghan Authorities". These formalities are, together with the communication channels used, the vehicles by which intelligence operators on all levels influence and control the dissemination of their products. Here is where the producers display restraints and fears and where they prove their good will or credulity related to intelligence collaboration and sharing. Much more than personal credibility is at stake, something that will be discussed later.

The last model to be introduced is one that Sir David Omand (2009) presented during the autumn 2009 Professional Advanced Intelligence Course at the Norwegian Defence Command and Staff College in Oslo. To answer some of the criticism of earlier models he places user interaction outside the cycle, while keeping corporate direction of intelligence collection and production inside.[6] He then includes a new first (and last) step of the cycle highlighting the overall intelligence goal of improving decisions and enabling action. Herman's first stage and Clark's collection step has been developed under the new label "accessing", highlighting that modern intelligence operations not only happen behind enemy lines, but also by accessing data protected personal information (something Omand labels PROTINT) and through more extensive use of open source information. Another difference is that Herman's analysis and intermediate assessment stages, or Clarks analysis and production step, has been grouped under the new label "elucidating".

[6] Scholars and practitioners tend to discuss exactly how close the interaction or dialogue between intelligence producers and their customers should be, and how the production should be directed. As for products, the end users of intelligence typically want (Omand, 2009): "Raw reporting, as fast as possible (but validated and caveated) [then] analysed intelligence, in its context with understanding of significance [and finally] assessed intelligence, all-source, with explanatory power, forward looking but informed by understanding of the past."

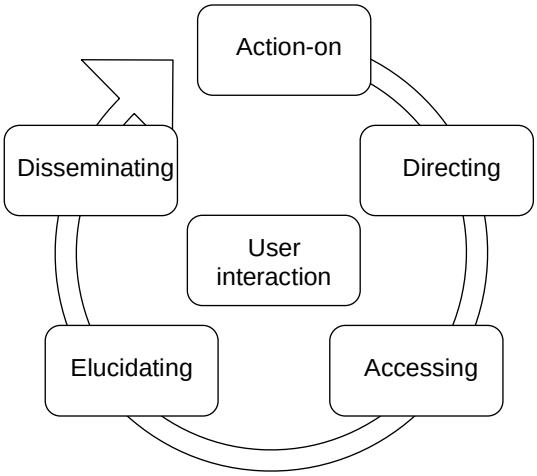

Figure 3: Omand's new intelligence cycle

This latest model answers, though it could be argued in a too simplistic way, much of the earlier criticism of user interaction with the different steps or stages of the intelligence process. However, it still presents it as a one-way continuous cycle. This is not wrong, but as earlier argued nor does it tell the full story. The model still misses to visualize intervening feedback loops as well as the separate mini-cycles that occur within each collection agency or section. The latter point is especially relevant for understanding problems related to multinational intelligence sharing in a setting where all-source analysts are pooled together from different nations and cultures and fed a mixture of single and all-source products over which they have little ownership or influence. Analysts simply have to view received information as a product of its own intelligence cycle and they have to honour its security classification and authorized disclosure.

3.2.2 A modified model that visualizes challenges for sharing

A modified model, specific for this study, is informed by all three versions above and proposes a baseline for better understanding intelligence collaboration between international partners, including between a multinational force and the host nation. It could be argued that it also better reflects the overall intelligence universe where collectors and analysts receive and utilize information from both domestically controlled sources and foreign partners alike, and were they disseminate their products to national and foreign users as well as to intelligence colleagues within their own community. In order to promote a holistic understanding of the intelligence production cycle, and for completeness, the model includes a typical user-producer interaction

with on the one hand the resource and tasking dialogue informed by intelligence requirements and costs, and on the other the product dialogue where the producer supports the user acquiring the best possible understanding of the disseminated intelligence. The product dialogue is typically also used for clarifications and adjustments of the requirements.[7] In a multinational setting where the distance is greater between producers and users and where there are more hurdles, the interaction will often be limited to responding to each other's formal requirements for information with less room for dialogue or discussions. In accordance with mutual understanding and agreements the partners provide each other with anything from raw data to finished products, but the flow will be controlled by a stern disclosure process.

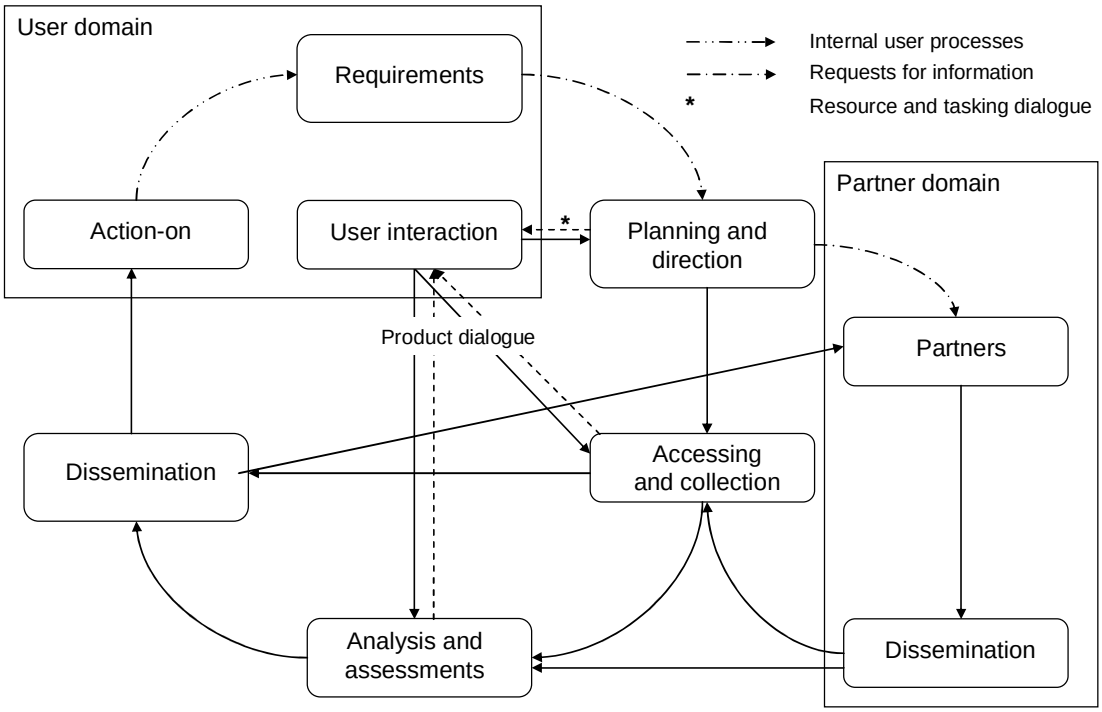

Figure 4: A modified intelligence cycle

The model depicts the partner as a user of intelligence in its own right, as well as being a source disseminating its own single-source and finished intelligence products. For this exchange to be meaningful both partners have to interpret information and intelligence in a similar way across cultural and language barriers, something that gives rise to a need for interpretation and wider cultural awareness. The model also visualizes the risk of intelligence flowing back via the

[7] Product is here understood in accordance with Abram N. Shulsky's rather wide definition: "The product of the intelligence process can be any means, from a formal report to a hurried conversation […]".(1993, p. 63)

partner into the production cycle from the dissemination steps, either directly to analysis and assessments or via the accessing and collection step as circular reporting.[8] This could be intentionally where the partner even fabricates or alters the original information in order to serve some selfish purposes, or it could be by chance. Lacking mechanisms for dealing with both these challenges will reduce the multinational force's ability for sharing intelligence with its partners.

3.3 How secrecy and information defences limit sharing

After determining how the host nation fits into the overall intelligence cycle and challenges related with that, it is now time to introduce the three focussing factors or lenses that constitute the sharing environment in this study; first *secrecy* and then *multinationality* and *ethics*. These will affect all intelligence cooperation, but could be exacerbated by special characteristics of the host nation, including the often immature and heterogeneous nature of its intelligence services and security forces.

Secrecy and the corresponding security arrangements are potentially the most limiting factor on a multinational force ability to share intelligence, something that makes it necessary to explore this phenomenon in some detail. Secrets are protected by formal security markings that differ from nation to nation, and these "labels" act as limiters both for the use of sensitive information and for its further distribution. For intelligence producers to willingly share their products the receiving party has to be; (1) sanctioned as a legitimate user in general and also of each specific product, indicating that they could receive it as long as; (2) the person(s) actually receiving the products are authorized for it; and (3) the organization they represent need the information in order to perform their duties or execute their missions. As a consequence of their personal security responsibilities, intelligence professionals will typically also on a more subjective basis consider the recipient's trustworthiness before sharing.

To sanction a new user and to approve the release of certain types of intelligence is a matter of policy, but how to implement the policy is a matter of procedure and processes as well as knowledge, education and real world experience. To determine what intelligence the new user or partner need to know is on the other hand based on judgement. A lack of formal authorization

[8] The problem of circular reporting in a multinational environment is highlighted by the United States Air Force: "Several times during Operations PROVIDE PROMISE and DENY FLIGHT, (US operations in Bosnia) information collected from US sources was passed to NATO officials, who later reported the information back into the US intelligence system. The same thing happened in reverse." (United States Air Force, 2007, p. 18)

should normally exclude the dissemination of intelligence while a lack of trust between individuals and organizations will hamper it, even if the intention is to share. The use of security markings, authorization procedures and the much debated need-to-know mantra will be examined further in theory. Only experience will however reveal if a partner properly safeguards and does not misuse the intelligence he is provided. This can be measured, but in practice it will be ascertained more by perceptions and suppositions of those involved in sharing.

3.3.1 Reasons for secrecy and protective security

In “Intelligence Power in Peace and War”, Herman (1996) opens with a passage on the history of “secret intelligence” were he points out that spies and informers providing sensitive information are as old as government itself. When later discussing characteristics of intelligence collection he states that “[it] seeks to penetrate what is denied to normal information gathering.” (p. 88). He follows up with highlighting three reasons for secrecy: (1) it adds value by opening possibilities because the target does not know what has been collected; (2) it conceals methods from possible peacetime doubts over legality and propriety; and most important (3) it protects the collection process and consequently single sources vulnerable to countermeasures. These reasons can be summarized as the requirement for protecting intelligence capacity, methods and sources, and some would also add intentions. The objective is to protect the future flow of information more than the content of already provided intelligence. Herman proposes that “secrecy’s effects run throughout the complete intelligence system and are its most distinctive feature.” (1996, p. 98).

There is little discussion about the needs for secrecy, and the concept of “secret intelligence” has broad academic support. When Jennifer E. Sims criticizes the American “propensity to equate intelligence with secrets […]” (2005, p. 38) as a dangerous cognitive block, she does not suggest that security should be relaxed – in many cases rather the opposite. What she asks for, along with other scholars, is a more active use of open sources in the intelligence production. In addition to increasing the information base, this would stimulate a necessary paradigm shift from a situation where intelligence users tend to emphasize and trust intelligence according to its security classification more than its contents and relevancy. The higher classification, the more important and interesting seems to be the mantra among practitioners and users still today. This is in itself an important discussion, however not part of the present research. Here it is sufficient to recognize that secrecy is ingrained in the intelligence community and expected by intelligence users. The concepts of secrecy and its guardian information security is honoured and rewarded throughout the intelligence universe.

Secrets are however not secrets for long without certain protection. This is why governments "erect information defences" (Herman, 1996, p. 165). Herman continues by identifying three different components of information security, where the first one; protective security[9] is most relevant for this study. Protective security include measures such as personnel vetting, control of contact with foreigners, access control to premises as well as rules for the classification, custody and transmission of documents – all serving a broad concept described as "need to know". Abram N. Shulsky claims that "in general, anyone controlling classified information is responsible for ascertaining a requester's need to know before providing the information." (1993, p. 113). In many countries this responsibility is covered by law. In Norway it is for instance a criminal offence punishable with up to one year in prison not to prevent the dissemination of classified information to unauthorized personnel (Security Act, 1998). Not surprisingly, the resulting fear of providing information to unauthorized users and bias towards protection seeps into the spine of intelligence professionals.

3.3.2 Sharing only with sanctioned users and the use of security markings

Before host nation organizations are entitled to receive intelligence they have to be sanctioned as legitimate users, something that is a policy question. Then each product has to be disclosed for their release, something that is subject to individual judgement and more of a procedural question. Intelligence producers contribute to this process by marking their products with the appropriate security classification and by advising what dissemination should be allowed. If we continue to use Norway and Norwegian law as example, section 11 of the Security Act (1998) establishes that "the person who issues or otherwise produces sensitive information shall ensure that the information is marked with the appropriate security classification. Security classification shall not be carried out to a greater extent than is strictly necessary, and the security classification used shall be no higher than necessary." It is further established that one of the following standards shall be used (translated from Norwegian): "TOP SECRET", "SECRET", "CONFIDENTIAL" or "RESTRICTED", and directions for their use are provided.

Not all countries adapt similar legislation or practices, but at least NATO nations adhere to the same basic principles. The U.S. system described by Shulsky (1993) is for instance very similar.

[9] There are several notions and definitions related to the concept of security. The Norwegian National Security Authority's (NSM, undated) description of *protective security* is for instance much wider than the one introduced by Herman and used in this study.

For the benefit of cooperation the security classification will be supplemented by amplifying directions for dissemination, such as e.g. “(originating country) SECRET - Releasable to NATO as NATO SECRET”. The complete security marking or parts thereof can be in the language of the originating country, or in English. Some producers will add supplementing directions, e.g. “this product is the property of (country or agency) – further release is (not authorized or authorized) to…”, and all will take it for granted that the shared information is not disseminated outside the predetermined countries or organizations without their explicit consent. There are, however, no universal standards for these markings and practices differ considerably between nations and agencies.

Working under a NATO umbrella this is different. Here nations have agreed to adhere to a common set of basic security regulations and standards coordinated and implemented by the NATO Office of Security (NATO, 2006). One of the Office’s responsibilities is to negotiate security arrangements with non-NATO countries that receive NATO classified information. Included in the mentioned standards are NATO approved security classifications, where the term “NATO” is a qualifier demanding that the information should be protected in accordance with NATO Security Policy (NATO, 2002). This signifies that a Force Commander working in the NATO chain of command is bound by NATO policy when handling NATO classified intelligence. He will in practice be given latitude for further dissemination of intelligence that is released to his command in the first place, including threat warnings and other time sensitive intelligence. The subtle nuances in how to treat intelligence marked with different types of security markings may be of superior importance for maintaining international trust, but they are very demanding for intelligence and security professionals alike.

Section 11 of the Norwegian Security Act (1998) also vaguely discusses the concept of international intelligence collaboration: “Provided that there is reciprocity, the King may make an agreement with a foreign state or international organization concerning the security classification of information received that is so classified by the state or international organization in question, and concerning the obligation to take steps to secure such information.” This alludes to the sensitivities involved in handling information received through international cooperation. Herman notes: “Those given access to sensitive intelligence by a foreign partner have to follow the partner’s rules to the letter.” (1996, p. 211). His point is underlined by Hans Born and Ian Leigh who state that (2005, p. 64):

> […] bilateral relations can only be maintained and continued if both parties fully and strictly respect the basic agreement underlying their intelligence sharing: that the origin and details of intelligence provided by the partner service will be protected according to its classification and will not be passed on to third parties.

Even stable relationships nourished by deep mutual trust are fragile and susceptible to immediate curtailment or even termination if mishandled. To understand how intelligence organizations work and how sharing is practiced it is vital to acknowledge these sensitivities as well as the personal responsibilities and legal accountabilities involved, often held by junior analysts with limited experience. Intelligence cooperation could even in the most benign of circumstances be described as difficult, and "security makes states think twice about international collaboration that involves sharing" (Herman, 1996, p. 192).

3.3.3 Sharing only with authorized personnel – vetting and security clearance

After establishing that the host nation is a sanctioned user and that a specific intelligence product is disclosed for their release, those involved in the dissemination process should ascertain that the receiving person(s) are actually vetted and authorized for that security classification. A lack of authorized host nation personnel will consequently limit the multinational force ability to share intelligence. In Norway, also these responsibilities are covered by law: "Any person who might gain access to sensitive information, shall receive authorization." (Changes to the Security Act, 2008). The purpose of authorization is to ensure that only personnel with a potential *need to know* get access to sensitive information. Further: "Any person receiving authorization for access to sensitive information shall in advance undergo security clearance [my translations from section 19]." Security clearance is a national responsibility and is granted through a formal vetting process, also labelled as screening (Shulsky, 1993). The main purpose of this process is to assure the vetted persons ability to keep secrets. In Norway this process entails (Security Act, 1998):

> […] vetting shall cover information in the possession of the clearance authority concerned and searching of relevant public registers […]. Vetting may also cover other sources, including statements from places where the person being vetted has served or worked, public authorities or references that have been provided or are supplementary.

The objective of vetting or screening is thus to exclude unfit personnel from gaining a security clearance. According to section 21 of the Security Act (1998), “security clearance shall only be given or maintained if there is *no reasonable doubt* [my italics] as to the suitability of the person concerned with respect to security.” Of specific matters to be assessed is: “Connection with domestic or foreign organizations which have illicit objectives, which may threaten the democratic social order or which consider violence or acts of terrorism to be acceptable means.” In NATO countries such vetting processes progress through established routines as everyday business, and in most other countries it would be possible for the government to establish ad-hoc routines to satisfy at least rudimentary immediate vetting needs. In so-called failed states or former failed states this, however, becomes more difficult. Public registers may be of limited value or even non-existent, and personal papers of any kind will typically be in short supply. In Afghanistan these difficulties are exacerbated by the fact that many persons only answer given names, and many have fled or moved extensively throughout more than three decades of upheavals and armed struggle. Loyalty could be hard to measure in a country were survival has become art.

3.3.4 The final obstacle: sharing only with those who need to know

The final security related obstacle for intelligence sharing is that the receiving party has to need the information in order to perform its duties or execute its missions. This “need to know” principle has over time manifested itself into a mantra that typically works against sharing. The principle has recently been under attack, but it has so far managed to resist a louder and louder call for “need to share”, even within a single country or intelligence community.

Much as the present Afghanistan conflict itself, the recent call for change of policy and procedures for intelligence sharing originates from the devastating 11 September 2001 bombings in the United States. The executive summary of the 9/11 Commission Report highlights: “The U.S. government has access to a vast amount of information. But it has a weak system for processing and using what it has. The system of "need to know" should be replaced by a system of "need to share."” (2004, p. 24). Jumping five years forward to the aftermath of the failed 2009 Christmas Day bombing commented above, Congresswoman Jane Harman made the following comment (2009, Dec 30):

> As an author of the 2004 Intelligence Reform Act, I have been saying for years that better information sharing is needed and turf cannot be jealously guarded. That Act set up a process to

> transition from a "*need to know*" to a "*need to share*" culture, but the Christmas bomb incident is evidence that we have much work to do.

The call for change originates from the United States, and was first and foremost a finger pointed at U.S. intelligence and law enforcement agencies dealing with homeland security. Lately it has however also emerged in the context of ongoing coalition operations. In Iraq, a former commander of Multi-National Force – Iraq (MNF-I), General David H. Petraeus through his Counterinsurgency Guidance directed: "Operate on a "need to share" rather than a "need to know" basis; disseminate intelligence as soon as possible to all who can benefit from it." (2008, p. 2). In Afghanistan, the present commander's similar guidance is even more explicit on the importance of interaction between the coalition and the host nation security forces: "Live and train together, plan and operate together. Share the same battle-rhythm and information. Integrate your command and control structures." (McChrystal & Hall, 2009, p. 5)

The real issue, all the way from 9/11 via Iraq to Afghanistan, may be to identify more exactly what friends and partners alike need to know – as a means to an end – rather than to replace it with a "need to share" culture that sounds more like an objective in its own right. Few would argue that intelligence capacity, methods and sources, as well as sensitive information, suddenly have lost their vulnerability or need for protection. Used as a means, a recognized need to know status does not remove the requirements for authorization or the preceding vetting filters, or any other security measures for that matter. The challenge is to come to workable solutions in an environment where partnering and enhancing the capacity of local security forces is required and mandatory, but where the security risks are as huge as the host nation's ability for proper vetting and authorization are neglectable. To force a more active identification of who need to know could function as the longed for eye-opener and driver for change among intelligence operators and custodians of information defences alike, and it is a familiar concept.

Another point is that it's hard to measure success or hold anyone accountable for a "need to share" policy. Intelligence professionals could always argue that they are sharing that which is possible within the security constrictions they work. It is further difficult to support a widely interpreted "need to share" policy from a security official's point of view. The task of getting host nation individuals vetted and authorized for receiving large amounts of intelligence could be insurmountable. The same goes for the partner's ability to securely hold and store such intelligence. Based on their operational achievements and feedback it is somewhat easier to

judge if they get what they need to know in order to succeed and maintain adequate force protection, both for themselves and for the coalition troops with whom they cooperate. The multinational forces' ability for intelligence sharing is thus to a certain extent dependent on a coherent recognition and judgement of what the host nation partners need to know in order to perform their duties or execute their missions.

3.4 The Multinational Force

The organization of a multinational force will affect its internal coherence in different ways and on different levels, including its ability for intelligence sharing. As established above, the research will focus on the multinational aspects of intelligence sharing to include the coherence and compatibility of policy, procedures and information systems between the different troop-contributing nations as well as on existing multilateral intelligence frameworks. In order to better understand the complex multinational dynamics, it is useful to separately examine each organizational level of the force, from the lowest tactical level to the force headquarters before discussing multilateral frameworks for intelligence cooperation.

Not all components of a multinational force are equally engaged in truly multinational operations. As will be discussed below, the local level is often characterized by nationally homogenous units that answer to their own peculiar policies and regulations as much as to the alliance or coalition headquarters. Such units engage bilaterally with the host nation and share intelligence in accordance with pragmatic national policies. This is not to imply that intelligence sharing is unproblematic on a bilateral level or even within a purely national context. In his thesis on American lessons from the Phoenix Program[10] during the Vietnam War, Lieutenant Colonel Ken Tovo comments (2005, p. 10) :

> […] while senior leaders synchronized objectives at the highest level, organizations might still be working at cross-purposes at lower levels. This was particularly true in the intelligence arena, where organizational rivalries often hindered intelligence sharing, as agencies treated their best sources and critical pieces of intelligence in a proprietary manner.

[10] Phoenix Program is the code name for a five year long U.S. attack on the Viet Cong Infrastructure (VCI) during the Vietnam War. VCI were clandestine operatives living within the South Vietnamese society and supporting the Viet Cong and North Vietnamese units in the field.

To understand how intelligence works in a multinational setting it is also important to recognize that most headquarters practice certain compartmentalization of analytical responsibilities. Some analysts have functional responsibilities; for instance for counter-narcotics or insurgency funding, and some have geographical responsibilities where they more holistically cover the situation within the operational boundaries of one or a few subordinate commands. The result is that individual analysts within a single staff section interact with, and depend on contributions from different intelligence collectors and nations. Often geographically oriented analysts in a superior headquarters are from the same nation(s) that make up the majority of the subordinate headquarters within the analyst's area of responsibility, but not always. Likewise, functionally oriented analysts are often from nations that take lead in, or put special emphasis on a specific problem area, but not always.

3.4.1 Forces in the field – coherent but geographically fragmented

Forces in the field that engage in partnered operations are typically nationally homogeneous, or they have embedded smaller detachments from one, or more rarely a few other nations. One result of this set-up is more bilaterally oriented intelligence relations with local host nation forces, something that falls outside this study to discuss. Even so, to appreciate the web of such bilateral relations is important to understand the complex dynamics of the sharing environment in a setting like Afghanistan. These tactical level units are typically organized in brigade or battalion sized task forces, each assigned a geographical area of responsibility that most often coincides with the host nation political boundaries. In counterinsurgency operations a common operational technique is to conduct so-called Combined Action between coalition and host nation forces where small detachments down to platoon or even squad level live among and provide security to the indigenous population (Joint Chiefs of Staff, 2009). Such units have modest intelligence staffs and also more locally defined information needs.

Some units, like Provincial Reconstruction Teams (PRT) in Afghanistan, focus as much on enhancing local governance and development as on the security line of operation (NATO, 2008). Consequently their intelligence needs are wider than appreciating hostile capacities and intentions.[11] A common denominator for all tactical level units is, however, that they are the ones most frequently placing soldiers at risk. Even if authority in the form of operational control is

[11] See for instance Peter Dahl Thruelsen's (2008, p. 37) recommendations for the S2 (intelligence) staff section of the ISAF deployed Danish Battlegroup embedded in Task Force Helmand of Regional Command South.

transferred to the commander of the multinational force, their sending nation will continue to have a vested interest in both their use and safety.

The combination of nationally homogenous units and explicit demands for force protection are precisely why intelligence sharing often becomes easier and sometimes also more unrestricted at this level. When partners team up for interdependent combat missions their success and survival rely on a common understanding of the battlefield. Intelligence sharing will therefore be handled bilaterally and in as pragmatic and practical a manner as possible within national rules and regulations, putting a premium on mission accomplishment as well as shorter and longer term force protection. But even at this level the key word is trust. Experiences from Vietnam (Tovo, 2005) proved that the South Vietnamese security forces were infiltrated by the Viet Cong at every level, leading to curtailment of combined operations and intelligence sharing.

Units in the field are typically supported by forward deployed national logistics, and by reach back systems for administration and information support with all communication conducted in their own mother tongue. These "support" channels secure strong national control over the utilization of force contributions, and the information systems and procedures reflect national policy and capacity also in the field of intelligence and security. In sum this makes up a web of what could be described as pragmatic national battlefield approaches supported by separate policies, capacities and information systems. On a higher organizational level this complex web meets with a universal command requirement for uniformity and transparency.[12]

3.4.2 Regional headquarters – less coherent but regionally more independent

Regional headquarters are as different as their lead nations, but they are all in the front line of facing the challenges ingrained in multinational intelligence sharing. Between units in the field and the higher level coalition headquarters, the modern post cold war intervention or peace-keeping force typically deploy multinational headquarters with regional responsibilities. These are commanded by a lead nation that normally also provides the lion share of troops and headquarters staff. In Afghanistan a total of five regional headquarters have been established; RC Capital on rotation between Turkey, France and Italy; RC North led by Germany; RC West by

[12] See also Angela Gendron's discussion of political sensitivities and national interests in the context of intelligence ethics in peace support operations (2006, pp. 168-169).

Italy; RC South, so far on rotation between Canada, the Netherlands and the United Kingdom; and finally RC East led by the United States.

In such fixed regional settings the incentives are strong for the lead nation to deploy and maintain solid intelligence support; both in the form of assets assigned to the multinational force and nationally controlled ones. This “lead nation layer” will place itself on top of the local web of national battlefield approaches described above, and it will reflect the inherent differences in capacity and policy between the lead nations. Because of the multinational manning of most regional headquarters the lead nation cannot or will typically not impose its own information systems on the staff, but they will run them in parallel. The recognized information systems will be those supplied by the lead nation or alliance, and the manning of the headquarters and its intelligence staff will be along the same lines as those described for the force headquarters below. The exception to this norm is where the region is led by the U.S. Their headquarters and subordinate regional forces tend to be more homogenous than others, and they are typically run on national American information systems.

This regional set-up that is based on a local web of bilaterally oriented relationships produces tangible geographical differences with respect to intelligence coverage and capacity. To some extent the force commander can counter this by apportionment of force level assets, but huge differences will remain. More relevant for this study, however, are the openings this regional set-up creates for differences in policy and practices related to intelligence sharing. The multinational force and the emerging host nation security forces therefore have to expect and adapt to quite extensive regional and local differences.

3.4.3 Force headquarters – as coherent as its framework

It is the commander of the multinational force who, within certain limitations, determines policy for intelligence sharing, and it is his headquarters that promulgate procedures, processes and facilitating mechanisms for such sharing. High level coalition headquarters in the NATO chain of command are truly multinational, manned and led by staff and high ranking officers from different nations on rotation. How, and by what system this rotation is managed differs from case to case, and also over time. In ISAF the commander and some of his key officers has now been permanently assigned to the nation with most “boots on the ground” – the United States. The other participating nations will, however, make sure that they are represented with both leaders and staff commensurable with their national contributions. This is in theory also the case for

intelligence professionals. However, with only a few exceptions all intelligence positions have up to now been manned by NATO nations. The reason for this is that the main information systems have been supplied by NATO, and these are authorized for NATO access only. In coalition operations outside NATO the information systems will typically be supplied by the lead nation, and the intelligence staffs will emanate from the same – or in the case of Anglo-Saxon led operations, from one of the "five-eye" countries (see paragraph 3.4.4 below) authorized to access specific domains of those systems.

For intelligence collection and analytical support the force headquarters to a large extent depend on reach back to the participating nations, and in the case of NATO operations also to the NATO chain of command. For this reason and purpose, many of the nations will be represented on or near the headquarters compound by a National Intelligence Cell (Joint Chiefs of Staff, 2004, p. IV20). How this greater in-theatre intelligence community functions, and how nations engage and support the multinational force will influence the headquarters' ability to produce relevant, timely and reliable products and to cooperate effectively with any third party, including the host nation. An environment distinguished by differences in national policies, regulations and caveats will induce doubts and restraints in the minds of intelligence producers, something that would impact negatively on both the timeliness of reports and on information security. Even those smaller states that Gendron denotes as "free riders" and that in her words contribute "very little if anything to its [the peace alliance] effectiveness" can help overcome some of these hurdles by displaying positive sentiments and forming "regional coalitions in which intelligence is freely shared […]" (Gendron, 2006, p. 171).

In NATO led operations there are multitudes of information systems at work, especially at the force level, but also at regional levels. National Intelligence Cells utilize their own systems with air-gaps or firewalls[13] to the multinational systems. Intelligence collectors operate on highly sensitive national or NATO systems with air-gaps or firewalls between them, and with air-gaps to the less sensitive systems that analysts use in their work. Analysts on their side can use either "NATO secret" or specific "mission secret" systems with firewalls between them, while many Americans in addition will depend heavily on their national SIPRNET (Secret Internet Protocol Router Network) with air-gaps to NATO systems. As discussed above, all these systems require

[13] Air-gaps between information systems indicate that the systems are physically separated and that data has to be transferred manually between them. A separation by firewall on the other hand indicates that the systems are connected, and that they are able to exchange data pending the right "keys" to the firewall.

different authorization and seen together they will display a huge variety of security markings – both officially sanctioned and some more pragmatic and context dependent. This layout necessarily complicates the production of releasable products and it arguably represents one of the biggest obstacles for intelligence sharing.

3.4.4 Multilateral frameworks for intelligence cooperation

As intelligence cooperation between states is typically executed bilaterally, there are few real multilateral frameworks or "intelligence clubs" in existence. However, one such transnational club dates back to the Second World War and traces its origins from the close intelligence cooperation between the five English speaking allies U.S., UK, Australia, Canada and New Zealand (Born & Leigh, 2005). From this relationship developed what Herman (1996) describes as the "UK-US (and Old Commonwealth)" model based on the intelligence community with separate collection and analysis agencies, departmental defence intelligence and some sort of community assessments forming "a national *system*; […] to be managed as a national resource" (Herman, 1996, p. 27). The similarities are thus bigger than the differences between the five Anglo-Saxon countries that are included in this framework.

This successful wartime cooperation became permanent with especially signals intelligence integrated to the point of common manning and analysis. The relationship is further underpinned by "[…] comparable national security practices supplemented by special agreements for the handling of intelligence; *these include formal limitations on what can be passed outside the UK-US-Commonwealth circle* [my italics]" (Herman, 1996, pp. 210-211). This "five-eye" community obviously simplifies intelligence cooperation between the designated nations, and could in theory help to facilitate sharing also with other partners, including the host nation. The reverse effect is that it brings about a sense of class division among coalition members of being "inside" or left "outside", something that does not enhance cooperation and sharing.

The other multilateral intelligence framework worth mentioning is composed of the NATO alliance itself. Over the last 60 odd years it has developed to a mature and proven undertaking, with some probably arguing fixed and inflexible bureaucracy. The NATO framework does not employ much in the form of organic collection assets, and is therefore mostly based on its ability

to receive, handle and share large amounts of national intelligence outputs. With regards to security, Herman notes (1996, p. 364):

> The NATO system included multinational intelligence staffs, but always had the insoluble problem of protecting fragile intelligence sources in a multinational environment. […] nations judged their most important national intelligence to be too sensitive to be put into NATO in this 'official' way.

Also this framework leaves some "inside" and others "outside", something that was briefly discussed above with the composition of the force headquarters and manning of the intelligence staff. For practical purposes this implies that the intelligence community of multinational forces is divided into four ascending "access levels"; first the grand coalition with all troop contributing nations; then the NATO members; then the "five-eye" community or derivates thereof; and finally the national level with established or ad-hoc bilateral relations. Add then the host nation, and these five levels could be described as the multinational variant of Sir David Omand's "concentric circles of trust" (2007, pp. 120-122). The wider coalition community is supported by a "mission secret" information system, NATO members by a "NATO secret" system, and the five-eye community by access to shareable domains of national systems – all utilizing the English language. Finally, each individual nation is supported by national systems in their own mother tongue. So far, dissemination of intelligence to the outermost fifth circle or host nation has been "air-gapped" to them in the form of documents or, more frequently, through verbal communication.

Even during the Cold War when the alliance was much smaller than today and its member nations perceived an existential threat, intelligence exchange was hampered by a lack of trust in the wider NATO community's ability to keep secrets. In today's environment, with interventions and peace-keeping coalition operations in so-called failed states, the action is further away from home and most nations feel less existentially threatened. This could lead both ways with regards to their readiness for intelligence sharing. Some could be willing to take more risks; including sharing with the host nation, while others could, at least initially, draw the opposite conclusion. To operate with up to five concentric circles of trust that is built on a web of pragmatic national battlefield approaches and separate information systems is by its sheer complexity counteracting the very idea of intelligence sharing.

3.5 Intelligence ethics

When Angela Gendron discuss intelligence ethics in peace support operations, she comments that “a state’s failure to share relevant and timely intelligence is ethically indefensible unless there are strong grounds for supposing that the negative affects to the state or its allies outweigh the benefits.” (2006, p. 170). Her remarks may be pointed towards the internal intelligence sharing within peacekeeping forces, but they must be equally justified in situations where the fulfilment of a UN mandate demands sharing also with the host nation. She continues: “Classifying and continuing to review intelligence with the object of facilitating sharing may be a resource-intensive and complex procedure for organizations, but it is one which is necessary if it is to fulfil its international obligations.” (p. 170)

These comments must be seen in context with her remarks that some members of the force may anyway decide to withhold intelligence for their own national reasons, because they are restricted by third party rules or concerned that their information could be misused or not properly protected. One such third party rule could be that the intelligence in question has been based on bilaterally received information, something that precludes further dissemination without the originator’s consent. Examples of misuse could be that the intelligence is used to enhance the standing of one of the factions in internal host nation power struggles, or simply for tipping off criminals. As discussed above, the protection of sensitive information is neither simple nor clear cut even in a developed country with a mature security regime. The reasons for encouraging restrictive sharing policies are therefore valid and the risks taken by more liberal practices have ethical aspects and dilemmas of their own.

Gendron’s comments raises at least two moral dilemmas for those multinational staff workers that are engaged in the production of releasable intelligence: (1) what to do in situations where they judge that the intelligence on hand for different reasons should be released to the host nation, but where the source has classified it in a way that prohibits its release; and (2) how much they should let their own perceptions of the receiving party’s trustworthiness influence their intelligence sharing practices. Based on earlier discussions the textbook answer to the first question is to withhold such intelligence until the source has been consulted, and to the second as a minimum to make sure that the recipients “need to know” and that they have been authorized for the classification level they receive.

In a hectic operational environment where commanders and staffs necessarily have to apply some measure of pragmatic realism against both shorter and longer term objectives, both these answers could, however, prove insurmountable requirements. Gendron notes that (2006, p. 170):

> […] sharing often takes place in spite of the rules rather than because of them. Users in the field may resort to ad hoc creative and discretionary measures to compensate for the lack of formal arrangements or to circumvent rules that are seen as too restrictive.

There are also other ethical aspects of intelligence and intelligence sharing. In their timely work on oversight of security and intelligence services, Born and Leigh discuss how a professional code of ethics may help practitioners to "perform the respective jobs in a just and morally satisfactory manner" (2005, p. 47). They continue:

> To devise a professional code of ethics, and to offer training courses for intelligence staffers, is a useful means to set, communicate and maintain a minimum level of shared practices among intelligence employees.

To my knowledge none of the post cold war multinational peace support operations has codified intelligence ethics as part of their Standard Operating Procedures. However, it may be that a simple code and associated training classes could help overcome some of the limitations on multinational forces ability to share intelligence with the host nation. Another discussion in their chapter on International Cooperation concerns cooperation with foreign intelligence services in relation to human rights and especially torture (Born & Leigh, 2005, pp. 64-67). Agreeable to the fact that international law does not discuss the use of information obtained by a partner state's security services through torture, they anyway argue that it ought to be forbidden. A question or dilemma that might materialize for analysts about to share intelligence is thus whether that piece of information could lead to somebody being captured and then tortured. However important such ethical considerations are, many would argue that they should not impact on decisions to share intelligence. Arguably the Security Sector Reform with its education and training programmes and similar initiatives are better suited mechanisms for promoting basic human rights.

4 Recognized challenges for sharing

The purpose of this chapter is to identify what ISAF intelligence officers recognize as hurdles for intelligence sharing with the ANSF, including how they understand the force's policy and how they practice such sharing. In order to explain the context the chapter will, however, open with a short review of recent high-level developments in ISAF, to include: (1) how its command structure and partner integration has evolved; and (2) ISAF headquarters recent history for intelligence collaboration with the ANSF. Conforming to a long established practice never to reveal the identity of serving intelligence officers, both the name and rank of the interviewed officers cited throughout this chapter have been substituted with aliases. Capt. Anderson, Capt. Brown and Capt. Clark from IJC as well as Capt. Davis and Capt. Evans from RC (N) are all experienced professionals with a profound knowledge and understanding of ISAF partnering and sharing efforts.

4.1 Recent developments within the ISAF command structure and partner integration

Upon arrival in Kabul early February 2010 it became clear that the top echelons of ISAF had undergone dramatic changes since my departure in June 2009. The former ISAF headquarters in downtown Kabul had over a span of just a few months split in two, leaving a "four star" Commander ISAF headquarters at its old premises and a new "three star" headquarters at Kabul International Airport. Responsibilities are divided between them with the four star headquarters led by COMISAF, General Stanley A. McChrystal, handling strategic political-military aspects of the ISAF mission while the three star headquarters – ISAF Joint Command (IJC) – led by Lieutenant General David M. Rodriguez is running day-to-day military operations through the regional commands and Provincial Reconstruction Teams (NATO, 2009a). Also high level partnering has evolved with Afghan liaison officers from the three main branches of their security forces; the National Directorate of Security (NDS) charged with intelligence and security; the Afghan National Police (ANP); and the Afghan National Army (ANA) now permanently embedded in IJC and seated in the Combined Joint Operations Centre – an area where classified information is discussed and displayed on a continuous basis.

ISAF's higher level intelligence echelons have undergone intellectual developments that are no less dramatic. From quite recently being enemy-centric the efforts are now brought in line with the latest counterinsurgency thinking (McChrystal & Hall, 2009), focussing on understanding the Afghan society and its people. One effect of this change is that open and other non-sensitive sources of information have gained increased significance in the overall intelligence effort. Even

the name-change of the all-source intelligence shop in IJC from the traditional “Joint Intelligence Centre” (JIC) to “Information Dominance Centre” (IDC) bears witness to this mental development. Embedded in this centre’s cross-functional teams are personnel monitoring development and governance in addition to analysts looking at the more traditional security issues. Overall, IJC seems to favour the term information over intelligence as it better describes the needs of counterinsurgency operations, and because it is judged to simplify partnering and sharing (IJC, 2010). The intentions and directions of Major General Flynn (2010) are obviously taking hold.

Continual partnering is also establishing itself within intelligence circles. The fact that ANSF will be permanently represented by a liaison officer from the National Directorate of Security in the Information Dominance Centre is earth shattering for a multinational command bound by rigid NATO security regulations. What can easily burn itself into the mind of someone with former experience from NATO headquarters and multinational operations is the mental picture of a senior Afghan police intelligence officer that is meeting with a non-American analyst under a 40 inch plasma screen displaying the SIPRNET screensaver. This is not to suggest a lenient or senseless treatment of sensitivities, but the Americans are leading the way – and they are serious. In this pragmatic euphoria of change and partnership it is tempting to call to mind those basic purposes of protective security; the protection of capacity, methods and sources (and some would add intentions). Not all information can or should be shared.

At the time of data collection in February 2010, there were advanced plans for embedding ANSF officers also in the Combined Joint Operations Centre of RC (N), but there were no immediate plans for ANSF representation on the intelligence staff. Collaboration between partners was still conducted through liaison arrangements involving different sections and officers of the Regional Command with respective Afghan counterparts. The Provost Marshal kept in contact with the ANP, the HUMINT community with the NDS and the intelligence leadership itself with the ANA. RC (N) also kept a traditional organizational model for the intelligence staff, focussing mainly on the opposing insurgency forces. The command had, however, recently established a new staff element in the form of a multinational Intelligence Fusion Centre employing many of the same cross functions as IJC’s Information Dominance Centre. In many ways RC (N) seemed to be a small organizational step or two behind the Kabul developments, but in some areas at least catching up and preparing for more continuous partnering and sharing. It is fair to say that in February 2010 the higher command level was progressing steadily from a “we and them”

perspective to “us” and that the regional command was about to leave the starting block on the same journey.

4.2 ISAF headquarters history of intelligence collaboration with the ANSF

Partnering between ISAF HQ and its opposite ANSF headquarters is nothing new.[14] Also under the former Commander ISAF, General David D. McKiernan, this effort was seen as vital for meeting the mandate, and as condition for the exit strategy. Staff sections and individuals were encouraged to partner to the fullest extent possible, and had to keep meticulous records of all their ANSF interactions. A number of regular venues for reciprocal sharing of intelligence and information were also established, and some leaders and staff officers from both sides grew to know each other quite well. As long as people did not work together on a regular basis or had access to common information and communication systems there were, however, limits to how far this type of partnership could be stretched. In fact, it turned out to be harder than expected to get people and staff together on a scale that would make a noticeable difference. Something more had to be done in order to get partnering and cooperation on the right track.

It was therefore decided to station ISAF liaison officers within ANSF headquarters operation centres and in 2008 also to establish a common office space within the confines of the Afghan National Military Coordination Centre in Kabul for planning purposes. This entity was known by several names, but the most common was “Joint Planning Operation Centre (JPOC)”. The building itself was financed by American money, and it was fitted out with a combination of NATO and American sponsored equipment. The centre was permanently manned by ANSF planners, and it had separate office spaces with access to classified systems for ISAF planners working there on a semi-permanent basis. The JPOC building was certified to NATO security standards in 2009 and a handful of the Afghan officers working there were subject to vetting for proper ISAF security clearances and future authorization for access to classified ISAF areas and information. However, due to the lack of public records and other difficulties with establishing their past, this turned out to be a long-lasting process.

The problem with especially the ISAF part of the JPOC during the first year or so was that it almost developed into a “state within the state” with its separate agenda working around and

[14] This short historic account has been established through conversations with two intelligence officers that were central in the partnering process under general McKiernan and also in standing up the Joint Planning Operation Centre (JPOC).

outside of the normal ISAF staff, and sometimes keeping them in the blind. Their relationship with the Afghans developed impeccably throughout, but with a tendency to separate the two partner staffs instead of bringing them closer together. The reasons could be many, possibly including a sense or relief within the core ISAF staff that partnering was now firmly taken off their shoulders and borne by the overwhelmed JPOC staff. Consequently, the intended "jump-start" only worked for those inside, and they were fairly overworked already. Then, in June 2009 General Stanley A. McChrystal and his team turned up, adding a new momentum to the partnering efforts.

4.3 Communication and the use of interpreters

The first findings of this research relate to communication challenges. Very few if any of the analysts in either IJC or RC (N) speak Dari or Pashtu, and their ANSF partners' command of English is not much better. The use of interpreters is thus unavoidable. To translate a text or verbal communication is in itself difficult. The literal meaning of certain words and phrases differ in different languages and cultures, and poor interpretation could twist both the literal content and the intended message of an intelligence product. When Capt. Brown looks at information provided by Afghans, he occasionally finds that "whenever you look at it in English it really doesn't make much sense. So I'm assuming similarly going back into Dari." As in all human interaction and maybe more so in armed conflict and counterinsurgency operations where public perceptions are imperative, the consequences of poor translation and interpretation could be grave. Since "the ultimate object of intelligence is to enable action to be optimized by reducing ignorance" (Omand, 2007, p. 99), the consequences could be haphazard at best and even lethal at worst. Capt. Anderson is clear when he comments the use of interpreters:

> No, that's probably the weakest link we have right now. Because we depend on translators translating our intelligence into Dari, so depending on the skillset of the translator, he could actually get the right meaning, or the wrong meaning.

He then follows up with a couple of examples from his own experience. The first one is about the differences between mines and Improvised Explosive Devices (IEDs):

> We used to think that the Afghans didn't differentiate between mines and IEDs – [that] they call them all mines. That's not true, except the interpreter can't pick up on the difference or just the other word the Afghans are using when they defer to mines.

In a situation where IEDs are the number one killer of coalition soldiers this difference is not trivial. The other example could at first seem almost humorous, but that is only until one realizes how extremely delicate any interaction with Afghan women are:

> The English word is metal detector […] the Dari word they use is wooden baton. So the actual paragraph said: ISAF and ANSF forces will search females with a wooden baton. Obviously that doesn't work.

Both these examples are from the translation of documents, but also the use of interpreters during meetings has its challenges. After observing a couple of meetings between Afghan and ISAF partners it is clear that the use of interpreters has not been properly rehearsed, either by Afghans or by the multinational staff. The challenge is even bigger for those with English as a second language. Sentences and statements become too long and complicated and they cover too many topics before the "terps" get a chance to translate. Many also keep eye-contact with the interpreters rather than their partners making the atmosphere less personal than could otherwise have been possible. Except for this, the meetings were held in a positive and friendly tone.

4.4 The problem of circular reporting

The danger of circular reporting is something that troubles intelligence professionals in their quest for corroboration of developing intelligence products. Lacking or inadequate mechanisms for precluding such inputs from the intelligence cycle therefore complicates production and, because of the resource drain on analysts, it also limits the appetite for intelligence sharing. The problem with circular reporting and information screening is considerable in ISAF even before the host nation makes its entrance into the intelligence cycle (Sterzer, McDuff, & Flasz, 2008):

> Circular reporting will always be an issue in the intelligence function. One single event can and will be reported in a dozen different products […] and then re-reported yet again in the near future. Furthermore, because there are few standardized products and templates for modern counter-insurgency (COIN) agreed upon by all the nations contributing to ISAF, some organizations omit to put the source of the information whereas others rewrite the information itself (occasionally with mistakes or changes). For an analyst, this is a major problem to say the least. The screening process of the information as well as its analysis requires an immense amount of focus and crosschecking, taking time that could be better spent on more vital tasks.

A single-source piece of information or intelligence could be extremely valuable, but most of the time it has to be confirmed by other sources before a commander is willing or procedurally able to take action, especially if there is a danger for collateral damage. In a setting like Afghanistan the concepts of corroboration, confirmation and circular reporting is probably best explained through the use of artificial, but illustrative local examples. The first could be described as “ideal world – by the book”:

A few hours ago a human intelligence team from ISAF received a tip-off from a friendly source mentioning a new large-bore machine gun being installed on the roof of an abandoned building close to a village road sometimes used by ISAF and ANSF convoys. The team made their report and passed it up chain. Finally, it reaches the intelligence centre that judges it not to be very time sensitive, but anyhow starts the process for confirmation by cueing other collection assets. Imagery comes back with a clear picture of an old 20mm anti-aircraft artillery piece, and signal collectors report new and weapons-related insurgency transmissions in that cross-bearing. The initial report is now corroborated by three different sources, and everything is collated and assessed into a finished (and thus confirmed) intelligence product. The next stop for this piece of intelligence is the Joint Targeting Working Group, and after a thorough targeting process precluding the presence of civilians, a laser guided bomb destroys the gun without causing collateral damage or civilian casualties. That’s in the perfect world.

The second artificial example is illustrative of a situation where the analyst’s job becomes more difficult because of circular reporting:

Local citizen A has for years seen himself as the rightful heir to the job as police chief in district X, but was for political reasons passed over by distant citizen B. Citizen A has never come to terms with either citizen B or the sub-tribe he represents, and is looking for a way to get rid of him. The opportunity presents itself during a local meeting between Afghan security officials and ISAF. He accuses the absent police chief of being corrupt, and supports it with a plausible explanation. Both ISAF and Afghan officials take notes and walk away. The ISAF representative compiles his report to the regional command and sporadically mentions the incident. One of the Afghan officials decides to do some superficial investigation on his own, and happy with the results he distributes his report up the chain. One week later, in a regional meeting, an Afghan representative hands over to ISAF a report about a corrupt police chief in district X. An ISAF

analyst runs a database query and pulls out the week old report. Is this the corroboration he needs to confirm corruption? Maybe not, but the regional command anyway decide to include a short assessment of the two reports in their daily regional intelligence summary. Then the same happens again at the next higher level. The original, in this case fake report has been given a new spin at each level by both partners as it criss-crosses its way up the chain, and only a thorough criminal investigation can now confirm or deny what in the end looks like confirmed intelligence.

Even though the interviews and conversations missed to identify circular reporting as a major obstacle for sharing, Capt. Clark alluded to it when he stated:

> We have a good environment for information sharing right now. But it is not entirely coordinated. […] So, person A in ISAF may feed information or may share information with an official in GIRoA who in turn shares that information back to person B in ISAF as if it is information that belongs to the Government of Afghanistan.

Similar concerns are vaguely expressed by the intelligence leadership in RC (N). Looking at the problem from a slightly different perspective they sometimes uncover that the same basic information or intelligence trickles into their system from different host nation organizations, and that some of it also has what they describe as a bit too "sensational" or inventive twist – perhaps pointing to a certain unhealthy competition between them for attention. It does not take much spin on information to make it hard for analysts to preclude circular reporting. Capt. Brown comments that in order to reduce this problem you need to look carefully for similarities, keep open communication with the originator and meticulously source all reports: "But is it something that will happen? No doubt about it. I think it will happen […] a lot of times." In the extreme, false information could be used by competing Afghan factions to play the international force. Inventive modes of circular reporting would in that case be used proactively to convince both Afghan and ISAF intelligence staffs that they have got enough corroboration to conduct conclusive assessments that in turn could lead to indiscriminate action. In a worst case scenario this could lead to the targeting and killing of innocent civilians.

4.5 The burden of secrecy and related security concerns

When asked to elaborate on ISAF policy for sharing the three IJC officers seem quite confident, at least about the general gist of it. Capt. Anderson empathically responds "write-to-release",

indicating that analysts should concentrate on making releasable products. The two others open with describing what classification level the Afghans *could* receive and by what methods the dissemination may be executed. All three demonstrate a strong support for partnership and intelligence sharing and believe this is the way forward. Capt. Clark emphasizes that ISAF has come a long way in this direction only during his short stay. They, along with other intelligence analysts in the Information Dominance Centre, however become more uncertain when later asked if they had seen the actual paperwork, or where to find details about procedures and processes. When asking Capt. Davies of RC (N) the same general question he opens with stating that "the policy is given by IJC in respective FRAGOs [fragmentation orders]", which is objectively correct but that on the other hand could indicate a more distanced position to the challenge.

Capt. Anderson's immediate concern is what type of vetting process the Afghan recipients of ISAF intelligence have been subjected to: "There was never a […] supporting document that explained to the analyst how the ANSF staff were vetted." His point goes straight to the heart of protective security where the holder of intelligence has certain responsibilities with regards to its dissemination. In his mind the Afghan authorities have been introduced to security formalities like vetting processes and "need to know" policies, but all three officers are ignorant about how the Afghans execute these procedures. Consequently the analysts do not know if their opposite ANSF numbers are properly vetted and authorized to receive the information they are presented, and have to take it for granted that they are. It later turns out that ISAF and Afghan authorities are addressing the vetting problem with adaptive procedures fitting to the local context. At least all the Afghan officers that are embedded in ISAF headquarters have undergone such screening and are authorized.

When discussing release authority the three IJC officers agree that ISAF may release information and intelligence up to the ISAF SECRET level to the Government of the Islamic Republic of Afghanistan (GIRoA), and that there are three forms of dissemination: document release which means handing over a document in English or translated to Dari; information display where the information is visualized for the partners during a meeting, but with no copies handed out; and verbally during partner meetings and discussions. The two last methods turn out to be the officially preferred ISAF way of sharing. In Capt. Brown's words: "you can show them some intelligence things back and forth but most of the time it is through verbal communication." His

remark is also valid for RC (N), were most of the sharing is done through verbal communication. Sharing of documents is more infrequent and usually kept at a lower classification level.

During follow-up conversations it is established that releasable documents have to be marked in a special way: "NATO/ISAF [Security classification] REL GIRoA" or "NATO/ISAF [Security classification] FOR DISPLAY ONLY GIRoA", and that they have to be disseminated through the Theatre or a Unit Disclosure Officer[15] for review and recording. To follow these instructions is, however, a problem for RC (N) as they do not have this function manned. Capt. Davies laconically confesses: "So we face a problem, concerning that. So there is no basic, no routine exchange of written products, so far". A quick query of the main NATO database for finished intelligence products reveal that less than 1% of the archived ISAF related documents from 2009 carry these classification markings. Even if the percentage could be expected to increase somewhat in line with the higher emphasis on sharing, it underscores that most intelligence collaboration is done verbally.

Capt. Anderson accentuates the problem with security markings when he states: "There are no such things as "ISAF SECRET Releasable to GIRoA", indicating that such a marking has been in use, but that it is not an authorized security classification (as a matter of fact, it lacks the word NATO). This exemplifies the confusion that surrounds classification markings and caveats. It could sound like nugatory semantics, but it represents real uncertainty and frustration amongst analysts on how to extract and make use of intelligence protected by a multitude of different security markings for their partnering and sharing purposes. This frustration leads one of the survey respondents to demand: "Ensure proper markings and information is used within the markings." Capt. Anderson continues: "So you have to write your own product and try to figure out what is classified and needs to be protected, and what isn't or doesn't and draft your document like that – and you can share it." This points a finger to those that do not follow NATO (and ISAF) standards, including classifying documents paragraph by paragraph and indicating what can be released.

Another problem related to security classifications and sharing is highlighted in two survey comments, one of them emphasizing that "over classification tends to inhibit information sharing." This alludes to a known tendency amongst intelligence producers to tilt against over-

[15] These functions are tasked with supervising and controlling the dissemination of classified information and intelligence outside the alliance or coalition community.

classifying their products, be it for uncertainty, to make sure it has got enough protection, because of laziness or just to secure attention from the users. Classification markings are not only used for protecting sensitive information, but as Herman notes (1996) also for enhancing intelligence influence and as “departments’ badges and means of protecting and extending their territory.” (p. 93). Capt. Clark, however, observes a positive trend in ISAF where classifications are pushed down to the lowest level possible in order to facilitate sharing.

An illustrative example of the confusion caused by security markings can be found in the NATO classified e-mail system. When starting a new e-mail the user is challenged to choose a security classification with releasability annotations from a pull-down menu of standard and officially sanctioned labels. This list is growing longer as NATO engages in new operations and with more official partners, like e.g. SFOR, KFOR, ISAF and the Partnership for Peace or Mediterranean Dialogue programs. The classification markings are then used as keys to the firewalls against other information systems. However, in February 2010 there were still no labels annotating releasability from NATO or ISAF to the host nation; GIRoA or ANSF. Even if this has had marginal practical consequences so far, it adds to the uncertainty and frustration of analysts.

When discussing the problem of classification markings with other staff, and after searching the systems, it turns out that ISAF HQ has produced extensive documentation on both policy and procedures for how to share intelligence and information, most of it dated throughout the second half of 2009. Amongst these documents are classification guides and SOPs for information release and cooperation as well as clarifications on authority for sharing. The problem may be that people are overwhelmed and that theory to a certain extent is counteracted by the different but anyhow legitimate practices in use. A person using three different information systems soon finds that he has to adhere to three different standards for security markings, and he will receive even more from troop contributing nations that comply with their own national standards. A simple task that in a hectic operational environment should have been undemanding could soon turn into protracted detective work with continued negotiations between analysts and those contributing the intelligence. When discussing bottlenecks for sharing Capt. Brown suggests that: “It’s [the whole process] just time consuming. I think that is probably the biggest constraint”. In his mind uncertainty can spur analysts to turn to what they know best – their own national markings and caveats.

Capt. Anderson's statement on how he produces his releasable products must not be interpreted in a way to suggest that analysts are ignorant of security or moral dilemmas; they are not. They understand all too well the requirement for protecting intelligence capacity, methods and sources. They also acknowledge the overriding principle that release of classified information is subject to consent by the originator. A consequence of all this is that some analysts find it easier to write their own releasable products bottom up, and keep them on an unclassified level. Anderson continues: "That really means you are writing an unclassified document." This takes time, and it could hinder the sharing of critical information. Capt. Clark also alludes to this when he suggests: "If analysts don't know what they can bring to the table, then I think they are more reluctant to bring anything".

When asked about major security concerns and related bottlenecks for sharing most of the officers highlight dismal Afghan security standards. Capt. Davies laconically summarizes this as "the holes in the ANSF where information is melting away." Capt. Clark's tone is more diplomatic when he judges that "you can never be 100 percent sure that what you are giving to a government official will not end up in a place where it was not intended to be." Capt. Anderson on his side delivers a straight shot: "If I have a product in my hand, and I get to the Afghans there is zero degree of certainty that it is going to be safeguarded and kept", and further: "The safeguards aren't in place with GIRoA." This is backed up by survey comments mentioning experiences of leaks where insurgents have been able to prevent or more effectively counter ISAF operations.

What worries analysts most is apparently a different Afghan tradition and culture for handling of sensitive information as much as deliberate leaks. The examples they mention are leaving documents in places for others to view or grab and also uncontrolled access to meeting rooms. Capt. Clark exemplifies the last point: "You don't know what he [the servant] is overhearing […]". He continues with mentioning a more traditional security risk: "Third party intelligence services may be active within the country." These worries will not surprise anyone, and they are most certainly calculated into the risk of enhanced sharing and partnership. Partnership and information sharing are so vital for the counterinsurgency strategy that the generals are willing to accept much risk.

4.6 Multinationality and ISAF coherence

Some of the more important restraints for intelligence sharing that stem from multinationality have already been discussed under the secrecy factor above. The multitude of different information systems and associated security markings produce insecurity among intelligence professionals tasked with partnering and sharing. The preferred system in Afghanistan is the mission specific "ISAF secret" system, but the problem with that in Capt Anderson's mind is that there are not "a lot of ISAF secret terminals in the United States, or in Norway or in Britain or wherever." That means that intelligence reach back to the force contributing capitals, either directly, or more commonly through the National Intelligence Cells have to go via national systems, either through firewalls or manually air-gapped. This form of communication counteracts both timeliness and relevance of intelligence in a fluid operational environment. It also contributes to the effect of writing on a higher than necessary classification level because reach back analysts tends to use national classification markings without thought for the wider in-theatre sharing needs. Capt. Davies feels that this side-effect of traditional intelligence stovepiping best can be overcome if "everybody is working on one system, and ISAF secret is the system which has to be used".

The security markings that each nation applies to its intelligence products mirror national caveats and differences that contribute to the complicated web of dos and don'ts for tested intelligence professionals. Capt. Anderson cites one of the more extreme variants of these caveats that have been presented to him personally: "We will not release anything to Afghanistan." The discussion of national caveats is in itself sensitive, and to go into details or comment on specific nations is not possible in an open study. When pushed a bit, many of the analysts however acknowledge that there are big differences between the nations on how they look upon and practice sharing. As one survey comment puts it: "National level intel agencies do not share intelligence effectively. These nations do not write most of their finished intelligence production for sharing with ISAF and rarely if ever GIRoA." Such caveats and differences manifest themselves already at the lowest tactical level where some of the Provincial Reconstruction Teams in Capt. Anderson's mind are "prevented from getting a close working relationship with say their ANP or ANA partner". The resulting differences then reflect on the regional commands where according to Capt. Brown, some of them "are a lot better at sharing information than others." Such observations are supported by earlier findings (Bowman & Dale, 2009, p. 17):

> An additional challenge is information flow among ISAF participants. […] Constraints on information flow may include the use of different—national and NATO—communications channels, linguistic barriers, and some reluctance on the part of some countries to share information perceived to be especially sensitive.

Another sensitive issue is created by the multilateral intelligence frameworks and "concentric circles of trust" that are presented in chapter 3. Those staff members that come from a non-NATO country (but still ISAF troop contributing nation) will not even be allowed into many of the intelligence staff's workplaces. They simply lack the authorization to work in an environment where higher classified systems like the "NATO secret" system are present. Also NATO members outside the Anglo-Saxon "five-eye" community (or derivates thereof) are restricted from accessing certain areas, and on the top are national facilities and bilateral sharing arrangements. The fact that the overall intelligence capacity increases dramatically the closer to the centre the analyst finds himself does not help to alleviate mistrust and the feeling of being "inside" or left "outside". Capt. Davies goes as far as he can when he states: "Like in every multinational environment there are some frictions between nations, if they're NATO member or ISAF member […]." Another analyst admits that it can be frustrating to be in the centre of this circle as well. There is, however, a general feeling that ISAF is moving towards a more hospitable and inclusive sharing environment, something Capt. Brown articulate when he states that "the different nations that share with the headquarters is still a lot better than I've seen in other places". Capt. Clark agrees: "I see things now that I don't think I ever would [have] thought of seeing as far as information sharing among a multinational coalition."

The ISAF leadership has recently implemented certain initiatives that potentially could do much to overcome the barriers provided by multinationality, the first being a somewhat more open American intelligence posture. This is visualized by the appearance of SIPRNET terminals in the multinational Information Dominance Centre of IJC, a gesture that alone has done quite a bit to alleviate internal mistrust and friction. Capt. Clark thus believes that the overall picture is getting more coherent and "that our [ISAF] leadership is trying to ensure that it is." He continues: "The information sharing environment is very positive […] many nations are willing to give enough." Others are a bit less enthusiastic as exemplified by these survey comments: "In ISAF are already issues with intel sharing. National systems and national intel […]. Not shared with non-U.S. / non NATO countries." And: "Too many stovepipes!! Not enough lateral movement of intel from ISAF partners."

Another important initiative has been to establish multinational so-called Intelligence Fusion Centres at the regional commands. In RC (N) this element was separated from the traditional J2 (intelligence) structure, and will according to Capt. Evans conduct deeper cross-functional studies and projects including network analysis bringing together all relevant actors including Afghan ministries that contribute to the COIN strategy. This will leave the somewhat undermanned J2 structure (in Capt. Evans words) to work more conventional opposing forces tasks; putting together intelligence reports, conduct briefings and bring intelligence expertise to planning situations. He suggests that this centre, shielded from the daily trivialities, will "talk to the folks that have real equities and interests in describing certain functional areas of RC North's battle space." The mindset of the Intelligence Fusion Centre is to "make every effort to form a network to attack the network […]. We are reaching out across the battle-space to network with organizations that talk to us." This rather expansive objective implies intelligence sharing to be a major ingredient of the centre's work practices. Maybe this is why Capt. Anderson suggests: "Now that every RC has a fusion centre it will be even that much easier to get information shared, 'cause I just go to the fusion centre prior to going to the individual country in charge."

4.7 Intelligence ethics and moral dilemmas

Intelligence ethics are not codified by ISAF and ethical questions related to intelligence sharing do not figure prominently among analysts' expressed concerns. As one survey comment puts it: "Ethical questions should not play into the equation if clear guidance is/was provided to all incoming analysts." This comment may point towards the invaluable military ethos of readiness to serve and to comply with orders, but as with many other oversimplified generic statements also this one hides a wealth of shades and details. Many ethical questions are for instance moulded into the concept of secrecy which demands operators to protect intelligence capacity and methods as well as their sources. Capt. Brown states "that there is a very strong feeling by people to make sure that they are not compromising [the well-being and safety of their sources]".

The moral dilemmas faced on a daily basis by analysts may best be explained by the following survey comment:

> We are often told stories about how senior officers and combat commanders share information without going through proper clearing procedures. If analysts were to do the same they would be fired. Most of this is likely rumours [sic] but it does present ethical dilemmas.

Capt. Anderson addresses the same dilemma when he acknowledge that some of his counterparts may not have been properly vetted and authorized, but still finds it "a judgement call what you are going to give them, because you know that it will take a year or more to get that Afghan officer vetted […]."Angela Gendron's statement cited in paragraph 3.4 above that "sharing often takes place in spite of the rules rather than because of them" thus gets some support. Capt Clark for instance finds that "in many instances you have people who are executing from the spirit of the law but maybe not to the exact letter of the law – to avoid that bottleneck or that process".

Capt. Evans promptly acknowledges the explicit security dilemmas associated with risktaking, or "the ethics of assuming the risk with our countrymen's security […]", as well as with "the information we don't share". He continues: "Sharing would certainly come with a certain cost – and there are tradeoffs on this – on the information sharing we conduct – there are tradeoffs involved in the information sharing that we don't conduct." The optimal balance between sharing and security may never be found, and it may be that to get more security and force protection in the future one needs to accept more risk in the present. The problem is that the opposite could also be true. Analysts with their legal responsibilities therefore expect a clearly articulated policy framework with associated procedures and education for sharing. Capt. Anderson with his experience and long exposure to sharing dilemmas has found a way or method for how to rationalize this that represents a somewhat curtailed version of the prevailing "share till it hurts"[16] mantra:

> You need to ask yourself: […] what is [the] operational requirement – so what do the Afghans absolutely have to know in order to make partnered operations function, and what am I possibly compromising if I share that information.

When asked about their thoughts on how ISAF provided intelligence could be misused to support random factions in internal Afghan power struggles (e.g. conflicts between local and regional power brokers and former warlords), or to tip of corrupt officials or criminal networks like the narcotics industry, Capt. Clark's responses may be representative. "No, I have not seen that first hand […]" and "I haven't linked the two of them." Seen in context with other statements such comments may reflect that the interviewed analysts do not handle cases or share

[16] "Share till it hurts" is an expression that is attributed to the ISAF leadership and was much used in ISAF to explain the prevailing policy of intelligence partnering and sharing with the ANSF.

intelligence where these types of concerns would naturally surface. Only Capt. Anderson has thought about this and explains his way of reducing the possibility for misuse: “I share the intelligence across the board – that’s one of the mechanisms I have put in place. I have […] ANA, ANP [and] NDS in the same room”. He proposes that “you [have] got to ensure specifically that they all get the same information.” When elaborating he admits that some of the ways that the multinational forces organize and operate vis-à-vis the ANSF counteracts this requirement. But at least his section in IJC is aware and makes a point of inviting and encouraging all the three main Afghan security players to appear in partnered meetings. Such practices make it harder for any one of them to stovepipe and misuse intelligence.

4.8 Other hurdles for intelligence sharing

Some of the issues that were brought forward during interviews and observed or discussed in the margins cannot be grouped under any one of the above headings, or their subtle nature demands them to be commented upon separately. These are: (1) a lack of education and training opportunities for ISAF personnel; (2) the level of trust and confidence between ISAF and ANSF partners; and (3) internal Afghan cooperation and integration.

4.8.1 A lack of education and training opportunities for ISAF personnel

Some of the security concerns discussed in paragraph 4.5, like the vetting status of ANSF personnel, the use and understanding of different security markings and caveats, guidelines for what information should and should not be released and also best practices for making releasable products are typically alleviated through education and training. As discussed this is true also for the use of interpreters and for ethical issues. Capt. Anderson is very particular when he describes the needs:

> There ought to be a class that is vetted and proved by ISAF as to the best practices to share intelligence with ANSF. And if that programme of instruction along with appropriate and pertinent SOPs and directives from ISAF were made available to the individual analyst, they might feel a little more comfortable in sharing more intelligence.

This is supported by a survey comment where an analyst complains about the lack of training on intelligence sharing before deploying to ISAF. Another officer mentioned a course he had attended teaching how to disclose intelligence to allied nations and ISAF, but that was more from a national policy viewpoint than supporting ISAF practices. The intelligence leadership in

IJC however expects that such issues will soon find their way into the existing pre-deployment staff training. There was, however, no mentioning of any in-theatre training opportunities.

4.8.2 Trust and confidence between the partners

Partnering in general and intelligence sharing in particular are dependent on a certain level of trust between those involved, something that will be examined further in chapter 5. Capt. Clark however hints to this when he mentions that ISAF's intention is to "partner with them, live with them, work with them – over their shoulder." He continues: "I think there is an element of trust that we must demonstrate to achieve success. So until we show that trust our relationship cannot work." Capt. Anderson picks up on this when he claims that during his long but intermittent stay with ISAF, he has never seen the command as engaged in partnering one on one as right now, and especially the senior leadership: "There is a good level of shared confidence". Even among newly arrived staff members he finds a high level of confidence in their Afghan counterparts. Capt. Davies from RC (N) is a bit more reserved. He agrees that a certain level of trust has been established between a limited numbers of officers with a long term relationship, but he also reflects on examples of the opposite were their counterparts have proven less trustworthy.

Herman's citation above that every new foreign exchange represents a new risk is mostly about trust or the lack thereof. Capt. Clark compares the risks of sharing with that of giving a gift:

> You don't know what the recipient is going to do with that [gift] in the end. So you give it with one thing in mind, and the biggest risk would be that they do not use it for the intended purpose. Because knowledge is power, if you, if we would share something and the recipient just holds on to it in order to further his own agenda, I think that is the biggest tactical risk of sharing – of information sharing. […] but if you don't take that risk, you may not have a chance of success.

Capt Evans discusses another aspect of trust. He mentions the impression that some nations are willing to share only to the extent that it is consistent with the reasons for their ISAF participation and that the Afghans are willing to share only if they see an immediate benefit to themselves or their organization. As long as this impression remains he fears that "there will continue to be severe lack of trust […]", something he believes will put the COMISAF mandated sharing relationship at a disadvantage.

4.8.3 Internal Afghan cooperation and integration

IJC staff officers often hinted that cooperation amongst the three main Afghan intelligence agencies (NDS, ANA through the Ministry of Defence and ANP through the Ministry of Interior) could improve, a view that is supported by earlier findings (U.S. SECDEF, 2008, p. 14):

> Historically, information has rarely been shared; collaborative analysis and coordinated collection have been the exception rather than the norm. [….] much work remains to build national intelligence structures that encourage intelligence sharing […].

To overcome such obstacles, the international community and their Afghan partners have recently established mechanisms like Regional and Provincial Operational Coordination Centres (OCC-R / P).[17] These facilities act as permanent meeting venues for the promotion of internal cooperation and integration within ANSF and between ANSF and ISAF (Dillard, 2009).

To streamline inter-agency collaboration has however proved to be a difficult proposition even during the most benign of circumstances. The importance for ISAF comes from the fact that improved ANSF cooperation simplifies sharing and reduces the dangers of circular reporting. One way to pursue this is precisely through increased partnering and sharing efforts. Capt. Anderson alludes to this when he points out that: "through pressure from us, […] we have brought in those who are willing to cooperate amongst the various agencies". In practical terms this means to get ANA, ANP and NDS together in the same room, motivate them to share intelligence and also have them engaged in collaborative planning efforts.

In such a setting ISAF analysts often find themselves in a role as facilitators, collecting and collating Afghan intelligence into a single coherent picture. They then compare this picture with ISAF's own, and provide feedback to their Afghan counterparts suggesting where to focus further or have another look. This method facilitates the establishment of common situational awareness necessary for partnered planning and operations and it promotes development of the Afghan security sector. In addition to making Afghan agencies cooperate, it helps them to improve their entire intelligence chain from information requirements and capacity, via methods

[17] Funding for these centres are justified in the American defence budget for 2010: "[…] funding will augment operational coordination centers at the regional and joint provincial level to enable ANA, ANP, National Directorate of Security, and International Security Assistance Force (ISAF) operational coordination and *intelligence sharing* [my italics]." (U.S. SECDEF, 2009, p. 5)

and processes to products. The added bonus for ISAF is that it minimizes the needs for revealing sensitive information without necessarily compromising on efficiency or accuracy.

5 ISAF analysts knowledge and perceptions

The purpose of this chapter is to expand on the qualitative research and to identify how analysts' perceptions of the sharing environment influence ISAF's ability for intelligence sharing with the ANSF. The chapter presents the results of the survey and discusses to what extent the findings support or contradict the findings in the previous chapter. The survey focus is on the secrecy, multinationality, and ethical factors that constitute the sharing environment in this study. As secrecy and the related security concerns were identified as the main challenge for sharing in both the analytical framework and qualitative interviews, these factors will be the main focus also in this chapter.

The survey of all-source intelligence analysts resulted in 19 returns from the Information Dominance Centre of IJC and seven from the Joint Intelligence Centre of RC (N), representing the majority of such personnel in those organizations. Each of the 25 items on the self-administered questionnaire presented five alternative answers on a Likert scale from "strongly agree" via "agree" and "uncertain" to "disagree" and "strongly disagree". When commenting on the results, the two first and two last alternative answers are normally grouped. More resolution is, however, provided if significant or otherwise deemed necessary.

Figure 5 presents the respondents' accumulated employment time as intelligence analyst with ISAF. It shows that almost 50% of them have more than six months' experience, something that for many nations represents more than one full deployment period or rotation. The level of experience is somewhat higher in Kabul than up north, with a mode between six months and a year in IJC versus between two and six months in RC (N). A main difference between the two commands, however, turns out to be their analysts' experience from interaction with Afghan counterparts (figure 6). All RC (N) analysts responded that they personally seldom or never interact with Afghan counterparts, whereas 37% of the IJC analysts answered that they interact on a weekly basis or more. Only three of the 19 IJC analysts respond that they seldom or never interact. In the near future it is expected that this difference will level out, with the recently

Experience		
	Frequency	Percent
Less than two months	5	19
Less than six months	9	35
More than six months	9	35
More than a year	3	11
Sum	**26**	**100**

Figure 5: Experience as intelligence analysts with ISAF

established Intelligence Fusion Centre at RC (N) handling most of the regular host nation contacts. Finally, it turned out that all except one of the responding analysts were military, precluding this variable from further analysis.

Interaction		
	Frequency	Percent
Seldom / never	10	39
Once a month	5	19
More than once a month	4	15
Once a week	2	8
More than once a week	5	19
Sum	**26**	**100**

Figure 6: Analysts' interaction with ANSF counterparts

The importance of each analyst's judgements with regards to intelligence sharing was discussed in chapter 3. Consequently, how they personally execute ISAF's policy to a large extent determines ISAF's overall ability for such sharing. In chapter 4 it was established that ISAF HQ has produced extensive policy documentation and procedures for sharing. When respondents are confronted with the statement "I believe ISAF's partnership with the ANSF requires intelligence sharing", 96% of them agree and 62% even strongly agree, suggesting an impressive level of support for a proactive sharing policy. It further turns out that 85% of the analysts are not afraid of making wrong judgements regarding such sharing, indicating confidence in their own skills. However, when challenged with the following statement "ISAF has provided me with *clear* policies for intelligence sharing with the ANSF", six out of seven analysts in RC (N) disagree. Also in IJC the opinions are split. Less than half of the analysts agree, 21% disagree and the rest are uncertain. On the more specific statement "ISAF has established *clear* procedures and processes for disseminating intelligence to the ANSF", the responses are evenly distributed with 44% agreeing, 16% uncertain and 40% disagreeing. These results support the findings from the interviews in which the analysts' depth of policy knowledge proved superficial, and it highlights a lack of education and training opportunities.

When comparing the experience and interaction variables with how analysts respond to the statement “I know my ANSF counterparts well enough to assess their integrity and honesty”, there are also big variations. Only two out of five analysts who combine more than six months experience with weekly or more interaction find that they can agree with this statement, and the others are uncertain. Those with the shortest employment time and most infrequent interaction are typically the ones who are most doubtful. Of the approximately 40% that strongly disagree, 90% have less than six months’ experience and 70% interact with Afghans on a monthly basis or less. In conclusion, it takes time to build personal relations, and even more so in a multicultural setting framed by secrecy and suspicion. As an anecdotal afterthought it is worth mentioning that while ISAF analysts come and go, Afghan officials remain in position longer and have to go through this process over and over again. The fact that only 11% of the responding analysts have accumulated more than a year of in-theatre intelligence experience indicates that ISAF’s ability for partnering and sharing is influenced negatively by its relatively inexperienced staffs.

5.1 How to produce intelligence for sharing, and are shared secrets still secrets?

Secrecy is a diverse concept, and the related security provisions are quite demanding even for experienced operators. This makes collaboration between even long-time trusted partners difficult. Security sensitivities are therefore the main reason why multilateral intelligence sharing, and especially with strange host nations, becomes the extreme sport of international relations. Maybe the most important player in this perilous ISAF “sporting event” is the lonely analyst who produces shareable intelligence and in some way, shape or form also perform the actual dissemination of it, either by hand or through vocal and/or visual sharing. The analyst’s knowledge of ISAF’s procedures and processes for intelligence sharing as well as perceptions of the security environment to a large extent determine ISAF’s ability to share intelligence with its Afghan partners. As military personnel they are expected to follow orders and carry out assigned tasks as best they can within the limitations they are given, but as already established; the personal responsibilities for protection of secrets are explicit and even covered by law in many countries.

When analysts are confronted with the statement “I’m confident how to produce intelligence products releasable to the ANSF” more than 60% agree, and some even strongly. However, approximately 20% disagree and 20 % are uncertain. This picture does not change much when asked if they are confident how to mark intelligence products. The overall confidence in their

own skills seems to be somewhat higher among those who also find that ISAF has provided them with clear policies and established clear procedures and processes for sharing. It is on the other hand interesting that 30% of those responding that they are uncertain or disagree with the claim that ISAF has provided them with clear policies and established clear procedures and processes for sharing, are still quite positive when assessing their own skills. Some of this inconsistency could hypothetically be explained with former experience from multilateral intelligence sharing and disclosure processes, and partly by analysts simply following established work habits and routines. There seems to be even less correlation between how analysts perceive their own skills and their actual in-theatre experience, or even by how often they interact with Afghans. IJC analysts, however, appear to be more confident than their RC (N) colleagues. These findings suggest that analysts arrive in theatre with a reasonably sound general understanding and know-how on how to produce and label intelligence products for sharing, but that they lack mission specific introductions. It could also point to an unhealthy tendency of taking on established work habits without necessary consideration.

The next logical step is to ask if the analysts trust that ISAF procedures and processes facilitate secure sharing with the ANSF. Almost 60% of the IJC analysts believe so, compared to none of those from RC (N). Most of the remaining IJC analysts respond that they are uncertain, with only 10% of the total sample disagreeing.

However, when asked to consider the statement "I believe the intelligence we share with the ANSF is not compromised", only 20% agree, while almost 60% disagree (figure 7). Those who agree with the statement are among those who also believe that ISAF's procedures and processes facilitate secure sharing. All this could indicate that whatever procedures and processes ISAF establishes, most analysts still perceive that secrets will be compromised. A notable minority on the other hand believes that such procedures will actually succeed in protecting secrets. The differences between IJC and RC (N) may also indicate that increased interaction and collaboration could increase analysts' belief in the utility of procedures and processes.

I believe the intelligence we share with the ANSF is not compromised

	Frequency	Percent
Strongly agree	**2**	**8**
Agree	**3**	**12**
Uncertain	**6**	**23**
Disagree	**10**	**38**
Strongly disagree	**5**	**19**
Sum	**26**	**100**

Figure 7: Analysts' security perceptions

As discussed briefly in chapter 4, there are many reasons why secrets are compromised, all the way from a lack of basic security routines via corruption to regular espionage staged by foreign intelligence services. Figure 8 present how ISAF analysts respond to statements that discuss serious security risks which potentially could threaten their Afghan counterparts. In turn, this indicates how well analysts believe the ANSF are able to protect classified material. Only a small minority believe their counterparts to be relatively free from corruption and safe from extortion and infiltration. A solid majority does not agree, indicating that they rather believe the opposite to be the case. There is no evident correlation between these findings and the analysts' in-theatre experience or frequency of interaction with their partners. In summary, ISAF analysts believe that their Afghan counterparts are subject to substantial security threats.

	I don't believe corruption is a problem among our specific ANSF counterparts		I believe our ANSF counterparts are relatively safe from extortion		I don't believe our ANSF counterparts are infiltrated	
	Frequency	**Percent**	**Frequency**	**Percent**	**Frequency**	**Percent**
Strongly agree	**0**	**0**	**0**	**0**	**0**	**0**
Agree	**2**	**8**	**4**	**15**	**3**	**12**
Uncertain	**8**	**31**	**8**	**31**	**5**	**19**
Disagree	**9**	**34**	**11**	**42**	**11**	**42**
Strongly disagree	**7**	**27**	**3**	**12**	**7**	**27**
Sum	**26**	**100**	**26**	**100**	**26**	**100**

Figure 8: Analysts' security perceptions in more detail

When asked to consider the statement "I sometimes feel pressured to share intelligence that I believe should be withheld on security reasons", 62% of the respondents disagree and of those 23% even strongly. However, a substantial minority of 23% agrees and 15% are uncertain. The survey does not reveal common characteristics between these analysts, but it is noteworthy that so many of them strongly disagree and seemingly never feel pressured to forsake security. However, most of these respondents have less than two months of in-theatre experience. The responses on the next statement: "I believe security concerns always trump the need for sharing" is perhaps more surprising with 34% agreeing and as many as 38% disagreeing. Even if it is not possible to draw firm conclusions from these responses, pressure to share intelligence does not appear to figure prominently among most analysts' worries. Many on the other hand seem to have an almost stoic "matter of fact" attitude towards manifest security risks, and appear not to be such deep-rooted security absolutists that some may expect.

Evidently, quite a few analysts can imagine instances were security should yield for some higher purpose. This is reinforced by their responses to the next two statements. 27% agree that when in doubt they "tend to lean towards sharing and accept some security risks" while 15% are uncertain, and the rest disagree. In fact, almost all those IJC analysts that tend to lean towards sharing or respond that they are uncertain, at the same time trust ISAF procedures and processes to facilitate secure sharing. They also tend to agree with the following statement: "I principally trust and follow my own judgement on what to share and what not to share". It turns out that 77% of all respondents agree to this and 19% even strongly agree. This is one of just two items were no analysts respond that they are uncertain, and the remaining 23% are evenly split between disagreeing and strongly disagreeing. Of those 23%, two thirds seldom or never interact with their ANSF counterparts. Drawn together this indicates that most analysts trust their own judgement when it comes to sharing and that quite a few of them, at least occasionally, tend to favour sharing over security.

These rather wide ranging findings support what was exposed in chapter 4: that analysts lack detailed knowledge about ISAF policies, procedures and processes for intelligence sharing with the ANSF. While they seem to be enthusiastic about such sharing and to a certain extent also positive with reference to their own skills and the usefulness of ISAF procedures and processes, they at the same time seem to be quite realistic about the security risks involved. In other words most analysts: (1) feel that they know what is expected of them; (2) to a certain extent believe they know how to do it; and (3) have a sobering appreciation of the risks involved. The responses also support earlier findings which indicate that quite a few analysts are pragmatic when it comes to security, and that they seek to find workable solutions for sharing where possible. The question is whether their perceptions of the security environment limit ISAF's overall ability for intelligence sharing. Given each analyst's (legal) obligations for the protection of secrets, the answer is self-evident. There is also a limit to how much risk individuals are willing to take. When reviewing how they expressed themselves during interviews and comparing that with how they responded on the survey, there is little to indicate that analysts are negligent or careless when it comes to security. Some private initiatives to overcome the security challenges and dilemmas were discussed in chapter 4, but they are both isolated and resource intensive. There is little to suggest that "best practices" on sharing is widely debated.

5.2 Multinationality – adding another layer to the complexity

Findings in chapter 4 indicate that there are substantial differences between ISAF's troop-contributing nations in how they look upon and practice (local) intelligence sharing with the ANSF. Even if analysts recognize that ISAF is moving towards a more hospitable and inclusive environment for information sharing, they find that national caveats and differences still cause friction and prevent a uniform ISAF-wide sharing regime. Some use the term "stovepipes" when discussing national and agencies sharing practices. It was further identified that differences in national processes and procedures as well as a multitude of information systems cause problems for sharing. In an open study many such aspects can only be superficially examined and nation-specific variables must in general be left out. Analysts' ability for producing and disseminating shareable intelligence will, however, be influenced by the support given from ISAF's organic intelligence collectors and national agencies alike, and also by how well the analyst knows the practices and routines of subordinate headquarters. The last aspect is important for him for different reasons, among them to preclude or at least estimate the dangers of circular reporting.

The responses on the statement "In general I'm aware of what our subordinate headquarters share with the ANSF (within my functional or geographical area of responsibility)" are varied with 42% agreeing, the same number disagreeing and the rest being uncertain. Also those that agree or disagree strongly are equally split with 8% on each. In RC (N) most analysts disagree, but with the small sample size this is not indicative of a major difference between the two headquarters. However, that so many analysts from a regional command disagree coincides with the proposition that local intelligence relations between homogenous national forces and local host nation are more bilaterally oriented (and thus more isolated from multinational reach or review).

To produce shareable multinational intelligence the analysts depend on collectors and nations to supply them with information and intelligence that can be released further and that are marked accordingly. It turns out that 50% of the analysts agree that "intelligence collectors usually mark their information if further dissemination to the ANSF is permissible." 31% disagree, and the rest are uncertain. It is important to establish that agreement to this statement does not indicate if analysts are content with the volume of releasable products, only that they are not kept in ignorance. One collector agency could for instance mark all their products "not for further release" and still fall within the statement. As was mentioned in chapter 4, one nation asserted that they would not share anything. When asked to comment on the same statement substituting

“intelligence collectors” with “nations”, 62% agree and 31% disagree that nations usually mark their information if further dissemination to the ANSF is permissible. Notably 23% changed their response from agreeing or disagreeing to the opposite. If nothing else, this supports the findings that analysts have mixed experience with how nations and collector agencies practice sharing and also how they support ISAF’s sharing initiatives.

5.3 Ethics – the absent debate

The last factor to be examined is how analysts’ knowledge and perceptions related to intelligence ethics and local moral dilemmas may limit ISAF’s ability for intelligence sharing. As established in chapter 4, ISAF has not codified ethics for intelligence sharing as part of their documentation and ethical questions related to sharing does not appear to figure prominently among analysts’ expressed concerns. Even so, 38% of them agree to a statement proclaiming that “ISAF has clear ethical standards for intelligence sharing with the ANSF” while the same number is uncertain and 24% disagree. There are few noticeable differences between how analysts from the two commands respond to this and subsequent ethical statements, and also little correlation with what they have answered on other statements. In fact, 35% of them see few ethical problems with disseminating intelligence to the ANSF, while 46% disagree and 11% even strongly disagree. This indicates that some analysts believe they are following expressed ISAF standards and guidelines, but also that many are concerned about underlying ethical challenges related to sharing. One dilemma that most of them have to relate to is the ever present conflict between obeying security demands and fulfilling sharing needs. This combined security and ethical dilemma is hypothetically what drives analysts’ responses. As alluded to in the interviews, some may be of the opinion that ISAF’s policy for intelligence sharing renders separate ethical guidelines redundant.

The statement “I don’t believe ISAF provided intelligence fuel Afghan power struggles or otherwise cause civilian suffering” is designed to force analysts to consider specific ethical issues that relate to Afghanistan’s recent history where warlords, strongmen and powerbrokers have ruled the hinterlands and been in control of much of the local politics. 38% agree with the statement, and 31% disagree. The percentages which strongly agreed or strongly disagreed were also of equal size. These rather inconsistent answers could indicate that analysts disagree between themselves if shared intelligence is misused in this specific way, or simply that the statement opens for different interpretation. Seen in context with the interviews and also with the general field observations and conversations in theatre, the mixed responses could however also

indicate that many analysts do not work on issues or share intelligence where these types of concerns would naturally surface. However, the mixed responses suggest that many analysts are concerned about the cascading effects of ISAF's intelligence sharing.

When confronted with the statement "I see few dilemmas between my professional ethics and ISAF's policy for intelligence sharing with the ANSF", 54% respond that they agree. There is, however, a substantial minority of 23% that disagree and also a relatively big share responding that they are uncertain. This suggests that many analysts are content, but it also highlights that quite a few recognize dilemmas and could be anxious about the results. On the next statement; "I sometimes feel pressured to share intelligence that I believe should be withheld on ethical reasons", only 8% agree. 38% disagree and another 27% strongly disagree. There are some interesting similarities between how analysts respond on this statement and on a similar statement above were "ethical reasons" was substituted with "security reasons". Of those analysts who strongly disagree that they feel pressured to share intelligence, all but one responded the same way for security reasons. Also, just one analyst has opposite responses on these two statements. This may indicate that analysts are not typically put under pressure to share specific intelligence products, but rather given latitude to perform partnering and sharing in a way that does not compromise their professional ethics or security concerns. The relatively wide and incoherent distribution of responses on ethical statements may, however, indicate a lack of dialogue and attention to such challenges and moral dilemmas involved in intelligence sharing. This could be accentuated by a lack of codification and of missing education and training opportunities. To leave ethical considerations solely to the individual analyst could reduce both the coherence and efficiency of ISAF's intelligence sharing.

6 Conclusion

The purpose of this chapter is to present the most important findings from the research and draw conclusions on issues that limit ISAF's ability for sharing intelligence with the Afghan National Security Forces. Except for the first point below, which arguably is the most important hurdle against sharing, the findings are presented in order of their appearance throughout the study. An overall conclusion is that ISAF share less intelligence with the ANSF than what is stipulated by ISAF policy. At the same time, the sharing that do take place seems to have a higher security cost than intended by the same policy. A main reason behind this is that intelligence analysts have to rely on their own subjective judgement when practicing intelligence sharing in overly complex working conditions. Some of the hurdles and challenges identified in this study are within ISAF's mandate to mend, while others depend on international cooperation and goodwill.

- **Lack of education and training on intelligence sharing**. Analysts are very specific about the lack of more formal education and training opportunities on ISAF's policies, procedures and processes for intelligence sharing. Documentation for such sharing exists in the form of written communication and Standard Operating Procedures, but the analysts' knowledge about the contents proved superficial. The effect is insecurity and restraints among intelligence professionals as well as force-wide differences in sharing practices and performance. Security concerns like the vetting status of ANSF personnel; the use and understanding of different security markings and caveats; guidelines for what information should and should not be released and also best practices for making releasable products are among those issues that could be eased through education and training. Education and training could also teach intelligence professionals to make better use of interpreters, and it could be used as a venue for discussing ethics and moral dilemmas related to sharing. The rapid turnover caused by short rotation periods for military personnel just underscores the importance of a more formal system for the transfer of experience and maintenance of corporate memory.

- **Missing quality control with translations and poor utilization of interpreters**. Through their work analysts sometimes experience that translated information simply does not make sense, or that mistakes have humiliating or even serious operational effects. They are however not aware of any ISAF specific mechanisms for quality control with the work of interpreters, and some even feel that this is one of the major weaknesses with ISAF's partnering efforts. Furthermore, the use of interpreters during partner

meetings has not been properly rehearsed, either by Afghans or ISAF analysts. Sentences and statements tend to become too long and complicated and cover too many topics for interpreters to keep up. The result may be poor translations that fail to convey facts and messages from intelligence products and conversations.

- **Lack of mechanisms for preventing circular reporting**. Even though circular reporting is a widely recognized problem amongst intelligence professionals, the research does not identify it as being much debated or emphasized within ISAF. Some analysts and leaders acknowledge certain problems with circular reporting related to sharing, but individuals that work to preclude it from being accidentally or intentionally introduced into the intelligence cycle are seemingly left to find and implement their own countermeasures. Such sporadic and isolated efforts influence ISAF's coherence and effectiveness, and therefore also to some extent its ability for intelligence sharing. Rather surprisingly, the research did not identify the fear of circular reporting as a main obstacle for sharing.

- **Inconsistent security marking of intelligence products**. None of the analysts, either interviewed or asked in the margins, was able to explain precisely which security markings to use on which system for intelligence sharing with the ANSF. Without global standards, troop-contributing nations follow their own regulations or NATO standards, or even a mix thereof, when labelling secret products. The resulting variations and differences add to analysts' insecurity and restraint. Even though the situation is improving, many nations and agencies still do not specify if their intelligence can be shared with Afghans or not. Those who do, often mark the whole document rather than each individual paragraph as is intended with security markings. The result is that analysts often must confer with sources on every tiny bit of information they want to include in their releasable products, something that takes time, if at all feasible.

- **Too many information systems and access levels**. Some ISAF analysts use three different classified information systems in their daily work; a "mission secret" system; a "NATO secret" system; and finally, a national system like the American "SIPRNET". To work several systems with limited interconnectivity is always demanding, but it becomes even more confusing when each system brings separate standards for security markings and access rules. This diversity of information systems highlights another source of irritation, especially amongst intelligence professionals from non-NATO countries. Not

only are they denied access to certain information and intelligence, but most of them even have restricted access to work-spaces where “NATO secret” systems are present. This class-system with its concentric circles of trust creates internal differences, leaving some coalition members less informed and involved in intelligence matters than others. To operate more than one mission wide information system is thus an obstacle for all types of intelligence sharing.

- **Underdeveloped Afghan security standards.** ISAF’s ability for legitimate disclosure and dissemination of intelligence depends on their Afghan partner’s ability to protect secrets. Generally, ISAF analysts highlight dismal Afghan security standards as the major security concern and bottlenecks for sharing. What causes most concern is obviously a lack of “NATO-compatible” Afghan traditions and culture for handling sensitive information as much as deliberate leaks. This points to a moral dilemma that is troubling many analysts; the dilemma between security and sharing. To share what should have been withheld could in a worst case situation have fatal consequences, but so could the opposite. Intelligence sharing is, however, so important for the counterinsurgency strategy that the ISAF leadership is willing to accept much risk. Even so, this does not release intelligence professionals from their individual (legal) responsibilities for the protection of secrets, and especially secrets that are provided by a third party. To carry out sharing in a high risk environment requires a high degree of trust, something that is not always present.

- **Different national policies, procedures and caveats.** ISAF has limited integral capacity for intelligence collection and depends on support from the troop-contributing nations to accomplish their mission. However, each nation comes with its own set of policies for intelligence sharing and they enforce their own caveats. Intelligence professionals experience big differences, and some nations and agencies are very restrictive. These differences lead to geographical variations that accumulate from the local tactical level all the way up to the force headquarters, with some units and headquarters being more forthcoming at sharing than others. In addition, some nations employ complex and time-consuming procedures for intelligence disclosure and dissemination, leading to a loss of both timeliness and relevance especially when dealing with Afghan partners.

- **Lack of debate on intelligence ethics and moral dilemmas.** Intelligence ethics are not codified by ISAF and ethical questions related to intelligence sharing does not appear to be at the forefront of the analysts' concerns. Even so, most analysts are aware that ethics influence their sharing efforts. In fact, moral dilemmas are manifest in much of their daily work where the main struggle seems to be between security demands and the operational necessity of sharing intelligence with a challenging partner. This plight of being "damned if you do and damned if you don't" seems to worry individuals more than ISAF as an organization. Some analysts seem to put security first, while others seem to prioritize sharing. The lack of a "Unit Disclosure Officer" in Regional Command North just accentuates the point that this is mostly left as an individual dilemma. The cost for ISAF is a loss of influence on important security questions and sharing priorities as well as less uniformity of its sharing efforts.

This study's analytical framework presented some basic assumptions of factors that potentially could limit intelligence sharing from a multinational force to the host nation in contexts such as Afghanistan. A modified model of the intelligence cycle highlighted *communication* and *circular reporting* as two such factors. Communication was found to be important while circular reporting appeared to be of less significance in this case. The reason for this is uncertain, but the lack of attention to circular reporting could indicate a weakness with ISAF's intelligence production and sharing efforts. The model suggests that the possibility of shared intelligence being channelled back into the intelligence cycle as new information should have constituted a bigger concern within ISAF, and that more staff resources should have been allocated to prevent such results from intelligence sharing. The analytical framework then introduced the "sharing environment" consisting of the three factors s*ecrecy*, *multinationality* and *ethics*. All of these proved to influence and limit ISAF's ability for intelligence sharing. However, the ethical factor proved a little less salient and it was less explicitly discussed and recognized among intelligence analysts.

In conclusion, a similar framework with the five listed factors could be used for studying intelligence sharing in contexts where a multinational force supports a host nation government fighting insurgencies. The modified model of the intelligence cycle is even less specific, and could have wider application for intelligence theory. Another important discussion presented in the analytical framework was whether shifting from a "need to know" to a "need to share" approach to intelligence sharing would increase collaboration between agencies and international

partners. It was suggested that it would be better to identify more exactly what friends and partners need to know rather than to advocate a new culture. The wide range of responses from ISAF analysts when asked to consider statements which prioritize between sharing and security, accentuated the restraint and uncertainty that was expressed during the interviews. In practical terms, the all-source community appears slightly divided and even confused in their response when sharing is stated more as a separate objective than as a means. A forced mental process of identifying who actually need to know certain information, also among host nation agencies, could help to realign the community. Over time, active identification of all those who “need to know” could increase the amount of intelligence sharing without unnecessary compromising on security.

References

Born, H., & Leigh, I. (2005). *Making intelligence accountable: legal standards and best practice for oversight of intelligence agencies*. Oslo: Pub. House of the Parliament of Norway.

Bowman, S., & Dale, C. (2009). War in Afghanistan: Strategy, military operations, and issues for Congress. Retrieved Mar 18, 2010, from http://www.fas.org/sgp/crs/row/R40156.pdf

Changes to the Security Act. (2008). Act of 11 April 2008 No. 9 relating to changes to law on protective security services (the Security Act). Retrieved Jan 27, 2010, from http://www.lovdata.no/all/hl-20080411-009.html

Clark, R. M. (2007). *Intelligence analysis: a target-centric approach*. Washington, D.C.: CQ Press.

Cordesman, A. H. (2009). Afghan National Security Forces: Shaping the path to victory. Retrieved January 7, 2010, from http://csis.org/files/publication/090727_ansf_draft.pdf

Creswell, J. W. (2009). *Research design: qualitative, quantitative, and mixed methods approaches*. Los Angeles: SAGE.

Dillard, P. (2009). OCCs take shape in time for elections. *The Enduring Ledger*. Retrieved February 14, 2010, from http://www.cstc-a.com/News/enduring%20ledgers/2009endledger/JulyEL.pdf

Flynn, M. T., Pottinger, M., & Batchelor, P. D. (2010). Fixing Intel: A blueprint for making intelligence relevant in Afghanistan. *Voices from the field*. Retrieved January 24, 2010, from http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf

Gendron, A. (2006). The ethics of intelligence in Peace Support Operations. In D. Carment & M. Rudner (Eds.), *Peacekeeping intelligence: new players, extended boundaries* (pp. 158-175). Abingdon: Routledge.

Harman, J. (2009, Dec 30). Harman statement on security and information sharing. Washington, DC: FDCH Press Releases.

Herman, M. (1996). *Intelligence power in peace and war*. Cambridge: Cambridge university press.

Herman, M. (2001). *Intelligence services in the information age: theory and practice*. London: F. Cass.

IJC. (2010). Command Brief. Unpublished presentation. ISAF Joint Command.

Joint Chiefs of Staff. (2004). Joint Publication 2-01: Joint and national intelligence support to military operations. Retrieved February 8, 2010, from http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf

Joint Chiefs of Staff. (2007). Joint Publication 2-0: Joint intelligence. Retrieved Jan 28, 2010, from http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf

Joint Chiefs of Staff. (2009). Joint Publication 3-24: Counterinsurgency operations. Retrieved January 24, 2010, from http://www.dtic.mil/doctrine/new_pubs/jp3_24.pdf

McChrystal, S. A., & Hall, M. T. (2009). ISAF Commander's counterinsurgency guidance. Retrieved Jan 29, 2010, from http://www.nato.int/isaf/docu/official_texts/counterinsurgency_guidance.pdf

NATO. (2002). Security within the North Atlantic Treaty Organization (NATO). Retrieved Feb 6, 2010, from http://www.freedominfo.org/documents/C-M(2002)49.pdf

NATO. (2006). *NATO Handbook*. Brussels: NATO Public Diplomacy Division.

NATO. (2008). Afghanistan briefing. *NATO briefings*. Retrieved Jan 29, 2010, from http://www.nato.int/nato_static/assets/pdf/TEST-PDF/2008_11_687B00694B0B4918A2143DBD2EB990F5_afghanistan2008-e.pdf

NATO. (2009a). ISAF command structure. Retrieved Feb 5, 2010, from http://www.nato.int/isaf/structure/comstruc/index.html

NATO. (2009b). AAP-6(2009) NATO Glossary of terms and definitions (English and French). Retrieved March 4, 2010, from http://www.nato.int/docu/stanag/aap006/aap-6-2009.pdf

Neville-Jones, P. (2003). Foreword. In B. d. Jong, W. Platje & R. D. Steele (Eds.), *Peacekeeping intelligence: emerging concepts for the future* (pp. i-vi). Oakton, Va.: OSS International Press.

NSM. (undated). About NSM. Retrieved Jan 25, 2010, from https://www.nsm.stat.no/Engelsk-start-side/About-NSM/

Omand, D. (2007). Reflections on secret intelligence. In P. Hennessy (Ed.), *The new protective state: government, intelligence and terrorism* (pp. 97-122). London: Continuum.

Omand, D. (2009). Modern secret intelligence: the relationship with the customer. Unpublished presentation. The Norwegian Defence Command and Staff College.

Petraeus, D. H. (2008). Multi-National Force-Iraq Commander's counterinsurgency guidance. Retrieved Jan 28, 2010, from http://www.centcom.mil/images/multimedia/cg%20coin%20unclass%20anacondaguidance%2020july08.pdf

Security Act. (1998). Act of 20 March 1998 No. 10 relating to protective security services (the Security Act) [unofficial translation by the University in Oslo]. Retrieved Jan 26, 2010, from http://www.ub.uio.no/ujur/ulovdata/lov-19980320-010-eng.pdf

Shulsky, A. N. (1993). *Silent warfare: understanding the world of intelligence*. Washington: Brassey's.

Simons, H. (2009). *Case study research in practice*. Los Angeles: SAGE.

Sims, J. E. (2005). Understanding ourselves. In J. E. Sims & B. L. Gerber (Eds.), *Transforming U.S. intelligence* (pp. 14-59). Washington, D.C.: Georgetown University Press.

Sterzer, M., McDuff, P., & Flasz, J. (2008). Note to file - The challenge of centralized control faced by the intelligence function in Afghanistan. *Canadian Army Journal, 11*(2), 96-100.

The 9/11 Commission. (2004). The 9/11 Commission report: Final report of the National Commission on Terrorist Attacs upon the United States - executive summary. Retrieved Jan 28, 2009, from http://govinfo.library.unt.edu/911/report/911Report_Exec.pdf

Thruelsen, P. D. (2008). *Implementing the comprehensive approach in helmand - Within the Context of Counterinsurgency.* Copenhagen: Royal Danish Defence College.

Tovo, K. (2005). *From the ashes of the phoenix: Lessons for contemporary counterinsurgency operations.* U.S. Army War College, Carlisle, PA.

Treverton, G. F., Jones, S. G., Boraz, S., & Lipscy, P. (2006). Toward a theory of intelligence: Workshop report. Retrieved January 8, 2010, from http://www.rand.org/pubs/conf_proceedings/2006/RAND_CF219.pdf

U.S. SECDEF. (2008). United States plan for sustaining the Afghanistan National Security Forces; Report to Congress in accordance with the 2008 National Defense Authorization Act (Section 1231, Public Law 110-181). Retrieved Mar 18, 2010, from http://www.defense.gov/pubs/united_states_plan_for_sustaining_the_afghanistan_national_security_forces_1231.pdf

U.S. SECDEF. (2009). Department of Defense budget fiscal year (FY) 2010: Justification for FY 2010 Afghanistan Security Forces Fund (ASFF). Retrieved Mar 18, 2010, from http://asafm.army.mil/Documents/OfficeDocuments/Budget/BudgetMaterials/FY10/OCO//asff.pdf

UN. (2001). Security Council Resolution 1386 (20 December 2001). Retrieved Jan 12, 2010, from http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/708/55/PDF/N0170855.pdf?OpenElement

UN. (2006). Definition of basic concepts and terminologies in governance and public administration (5 January 2006). Retrieved Mar 11, 2010, from http://unpan1.un.org/intradoc/groups/public/documents/un/unpan022332.pdf

UN. (2009). Security Council Resolution 1890 (8 October 2009). Retrieved Jan 12, 2010, from http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N09/550/19/PDF/N0955019.pdf?OpenElement

United States Air Force. (2007). Air Force doctrine document 2-9: Intelligence, surveillance and reconnaissance operations. Retrieved Feb 11, 2010, from http://www.fas.org/irp/doddir/usaf/afdd2-9.pdf

Yin, R. K. (2003). *Case study research: design and methods*. Thousand Oaks, Calif.: Sage.

Zeleny, J., & Cooper, H. (2010, Jan 6). Obama says U.S. failed to understand intelligence on terror plot. *The New York Times* A11.

Annex A: Glossary

Part 1 - Abbreviations and acronyms

ANA	Afghan National Army
ANP	Afghan National Police
ANSF	Afghan national security forces
COIN	Counterinsurgency
GIRoA	Government of the Islamic Republic of Afghanistan
HN	host nation
HUMINT	human intelligence
IDC	Information Dominance Centre
IFC	Intelligence Fusion Centre
IFOR	Implementation Force
IJC	ISAF Joint Command
ISAF	International Security Assistance Force
JIC	Joint Intelligence Centre
JPOC	Joint Planning Operation Centre
KFOR	Kosovo Force
NDS	National Directorate of Security
NIC	National Intelligence Cell
NMCC	National Military Coordination Centre
OCC R / P	Operational Coordination Centre Regional / Provincial
PRT	Provincial Reconstruction Team
RC (N)	Regional Command North
SFOR	Stabilization Force
SIPRNET	Secret Internet Protocol Router Network
SOP	Standard Operating Procedures

Part 2 – Terms and definitions

The terms and definitions used in this paper are in priority order drawn from one of the cited official references; (1) NATO standards in accordance with AAP-6; (2) U.S. standards in accordance with Joint Publications 2-0, 2.01 and 3-24; (3) U.N. standards in accordance with the "Definition of basic concepts and terminologies in governance and public administration" by the committee of Experts on Public Administration (UN, 2006); or (4) they are amalgamated or revised from corresponding definitions in those references and made specific for this study.

Accessing and Collection – Used here to describe the process of accessing any secret, open or data protected sources of information, acquisition of the relevant pieces of that information and converting it into forms suitable for analysis and assessment. This process is performed by collection agencies.

Agency – Used here for any organization or individual engaged in the processes of accessing, collecting and/or analysing and assessing information.

All-source intelligence - Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence. (Joint Chiefs of Staff, 2007)

Analysis and assessment – Used here to describe the process of conversing information into finished intelligence through the integration, evaluation, analysis, and interpretation of all source data, with assessments being those products with a *forward-looking* perspective. This process is performed by all-source agencies.

Circular reporting – Used here for describing a situation where shared intelligence information is channelled back into the intelligence cycle as new information (duplication), sometimes also being distorted or interpreted differently on the way deceiving analysts to believe that they have got corroboration on earlier reports.

Collation - (1) The grouping together of related items to provide a record of events and facilitate further processing; and (2) To compare critically two or more items or documents concerning the same general subject; normally accomplished in the processing and exploitation portion of the intelligence process. (Joint Chiefs of Staff, 2007)

Confirmation - An information item is said to be confirmed when it is reported for the second time, preferably by another independent source whose reliability is considered when confirming information. (Joint Chiefs of Staff, 2007)

Corruption – Influencing the decision-making process of a public officer or authority, or influence peddling; dishonesty or breach of trust by a public officer in the exercise of his duty; insider dealing/conflicts of interests; [and] influence peddling by the use of fraudulent means such as bribery, blackmail, which includes the use of election fraud. It is a form of behaviour that deviates from ethics, morality, tradition, law and civic virtue. (UN, 2006)

Counterinsurgency (COIN) - Comprehensive civilian and military efforts taken to defeat an insurgency and to address any core grievances. (Joint Chiefs of Staff, 2009)

Disclosure – Used here to describe the process of clearing intelligence for release and its subsequent dissemination to authorized users outside the originating nation or organization.

Dissemination - The timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it. (NATO, 2009b)

Ethics – Used here as the standards which guide the behaviour and actions of organizations and personnel involved in intelligence sharing and which may be referred to as moral laws or policy.

Governance - The state's ability to serve the citizens through the rules, processes, and behaviour by which interests are articulated, resources are managed, and power is exercised in a society, including the representative participatory decision-making processes typically guaranteed under inclusive, constitutional authority. (Joint Chiefs of Staff, 2009)

Host Nation (HN) – Used here to describe a nation which voluntary receives the forces and/or supplies of a multinational peace support or intervention force to be located on, to operate in, or to transit through its territory.

Intelligence - The product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity. (NATO, 2009b)

Information systems – Used here to cover all aspects of IT support to the multinational force and its national contributions but with a particular emphasis on those systems that intelligence analysts use for their normal work as well as those national systems they access and/or or get information from on a routinely basis.

Insurgency - The organized use of subversion and violence by a group or movement that seeks to overthrow or force change of a governing authority. Insurgency can also refer to the group itself. (Joint Chiefs of Staff, 2009)

Intelligence Community – Used here to describe all departments or agencies of a government or multinational force that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role.

Intelligence cycle - The sequence of activities whereby information is obtained, assembled, converted into intelligence and made available to users. (NATO, 2009b)

Planning and direction - The determination of intelligence requirements, development of appropriate intelligence architecture, preparation of a collection plan, and issuance of orders and requests to information collection agencies. (Joint Chiefs of Staff, 2007)

Operational control - The authority delegated to a commander to direct forces assigned so that the commander may accomplish specific missions or tasks which are usually limited by function, time, or location; to deploy units concerned, and to retain or assign tactical control of those units. It does not include authority to assign separate employment of components of the units concerned. Neither does it, of itself, include administrative or logistic control. (NATO, 2009b)

Reach back - The process of obtaining products, services, and applications, or forces, or equipment, or material from organizations that are not forward deployed. (Joint Chiefs of Staff, 2009)

Secret Internet Protocol Router Network (SIPRNET) - Worldwide SECRET level packet switch network that uses high-speed internet protocol routers and high-capacity Defence Information Systems Network circuitry. (Joint Chiefs of Staff, 2004)

Security - The condition achieved when designated information, materiel, personnel, activities and installations are protected against espionage, sabotage, subversion and terrorism, as well as against loss or unauthorized disclosure. (NATO, 2009b)

Security Classification - A category or grade assigned to defence information or material to indicate the degree of danger to NATO/national security that would result from its unauthorized disclosure and the standard of protection required to guard against unauthorized disclosure. (NATO, 2009b)

Security Clearance - An administrative determination by competent national authority that an individual is eligible, from a security standpoint, for access to classified information. (NATO, 2009b)

Security Sector Reform (SSR) - The set of policies, plans, programs, and activities that a government undertakes to improve the way it provides safety, security, and justice. (Joint Chiefs of Staff, 2009)

Source - The means or system that can be used to observe and record information relating to the condition, situation, or activities of a targeted location, organization, or individual. An intelligence source can be people, documents, equipment, or technical sensors. (Joint Chiefs of Staff, 2007)

Threat Warning - The urgent communication and acknowledgement of time-critical information essential for the preservation of life and/or vital resources. (Joint Chiefs of Staff, 2004)

Annex B: Interview guide

Name……
Rank……
Position…….....
Time……

My research objective is to reveal limitations on ISAFs ability to disseminate *multinational* intelligence to Afghan National Security Forces (ANSF). The collection of empirical data consists of two parts; first a few semi-structured interviews with central intelligence officers like yourself to investigate ISAF procedures and routines as well as recognized problem areas, and then, adjusted as necessary for the findings during these interviews, a survey of intelligence analysts in ISAF HQ and RC North to reveal their knowledge and attitudes for producing and disseminating releasable intelligence.

The interview will last approximately 1 hour, and it will cover the following areas:

- General issues (ISAF policy and practice)
- Security issues
- Issues stemming from the multinational composition of ISAF
- Ethical issues

This research is conducted at the **UNCLASSIFIED** level and the interviews will be taped, transcribed and stored by the researcher.

Your responses will be used for research purposes only.

ISAF Policy

The first issue I would like to discuss is ISAF's policy for dissemination of intelligence to the ANSF. Could I please ask you to elaborate a bit on this, and also how you view the performance of this headquarters?

- Procedures and processes - responsibilities and roles
- Major challenges and/or bottlenecks *(weaknesses in the chain)*
- Education and training opportunities *(for those producing intelligence for sharing)*

Security

Proceeding from general policy matters, I would now like you to comment on security issues related to sharing. What do you see as the major challenges here?

- NATO security regulations *(strengths and weaknesses)*
- Vetting and authorization of Afghans *(how many – what problems)*
- Procedures for the translation of written and oral products / quality control *(literal accuracy and how the message is understood by Afghan audiences)*
- Level of trust between this headquarters and its ANSF counterparts.

Multinationality

Then, I would like to discuss how multinationality influence sharing. Could you please include some comments on coherence between the different headquarters and nations?

- Influence of formalities such as document templates, security labels and dissemination keys *(asset from know-how and uniformity or drawback from habitual behaviour - "copy last")*
- Biggest risks. *(Circular / contradictory reporting)*
- Common databases and analytical tools.

Ethics

My last theme is about ethics. Could I please ask you to elaborate on ethical challenges and possible consequences of sharing, including what ethical guidelines ISAF employ?

- Showcasing of coalition differences *(opening for manipulation)*
- Fuelling of internal Afghan power struggles *(unintended ethnic favouritism)*
- Other misuse *(organized and petty crime e.g.)*
- The divide between internal security and foreign intelligence *(democratic challenges)*.

Annex C: Survey questionnaire

1 Purpose of this questionnaire

The purpose of this questionnaire is to investigate ISAF intelligence analyst's knowledge and attitudes for producing and disseminating intelligence to the Afghan National Security Forces (ANSF).

By participating in this study you will get the opportunity to communicate your experiences and perceptions regarding important aspects of the multinational strategy for Afghanistan in general and for ISAF partnering with the ANSF in particular.

2 Your rights as participant

As participant in this study, you have the right to:

1. Decline participation.

2. Withdraw from the research at any time during your participation.

There will be no consequences of declining or withdrawing from the study.

If further information about the research or your rights as participant is needed, please contact Helge Arnli in person or at helge.arnli@gmail.com.

3 Instructions

Your responses to this questionnaire will be treated as **anonymous and confidential** and will only be used for research purposes. Please answer **all** questions.

The questionnaire is expected to take approximately 15 minutes to complete.

1. Please indicate your response to each question by encircling one of the provided alternatives. If you want to correct, please make an X over the false option.

2. Statistically respondents tend to lean towards a central tendency, i.e. the middle of the scale. Please keep this in mind and make, if possible, choices based on preferences.

3. Please read the questionnaire carefully and reflect for a moment before answering.

4. The questionnaire is individual and cooperation would ruin the research reliability.

Thank you for your participation. Your contribution is highly appreciated!

☐ **By checking this box I agree that I have been informed of my rights reference participating in this research and give my consent for the researchers to use my response for research purposes only.**

DEMOGRAPHIC DETAILS

Please mark the appropriate option.

Employment type:

Military ☐ 1

Civilian ☐ 2

Total accumulated employment time as intelligence analyst with ISAF:

Less than two months ☐ 1

Less than six months ☐ 2

More than six months ☐ 3

More than a year ☐ 4

Please indicate to what extent you agree with the statements below by encircling the corresponding number.

Q	Statement	Strongly Agree	Agree	Uncertain	Disagree	Strongly Disagree
1	ISAF has provided me with *clear* policies for intelligence sharing with the ANSF.	1	2	3	4	5
2	ISAF has established *clear* procedures and processes for disseminating intelligence to the ANSF.	1	2	3	4	5
3	I'm confident how to produce intelligence products releasable to the ANSF.	1	2	3	4	5
4	I'm confident how to mark intelligence products releasable to the ANSF.	1	2	3	4	5
5	I believe ISAF's partnership with the ANSF requires intelligence sharing.	1	2	3	4	5
6	I trust that our procedures and processes facilitate secure sharing with the ANSF.	1	2	3	4	5
7	I believe the intelligence we share with the ANSF is not compromised.	1	2	3	4	5
8	I don't believe corruption is a problem among our specific ANSF counterparts.	1	2	3	4	5
9	I believe our ANSF counterparts are relatively safe from extortion.	1	2	3	4	5

Please indicate to what extent you agree with the statements below by encircling the corresponding number.

Q	Statement	Strongly Agree	Agree	Uncertain	Disagree	Strongly Disagree
10	I don't believe our ANSF counterparts are infiltrated.	1	2	3	4	5
11	I have ANSF counterparts that I meet on regular basis (please encircle how often).	Seldom/never	Once a month	More than once a month	Once a week	More than once a week
12	I know my ANSF counterparts well enough to assess their integrity and honesty.	1	2	3	4	5
13	I sometimes feel pressured to share intelligence that I believe should be withheld on security reasons.	1	2	3	4	5
14	I believe security concerns always trump the need for sharing.	1	2	3	4	5
15	I principally trust and follow my own judgement on what to share and what not to share.	1	2	3	4	5
16	When in doubt I tend to lean towards sharing and accept some security risks.	1	2	3	4	5
17	In general I'm aware of what our subordinate headquarters share with the ANSF (within my functional or geographical area of responsibility).	1	2	3	4	5

Please indicate to what extent you agree with the statements below by encircling the corresponding number.

Q	Statement	Strongly Agree	Agree	Uncertain	Disagree	Strongly Disagree
18	Intelligence collectors usually mark their information if further dissemination to the ANSF is permissible.	1	2	3	4	5
19	Nations usually mark their intelligence products if further dissemination to the ANSF is permissible.	1	2	3	4	5
20	ISAF has clear ethical standards for intelligence sharing with the ANSF.	1	2	3	4	5
21	I see few ethical problems with disseminating intelligence to the ANSF.	1	2	3	4	5
22	I don't believe ISAF provided intelligence fuel Afghan power struggles or otherwise cause civilian suffering.	1	2	3	4	5
23	I see few dilemmas between my professional ethics and ISAF's policy for intelligence sharing with the ANSF.	1	2	3	4	5
24	I sometimes feel pressured to share intelligence that I believe should be withheld on ethical reasons.	1	2	3	4	5
25	I'm afraid of making wrong judgements regarding intelligence sharing.	1	2	3	4	5

Q26: Please state any additional remarks or thoughts with reference to security aspects of disseminating intelligence to the ANSF (how, in your mind, security aspects influences or should influence ISAF's intelligence sharing).

.

_____

_____

_____

_____

Q27: Please state any additional remarks or thoughts with reference to multinational issues of disseminating intelligence to the ANSF (how, in your experience, multi-nationality influences ISAF's ability for intelligence sharing).

_____

_____

_____

_____

Q28: Please state any additional remarks or thoughts with reference to ethical issues of disseminating intelligence to the ANSF (how you feel ethics influences or should influence ISAF intelligence sharing).

_____

_____

_____

_____

Thank you for completing this questionnaire.