INTRA-MILITARY COMMUNICATION

THE EXCHANGE OF INFORMATION BETWEEN THE DUTCH PROVINCIAL RECONSTRUCTION TEAM AND PSYOPS SUPPORT ELEMENT IN URUZGAN, AFGHANISTAN

S. van der Klaauw, BSc

Masterthesis

Nijmegen School of Management
Radboud University Nijmegen

INTRA-MILITARY COMMUNICATION

THE EXCHANGE OF INFORMATION BETWEEN THE DUTCH PROVINCIAL RECONSTRUCTION TEAM AND PSYOPS SUPPORT ELEMENT IN URUZGAN, AFGHANISTAN

Sven van der Klaauw

Nijmegen School of Management

Radboud University Nijmegen

October 2010

Supervisors:

Thesis Supervisor:	Dr. B. Bomert	Radboud University Nijmegen
Second Reader:	Dr. Ir. S.J.H. Rietjens	Netherlands Defence Academy
Internship Supervisor:	Capt. J.P. Kessely	Royal Netherlands Army

S. van der Klaauw

Intra-Military Communication: The Exchange of Information between the Provincial Reconstruction Team and the PSYOPS Support Element

Masterthesis, Radboud University Nijmegen, Nijmegen

Photo on cover: Afghan Boy with Kite. Copyright © 2010 Martin Huydink

Grote Kerkhof 21f
7411 KV Deventer
The Netherland
Email: svenvanderklaauw@gmail.com

‘*The more elaborate*
our means of communication
the less we communicate.’

Joseph Priestley

ACKNOWLEDGEMENTS

Let me be honest. Now that my thesis is finished, I would have loved to say that I accomplished this all by myself. That I spent hours reading about things that are not in books. That I reviewed my work as critically as an outsider would. That I answered all the questions I had by myself. That I made good use of all the experience I have with counterinsurgencies, psychological operations, civil-military coordination, information exchange, communication, information management, methodology etc.

Although I certainly tried my best, I have to admit that a great number of people helped me conducting my research and pointed me in the right direction when I got lost. Therefore I would like to thank the following people for their contributions to this thesis.

First of all, this thesis would not have been without the help, advice and critical views of my supervisor Dr. B. Bomert and second reader Dr. ir. S.J.H. Rietjens. Both supported me from the start and read and corrected my work with a lot of constructive criticism.

My thanks also go to my former colleagues at the staff of the Royal Netherlands Army Command in Utrecht. Although Lieutenant-Colonel A. Koppe was deployed in Afghanistan for the first few months of my internship, he was so kind to offer me the internship last year. Major R. van Essen and Major P. Tomas were always willing to answer my questions and offered me an excellent insight into the military organization. Captain J.P. Kessely was so kind to supervise me during my stay in Utrecht. Thanks to him my time as an intern turned out to be a great success (at least from my point of view). Finally I want to thank Warrant Officer 1 E. Hoogendoorn for allowing me to have my desk opposite to his, as well as the great fun we had.

I would also like to thank my senior lecturers, Dr. W. Verkoren, Dr. H.van Houtum, Dr. J. van der Lijn, Dr. O. Kramsch, Ir. M. van Leeuwen and Dr. M. van der Velde for all the insights into conflict analysis and management and the sometimes surprising new views on what I considered trivial concepts.

My thanks also go to course director Captain J. Hausch, and instructors Lieutenant-Commander A. Maurreau and Warrant Officer M. Corstjens for their contribution to a very instructive NATO CIMIC Basic Course.

To Lieutenant-Commander C.M. van der Klaauw I would like to express my gratitude for giving me the inspiration to write this thesis on the subject of the exchange of information between the PRT and PSE as well as for sharing a lot of experiences and information.

I promised all the interviewees who were willing to share their knowledge and insights, to remain anonymous. However, without their contribution this thesis would be meaningless.

SUMMARY

During the last four years two of the most important military actors that focus on the mind-set of the population during a counterinsurgency campaign, were deployed in Afghanistan as part of the Dutch Task Force Uruzgan. The Provincial Reconstruction Team and the PSYOPS Support Element each had to work on winning the hearts and minds of the Afghan population. However, the exchange of information between the two units did not function as efficient as it should be. Individual actions were not coordinated and too little information was shared.

This thesis will therefore try to find an answer to the question how the exchange of information between the PRT and PSE can be improved. It will start by presenting an introduction on counter-insurgency and the importance of clear and well-functioning lines of communication between military units. In order to raise situational awareness, these actors need to communicate as much as possible on relevant and critical topics like security and safety issues in general, but also on their individual activities.

Next their mutual relations and their activities related to the exchange and management of information will be discussed together with the structures of the two units and their place in the organization of the Task Force Uruzgan, the concept of a PRT and PSE, their tasks and goals.

An instrument for analysis, based on various military and non-military models on information and intelligence management will be used to assess the exchange of information between March 2009 and March 2010. The model contains nine phases: the construction of an information goal, the formulation of an information need, the collection of information, the organization of information, the storage of information, a production phase, a distribution phase and a phase in which the information is used. This last phase is connected to the first one through a feedback loop (the ninth phase) which essentially makes it a cycle.

Although I have always been aware of the fact that the model I created would not be as easily applicable as I liked, another major outcome more or less divided the information management process into two individual (but connected) cycles: a staff cycle and a tactical cycle.

Through various interviews with PRT and PSE representatives I was able to identify the actual information flows within both the PSE and PRT. The interviews provided me with the information to schematically visualize these flows of information and investigate their effectiveness and efficiency accordingly. Five areas were then identified that hamper the process of information exchange: interpersonal relations, a need-to-know mentality, a lack of feedback, the use of private databases and capacity problems.

In order to solve these problems, or at least reduce their risk of affecting the exchange of information negatively, a couple of recommendations were formulated. A decentralized organizational structure can eventually confront the problem of suboptimal information sharing. Working in clusters, according to the network centric warfare theory, along vertical lines in a flatter hierarchy together with the right infostructure could lead to an improved battlespace awareness. Therefore I suggest to invest in a solid information infrastructure. Every team, every single member for that matter, needs to have access to a shared information database. Not only to improve his own awareness, but also to contribute to the alertness of others by contributing to it. It simply cannot be that information sharing gets hampered by a lack of collators or other technical deficiencies. Together with the introduction of a network centric mind-set and the construction of clusters of related actors this could improve the discontinuity of informal networking.

At the same time future colleagues need to be familiar with each other's activities. As I suggested, this should be done by introducing each other's field of work in combined exercises during the preparation phase. By introducing a feedback loop, the process as a whole, can be constantly monitored.

Keywords: Afghanistan, Uruzgan, Netherlands, Provincial Reconstruction Team, PSYOPS Support Element, Cooperation, Communication, Information Exchange.

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

> *Protecting the people is the mission. The conflict will be won by persuading the population, not by destroying the enemy.*[1]

Fighting an insurgency is a complex undertaking. It was T.E. Lawrence, commonly known as Lawrence of Arabia, who described it as eating soup with a knife.[2] In the opening quotations U.S. Army Command Sergeant Major Hall and U.S. Army General McChrystal, summarize the essence of counterinsurgency (COIN): It is all about persuading the people, winning their heart-and-minds. As with all complex military operations, there are many actors involved in counterinsurgency. Especially since the wars in Afghanistan and Iraq, the complexity of coordinating activities within the military and activities between the military and their civilian partners (including the local population) became clear. Numerous studies have been conducted on the last, but internal military coordination, especially in the field of winning hearts-and-minds, has earned little attention. Yet a (military) counterinsurgency operation functions best if both external and internal coordination runs efficient.

As I will show in more detail later on, counterinsurgency is a very complex type of irregular warfare. It is made up out of numerous different military and civil actors, ranging from government institutions to local leaders, all of which have their own unique activities to perform. Nevertheless, it is possible to distinguish particular activities and arrange these actions into several ‘groups of actions’. These clusters of activities are for instance: kinetic[3] actions directed against the insurgent groups or actions aimed at providing physical protection. But the non-kinetic activity of winning hearts-and-minds is considered a group of actions as well.[4] This set of actions aimed at increasing the support for and the legitimacy of the counterinsurgency operation makes use of so called, non-kinetic means. It is the coordination between these means I want to focus on. More specifically, I want to look at the two key military actions involved: Psychological Operations (PSYOPS) and Civil Military Cooperation (CIMIC). As I will demonstrate in the coming chapters, both actions are suited and used for raising support and legitimacy under the local population (the pivot of every counterinsurgency campaign). In practice these actions are part of the ISAF operation and the Dutch Task Force, in their capacity as the Psychological Support Element (PSE) and as an important part of the Provincial Reconstruction Team (PRT).

In a complex counterinsurgency environment, where multiple actors carry out their individual activities, coordination and cooperation can make a huge difference to the efficiency of the overall campaign. Besides that, information and intelligence are fundamental for a counterinsurgency campaign. A shared situational awareness is key in such a complex environment. However, when this level of coordination is not reached, and the exchange of information is insufficient, the smallest action can hamper the overall mission.

Let me give an example of failing intra-military communication that occurred during the Dutch presence in Afghanistan.

In their attempts to build confidence among the people of Afghanistan, both the PSE and PRT had goodies at their disposal (footballs, volleyballs, Frisbees, radios, blankets, etc). The

[1] Micheal T. Hall and Stanley A. McChrystal, *Isaf Commander's Counterinsurgency Guidance* (Kabul: International Security Assistance Force, 2009), 13.

[2] Thomas Edward Lawrence, *Seven Pillars of Wisdom* (London 1926)

[3] Kinetic action is military jargon for combat operations.

[4] I will discuss the groups of action in more depth later on. See for an overview of the different groups: Royal Netherlands Army, "Combat Operations Adp Ii - Part C: Combat Operations Againts an Irregular Force," ed. Ministery of Defence (The Hague: Royal Netherlands Army, 2003), 574.

PRT was not very selective when they handed out these goodies: they were used as conversation starters for example. At the same time however, the PSE distributed these goodies with another more specific goal in mind. Radios were handed out in order to see who were allowed to use them and who were not, in order to identify hierarchical patterns and pinpoint leaders within the communities. Handing out these goodies simultaneously by both the PRT and PSE frustrated these objectives. However, the radios were at the centre of another conflict.

For the use of the radios a certain amount of explanation was necessary to make sure that the local population was able to charge and tune them. The members of the PRT took care of this explanation themselves to guarantee that the receiver got a radio that worked. If, after a while, this radio stopped working, it could be changed for a new one.

Again the PSE had another approach. Not until they came back with questions about how to turn it on or how to tune in to the local radio program, did they provide the people with an explanation. Based on this response the PSE was able to check if the radio was used, and if the receiver knew how to operate it. Soon the local population learned that one has to turn to the PRT for a radio and not the ‘unhelpful’ PSE.

The different methods of handing out the radios, again frustrated the work of objectives of the PSE.

In addition to these rather specific examples there was also the problem of the local population getting the same questions from the PRT and PSE and in some cases the Field Human Intelligence (HUMINT) Teams.[5] Although this might not be identified as a major problem at first, in the long run it portrays the military actors as unorganised, intrusive and therefore unreliable; unwanted characterizations in an environment where one wants to persuade the people.

These examples show that at least some actions lack a decent level of coordination. Therefore this study will focus on the exchange of information between the PSE and the PRT. It is this first step (communication, the exchange of information) that should lead to coordination. In other words, without clear communication it is impossible to cooperate and coordinate.

In the coming chapters I will take look at how information runs through the (PRT and PSE) organizations. I will also identify at what point communication takes place or should take place, so that future operations can run more efficient and can have a greater impact on the ever-changing counterinsurgency environment.

1.1 Background

Since the involvement of U.S. and coalition forces in the wars in both Afghanistan and Iraq, counterinsurgency, (defined by NATO as the set of “paramilitary, political, economic, psychological, and civic actions taken to defeat insurgency”[6]) triggered a renewed interest in this particular area of warfare. However, insurgency (and counterinsurgency for that matter) is nothing new. The British for example, experienced an insurgency in Malaya, the French in Indochina and Algeria, the Dutch in the Dutch East Indies, the U.S. in Vietnam and the Russians in Afghanistan. However some of them soon forgot about the valuable lessons that they learned during that period.[7] For example the Americans made that mistake after the lost

[5] See for example Jelmar Den Boer, "Informatie-Uitwisseling Tussen Het Mission-Team, Tactical Pys-Ops Team En Het Field Humint Team" (Nederlandse Defensie Academie, 2008).
[6] NATO, "Aap-6 Nato Glossary of Terms and Definitions," ed. NATO Standardization Agency (Brussels: NATO, 2009), 2-C-18.
[7] Thijs W. Brocades Zaalberg, "'Hearts and Minds' of 'Search and Destroy'," *Militaire Spectator* 176, no. 7/8 (2007): 290.

war in Vietnam.[8] Less than thirty years later, the United States and the coalition forces got involved in another counterinsurgency campaign, this time in Afghanistan. Unfortunately it took a while before the parties involved realized that they were in the middle of a counterinsurgency again and that they should adjust their activities likewise. Since then an extensive amount of literature is written about counterinsurgency. Before I turn to counterinsurgency, its goals and its means, I want to take a quick look at what is basically the reason for a counterinsurgency: the insurgency itself.

1.1.1 Insurgency

The North Atlantic Treaty Organization (NATO) defines an insurgency as “an organised movement aimed at the overthrow of a constituted government through one of subversion and armed conflict”.[9] The Royal Netherlands Army uses a similar but more extensive definition. According to the Army Doctrine Publication (ADP) II, part C, Combat Operations Against an Irregular Force, the term insurgency is defined as:

> *an organised movement aiming to bring about political, economic or social change, through use of armed conflict by a faction (insurgent group) against the de facto authority or, in the absence of a functioning state or government, against the majority of the population, organised or otherwise.*[10]

However, in a 2007 doctrine report that will be used to rewrite this doctrine, another definition has been introduced. According to Doctrine bulletin 07/02, an insurgency is “a struggle for control over a contested political space. This struggle takes place between a ruling authority (usually a government) and one or more, popularly based, challengers”.[11] Although the NATO definition is mentioned, the authors of the Doctrine bulletin argue that reality forced them to use an alternative approach.

The alternative definition is based on the work of Lieutenant-Colonel David Kilcullen, one of the leading counterinsurgency specialists. In his article ‘Three Pillars of Counterinsurgency’, he defines an insurgency as “a struggle for control over a contested political space, between a state (or group of states or occupying powers), and one or more popularly based, non-state challengers”.[12]

When we take a look at for example the Dutch and U.S. definitions of insurgency, NATO’s definition (as formulated in 1980) has been a point of reference. All three definitions speak of an organised group or movement that wants to establish at least political change. The Dutch definition adds economic and social motives, whereas the NATO definition speaks more specifically about the act of overthrowing a government. The movements (‘the insurgents’) try to achieve their objectives through armed conflict and subversion (those

[8] Ibid.

[9] NATO, "Aap-6 Nato Glossary of Terms and Definitions," 2-I-5. The U.S. uses the same definition in their Joint Publication 3-24 Counterinsurgency. See: Department of Defense, "Joint Publication 3-24 Counterinsurgency Operations," ed. Department of Defense (Washington: Department of Defense, 2009), I-1.

[10] Royal Netherlands Army, "Combat Operations Adp Ii - Part C: Combat Operations Againts an Irregular Force," 481. Notice that the definition speaks of “a de facto authority”. This might not be a legitimate authority, or as the doctrine publication states: “This definition deliberately refers to the de facto authorities, as the authorities in question might not be recognised by all parties [...] How people regard this government authority makes a fundamental difference to the issue of legitimacy”. So the de facto authority may not be a legitimate authority, in which case the “legitimacy of the existing government is equally debatable”.

[11] Opleidings- en Trainingscentrum Operatiën, "Doctrinebulletin 07/02: Counter Insurgency (Coin) En De Militaire Bijdrage," (Amersfoort: Opleidings- en Trainingscommando, 2007), 3.

[12] David Kilcullen, "Three Pillars of Counterinsurgency," in *U.S. Government Counterinsurgency Conference* (Washington2006), 2.

actions designed to weaken the military, economic or political strength of a nation by undermining the morale, loyalty or reliability of its citizens).[13]

However, one needs to realize that contemporary insurgencies differ from the classic ones on which at least NATO's definition seems to be based. Kilcullen mentions some important differences in his 2006 article 'Counter-insurgency Redux'.[14] Not all insurgencies are covered by the notion that the insurgents challenge a functioning state. The insurgents might fight for ungoverned space (Chechnya, Somalia) or the insurgents pre-date the government (Afghanistan). The Dutch (ADP) definition states that the insurgents want to bring about political change. Instead, in several campaigns (Iraq, Afghanistan) invading forces introduced political change. Moreover, in many cases the counterinsurgents represent revolutionary change, "while the insurgent fights to preserve the status quo".[15] Another important effect is the rise of a worldwide audience, due to improved information and communication technologies. The internet turns out to be an ideal medium to publicize a cause. Furthermore, modern-day insurgencies might not even aim at replacing an existing government, they rather seek to "paralyse and fragment a state" or the try to exhaust an occupying force.[16] Another flaw in classic counterinsurgency theory suggests that there is some kind of "binary struggle between insurgent and counter-insurgent"[17], while in fact there might be multiple insurgent movements or external factors involved.

Contemporary insurgencies do have some specific characteristics that are not covered by the older definition. Because of these differences I found it useful to use Kilcullen's instead of NATO's definition. The more elegant definition by Kilcullen (following Gordon H. McCormick[18]) does take the present developments into account. Therefore, I will refer to his definition of an insurgency, unless explicitly indicated otherwise.

1.1.2 Suppressing an insurgency

The fight against an insurgency cannot be won by the use of brute (military) force. The aforementioned historical events (e.g. Indochina, Dutch East Indies, Vietnam) show that it is very hard to fight an insurgency successfully, without using a delicate mixture of both military and non-military action. The British for example did use such a combination in Malaya, and successfully countered the communist guerrillas. Before I take a closer look at the basic elements of a successful counterinsurgency campaign, again a definition might be useful.

A very basic definition of a *counter*-insurgency introduced by David Kilcullen, reads "all measures adopted to suppress an insurgency".[19] This is of course a correct, but a rather unworkable definition; it does not really specify anything. Nevertheless NATO defines a counterinsurgency only slightly more specific. According to its glossary of terms and definitions, a counterinsurgency is defined as "those military, paramilitary, political, economic, psychological, and civic actions taken to defeat insurgency".[20] It basically only specifies the potential means. The Dutch Army Doctrine Publication (ADP) does not give a definition of counterinsurgency at all, but states that it includes "measures in the diplomatic, civil-government, political-legal, social, cultural, psychological and economic domains".[21]

[13] NATO, "Aap-6 Nato Glossary of Terms and Definitions," 2-S-14.
[14] David Kilcullen, "Counterinsurgency Redux," *Survival* 48, no. 4 (2006): 112-14.
[15] Ibid.: 113.
[16] Ibid.: 115.
[17] Ibid.: 116.
[18] Gordon H. McCormick, "Things Fall Apart: The 'Endgame Dynamics of Internal Wars'," (RAND), 2.
[19] Kilcullen, "Counterinsurgency Redux," 112.
[20] NATO, "Aap-6 Nato Glossary of Terms and Definitions," 2-C-18.
[21] Royal Netherlands Army, "Combat Operations Adp Ii - Part C: Combat Operations Againts an Irregular Force," 487.

The Doctrine Bulletin 07/02 that will be used to write a new doctrine refers to the NATO definition.[22]

The lack of a clear definition shows that the implementation of counterinsurgency is something that almost completely depends on the situation (i.e. the insurgency). However, the definitions give some starting points regarding the possible means. So does the U.S. Joint Doctrine description of counterinsurgency:

> *"COIN is comprehensive civilian and military efforts taken to defeat an insurgency and to address any core grievances [...] COIN is primarily political and incorporates a wide range of activities, of which security is only one".*[23]

Although I will refer to the NATO definition of counterinsurgency in the coming chapters (unless indicated otherwise), the U.S. Joint Doctrine definition points out a very important notion: counterinsurgency is primarily political. David Galula once mentioned that counterinsurgency is "80% political, 20% military".[24] But recent developments tended some scholars to state that COIN "may now be 100% political".[25] According to David Kilcullen, in our time "perceptions and political outcomes matter more than battlefield success".[26] In fact, because of globalization and the role of information the classic paradigm of COIN shifts towards a more global, perception- and information-based, notion.

In the fight over political power, both the insurgents and the counterinsurgents aim to get the people to accept its governance of authority as legitimate (Figure 1).

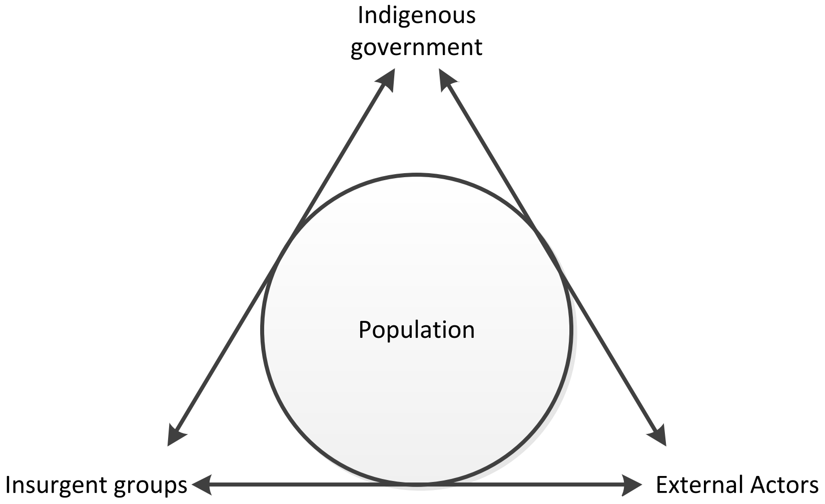


Figure 1 Counterinsurgency Framework[27]

The three main actors - the indigenous government, the insurgent groups and the external actors (foreign forces, terrorist networks etc.) - all fight over the favour of the population, not only because the support of the people legitimizes their actions, but they might also (voluntarily or forced by the insurgents) offer them assistance (money, logistics, recruits,

[22] Opleidings- en Trainingscentrum Operatiën, "Doctrinebulletin 07/02: Counter Insurgency (Coin) En De Militaire Bijdrage," 7.

[23] Department of Defense, "Joint Publication 3-24 Counterinsurgency Operations," I-2.

[24] David Galula, *Counterinsurgency Warfare: Theory and Practice* (London: Pall Mall, 1964), 89.

[25] Kilcullen, "Counterinsurgency Redux," 123.

[26] Ibid.

[27] After Jones, *Counterinsurgency in Afghanistan,* 12.

intelligence and other aid).[28] When we take a closer look at the population it becomes clear that it is generally made up out of three groups: a minority in favour of the cause, a minority against the cause and a passive or neutral majority. Eventually every major actor wants to win the majority of the population for its cause.

Based on the recent developments mentioned earlier, Kilcullen broadens the scope of popular support. “In modern day counter-insurgency, the side may win which best mobilises and energises its global, regional and local support base – and prevents its adversaries doing likewise”.[29] Instead of only relying on local popular support, both insurgents and counterinsurgents rely on their ability to mobilize supporters globally as well as locally. Counterinsurgents “must mobilise the home population, the host country, the global audience, the populations of allied and neutral countries, and the military and government agencies”.[30]

1.1.3 Multiple Actors

As indicated before, the various definitions of counterinsurgency show some important things. First of all, the nature of counterinsurgency is not fixed: “it evolves in response to changes in insurgency”, and therefore “there is no constant set of operational techniques” and thus no specific definition.[31] Second, counterinsurgency campaigns are not an exclusively military affair. In fact it involves a great number of political and civil actors as well. To mention but a few of the numerous possible participants in a counterinsurgency campaign:

- Military forces, including Host Nation (HN) forces
- Government agencies
- Nongovernmental organizations (NGOs)
- Intergovernmental organizations (IGOs)
- Multinational corporations and contractors
- HN civil and military authorities (including local leaders)[32]
- The public opinion (both ‘at home’ and abroad)

While the insurgents use all available tools to overthrow the existing (or newly introduced) authority, the counterinsurgents try to sustain an established or emerging government. To achieve this objective, not only safety and security is needed, the government might also need help in order to establish rule of law, economic growth, social services. “COIN thus involves the application of national power in the political, military, economic, social, information, and infrastructure fields and disciplines”.[33]

1.1.4 Counterinsurgency and the Military

In his article ‘Three Pillars of Counterinsurgency’, David Kilcullen introduces a framework for inter-agency counterinsurgency operations in which he distinguishes three pillars: a political pillar, an economic pillar and a security pillar. The first one focuses on mobilizing support for the government, extending its boundaries and building institutional capacity. The economic pillar includes humanitarian relief, development assistance, infrastructure management. The security pillar is where the military comes in (together with

[28] Seth G. Jones, *Counterinsurgency in Afghanistan*, vol. 4, Rand Counterinsurgency Study (Santa Monica: RAND Corporation, 2008), 12.

[29] Kilcullen, "Counterinsurgency Redux," 121.

[30] Ibid.

[31] Ibid.: 12.

[32] Department of the Army, "Field Manual 3-24 Counterinsurgency," ed. Department of the Army (Washington: Department of the Army, 2006), 2-2.

[33] Ibid., 1-1.

for example the police, private security companies or paramilitary organizations). It comprises police security, human security and military security, in order to secure "the population from attack or intimidation by guerrillas, bandits, terrorists or other armed groups".[34]

The pillars are based on a foundation of information that is the starting point for all other activities in an inter-agency COIN campaign.[35] In order to gain control (the overarching objective) over the "overall socio-political space", all actors (the security, political and economic pillar) should be supported by a common information strategy. Because today's COIN operations are aimed at influencing the perception of the population, a unified message should be send by the three pillars based on this information strategy. It includes "intelligence [or information] collection, analysis and distribution, information operations, media operations […] efforts to understand the environment […] understanding the effects of our operations on the population, adversaries and the environment".[36] This is where the PSYOPS and CIMIC activities are situated.

Kilcullen only introduces a model, a "basis for further development". He does not elaborate on the role and activities of the military in a counterinsurgency campaign; his thoughts only are only a rough idea of the role and the objectives of the military.

The concept of Network Centric Warfare (or NCW) however, offers a more concrete line of thought, especially on the military organization during a counterinsurgency.

In the last two decades this new kind of organizational thought was introduced in the civil (business) environment. Because of dynamic, turbulent and ever changing market demands commercial companies needed to respond quickly.[37] This situation, together with an enormous growth in information technology, led to the introduction of decentralized, team-based, and distributed structures.[38]

As a matter of fact, insurgencies pose similar threats to a military organization: insurgencies are turbulent, dynamic and in some cases even chaotic. These unstable environments demand novel structures.[39]

Therefore, recent military thinking has started to develop itself in the same direction of decentralized, network-based operations, called 'network centric warfare', 'network enabled warfare' or 'power to the edge'.[40] These new organizational forms are structured horizontally rather than functionally or vertically and they are referred to as "modular, cluster, learning, network, or perpetual matrix organization, spinout or virtual corporations".[41] Daft and Lewin describe these organizations as flatter hierarchies, with decentralized decision-making, a greater capacity for tolerance of ambiguity, permeable internal and external boundaries, the empowerment of employees ('power to the edge'), the capacity for renewal, with self-organizing units and self-integrating coordination mechanisms.[42]

[34] Kilcullen, "Three Pillars of Counterinsurgency," 5.
[35] Ibid., 4-5.
[36] Ibid., 5.
[37] S.L. Brown and K.M. Esienhardt, *Competing on the Edge: Strategy as Structured Chaos* (Boston: Harvard Business School Press, 1998).
[38] Jan Maarten Schraagen, Mirjam Huis in 't Veld, and Lisette De Koning, "Information Sharing During Crisis Management in Hierarchical Vs. Network Teams," *Journal of Contingencies and Crisis Management* 18, no. 2 (2010).
[39] Ibid.: 117.
[40] D.S. Alberts and R.E. Hayes, *Power Top the Edge: Command... Control... In the Information Age* (Washington: CCRP, 2003). D.S. Alberts, J.J. Garstka, and F.P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington: CCRP, 2000).
[41] Leoni Warne et al., *The Network Centric Warrior: The Human Dimension of Network Centric Warfare* (Edinburgh: DSTO Information Sciences Laboratory, 2004), 3.
[42] R.L. Daft and A.Y. Lewin, "Where Are the Theories for The "New" Organizational Forms? An Editorial Essay," *Organzation Science* 4(1993).

According to Alberts, Garstka and Stein "NCW focuses on the combat power that can be generated from the effective linking or networking of the warfighting enterprise".[43] This end state is reached through five different phases (Figure 2).

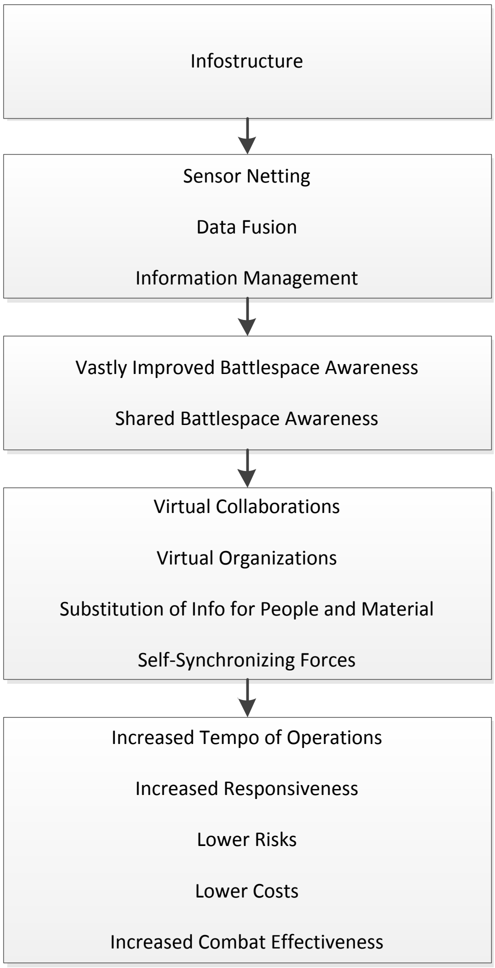

Infostructure
Sensor Netting
Data Fusion
Information Management
Vastly Improved Battlespace Awareness
Shared Battlespace Awareness
Virtual Collaborations
Virtual Organizations
Substitution of Info for People and Material
Self-Synchronizing Forces
Increased Tempo of Operations
Increased Responsiveness
Lower Risks
Lower Costs
Increased Combat Effectiveness

Figure 2 Network Centric Warfare[44]

Increased combat effectiveness starts with the right information infrastructure or 'infostructure': information technology that supports the process of sharing and exchanging information. It enables the different sensors to link to each other and fuse their data. Together with proper information management this leads to an improved battlespace awareness. The improved and shared awareness will allow virtual collaboration to exist as well as a virtual (or network) organizations.

The idea of NCW is taken seriously within the military. However, a fully shared awareness is not yet reached. As a matter of fact, some of the problems indicated in one of the previous paragraphs indicate that information management and data fusion (second phase in Figure 2) can still be improved.

If we want to know what the current state of affairs is and which tools the military uses to achieve these goals, we need to take a look at the doctrine again and the 'groups of actions' that it distinguishes.

[43] Alberts, Garstka, and Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*.
[44] Ibid.

1.1.5 Groups of Actions

The Dutch doctrine on combat operations against irregular warfare distinguishes five groups of actions in counterinsurgency operations.[45] The first is aimed at the insurgents: restricting their freedom of movement, cutting of their supply routes and eliminating the insurgents. Obviously this is a military and police function. The second group of actions is aimed at providing the population with physical protection and aims to divide the insurgents and population. The third group of actions focuses on the external support of the insurgents. The fourth group of actions is focussed on the mind-set of the population. The aim is to gain legitimacy for the counterinsurgency operation and support among the population. A fifth group of actions is aimed at providing the own troops and friendly personnel (including NGOs and IOs) with safety in order to retain freedom of movement.

In this thesis I want to focus on the fourth group of actions, that could be described as those actions aimed at 'winning the hearts and minds'. Although the concept of 'hearts-and-minds' in relation to counterinsurgency is frequently used in popular media, the Dutch army doctrine on combat operations against an irregular force uses the term to describe a certain type of operation:

> *In a broad sense, the hearts-and-minds operation is a government-led operation in which political, economic, social and military measures should be used to complement each other. More specifically, the hearts-and-minds operation is a military activity that is conducted in conjunction with other activities.*[46]

The role of the military, apart from providing security by deploying regular forces, consists of other so called 'non-kinetic' activities[47]:

- Psychological Operations (PSYOPS)
- Civil-Military Cooperation (CIMIC)
- Public information (PI)

In the next paragraphs I will take a closer look at these activities and introduce a difference between PSYOPS and CIMIC on the one hand and PI on the other.

1.1.6 Psychological Operations (PSYOPS)

Before I turn to the definition of PSYOPS as expressed by the Royal Netherlands Army in its Doctrine, I want to take a look at NATO's characterization of PSYOPS. Since 2002 there have been two NATO Allied Joint Publications (AJP) on Psychological Operations. The first one, AJP 3.7, describes PSYOPS as:

> *Planned psychological activities in peace, crisis and war directed to enemy, friendly and neutral audiences in order to influence attitudes and behavior affecting the achievement of political and military objectives.*[48]

In 2005 AJP 3.7 was followed by AJP 10.1 in which the same definition is used as expressed in the 2003, MC 402/1 NATO Military Policy on Psychological Operations:

[45] Royal Netherlands Army, "Combat Operations Adp Ii - Part C: Combat Operations Againts an Irregular Force," 574.
[46] Ibid., 685.
[47] Ibid.
[48] NATO, "Ajp-3.7 Nato Psychological Operations," ed. NATO (Brussels: NATO, 2002), 1-1.

> *Planned psychological activities using methods of communications and other means directed to approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives.*[49]

The Dutch Army Doctrine Publication (ADP) II-C defines PSYOPS according to the previous NATO description.[50] However, in a 2006 document on a Dutch PSYOPS policy, the 'new' NATO definition is used. In the next chapters I will refer to the current NATO PSYOPS definition.

The objectives, formulated in the definition, are met through at least four basic functions.[51] First, PSYOPS will be involved in face-to-face activities in order to gather information about fears and needs or information for the benefit of future (psychological) activities. As I will show in chapter 4, this information is of great importance for the target audience analysts. Second, PSYOPS also includes the spreading of information through so called PSYOPS products: pamphlets, newspapers, posters, goodies and radio stations. These products contain psychological messages but are also used to establish contact with the target audience. Third, PSYOPS will evaluate the effectiveness of their actions through pre- and post-tests. Fourth, PSYOPS units are also able to inform a target audience by using loudspeakers, for example to introduce a unit that enters a certain area.

1.1.7 Civil-Military Cooperation (CIMIC)

In NATO's Allied Joint Publication 9 (A) [52], CIMIC is defined as:

> *"The coordination and cooperation, in support of the mission, between NATO Commander and civil actors, including national population and local authorities, as well as international, national and non-governmental organizations and agencies"*[53]

CIMIC has three main tasks: civil-military liaison, support to the force and support to the civil environment.[54]

Civil-Military Liaison is conducted in order to establish and maintain the necessary coordination between the military and local, national and international authorities and NGOs/IOs, to facilitate and support the planning and conduct of operation. At the same time liaison contributes to situational awareness. Through the various contacts with civil organisations and institutions information about the environment is shared and thus contributes to a better understanding of the area in which CIMIC activities take place.

Support of the force is the second function of CIMIC. Through their contacts CIMIC personnel can provide a commander with knowledge about the civil environment on which he can base his decisions. CIMIC provides the opportunity for the commander to identify

[49] ———, "Mc 402/1 Nato Military Policy on Psychological Operations," ed. North Atlantic Military Committee (Brussels: NATO, 2003), 2.

[50] "... planned psychological activities in times of peace, crisis and war, directed at hostile, friendly and neutral parties with the intention of influencing the attitudes and behaviour which affect the established political and military objectives". Royal Netherlands Army, "Combat Operations Adp Ii - Part C: Combat Operations Againts an Irregular Force," 687.

[51] P.J.J. Tiggelman, "Psychologische Operaties: Treffers Zonder Met Scherp Te Schieten," ed. Koninklijke Landmacht (Utrecht: Koninklijke Landmacht, 2006), 15.

[52] Although the new AJP-9 is still a ratification draft its CIMIC definition is widely used. The definition is left unchanged. Because there is no national CIMIC doctrine available, NATO's definition is used in Dutch publications. See: NATO, "Ajp-9 Nato Civil Military Co-Operation (Cimic)," ed. NATO (Brussels: NATO, 2003), 1-1.

[53] ———, "Ajp-9(a) Nato Civil Military Co-Operation (Cimic)," ed. NATO (Brussels: NATO), 1-3.

[54] ———, "Ajp-9 Nato Civil Military Co-Operation (Cimic)."; Koninklijke Landmacht, "Vs 2-1353 Handboek Cimic," ed. Ministerie van Defensie (The Haque: Koninklijke Landmacht, 2002).; J. Van der Woerdt, "Toelichting Op De Rol Van Cimic in Militaire Operaties," ed. Ministerie van Defensie (The Hague: Ministerie van Defensie, 2007).

potential problems within the civil environment and take measures accordingly. At the same time CIMIC activities can be used in order to raise support for the presence of the force. As has been said before, especially during a counterinsurgency campaign force, acceptance is very important.

A third CIMIC function is support to the civil environment, in concordance with the (NATO) military mission.[55] One could think of providing information, personnel, material, equipment, communication facilities, specialist expertise or training. It is important however, that these supportive measures are only taken "where and when it is required to create conditions necessary for the fulfilment of the military mission" or because the task cannot be carried out by the appropriate civil authorities and agencies.[56]

1.1.8 Public Information (PI)

Although Public Information is an important part of the hearts-and-minds strategy, it differs from PSYOPS and CIMIC to a great extent.

> *Public Information is defined as information, which is released or published for the primary purpose of keeping the public fully informed, thereby gaining their understanding and support.*[57]

PI's objective is to inform the general public about the (military) activities. Contrary to PSYOPS, the aim is to provide as much information as possible in order to allow the public (the media and citizens of the countries concerned) to make their own judgement as independently as possible. "Scrupulous care should be taken, therefore, to avoid any propaganda connotations".[58]

Another major difference is that PSYOPS and CIMIC (together with Electronic Warfare, Command and Control Warfare and Computer Network Operations) fall under the broader concept of Information Operations (InfoOps): "actions taken to influence decision-making of adversaries in support of the Alliance overall objectives by affecting their information, information-based processes and systems while exploiting and protecting one's own".[59] InfoOps are limited in time (crisis management and war) and target (adversaries' public or decision makers). PI however is not focussed on a specific target audience. It informs all audiences at any time, again as independently as possible.

Although objectives and mandate differ significantly, PSYOPS and CIMIC on the one hand and PI on the other have also some common grounds. PSYOPS and PI make use of the same techniques and means to get a (sometimes similar) message out. Therefore integration of these activities matters greatly.[60] Both CIMIC and PSYOPS, as well as PI interact with the civil environment. However, because PSYOPS and CIMIC are both activities that are directed against adversaries and can be used to influence them, this thesis focuses on the cooperation and exchange of information between these two actors. As I said before, they target the same audiences, are part of InfoOps and operate under the same circumstances (crises and war).

[55] NATO, "Ajp-9 Nato Civil Military Co-Operation (Cimic)," 1-4.
[56] Ibid.
[57] ———, "Mc 457 Nato Military Policy on Public Information," ed. North Atlantic Military Committee (Brussels: NATO, 2001), 1-1.
[58] Ibid., 1-8.
[59] ———, "Mc 422/1 Nato Military Policy on Information Operations," ed. North Atlantic Military Committee (Brussels: NATO, 2002), 1-2.
[60] Van der Woerdt, "Toelichting Op De Rol Van Cimic in Militaire Operaties," 3.

1.2 Research objectives

As I indicated earlier I will look at CIMIC and PSYOPS in their capacity as Provincial Reconstruction Team and PSYOPS Support Element. Therefore the objective of this research is formulated as follows:

> *The goal of this research is to offer insight into and recommendation on the exchange of information between the PSE and the PRT, by analysing their mutual relations and their activities related to the information management process.*

1.3 Research questions

In the first paragraph of this chapter several problems between the PRT and PSE, concerning communication and cooperation, were mentioned. Activities were not coordinated and information gathered during patrols was not efficiently shared. Therefore I identified the lack of information exchange as a serious problem that could eventually hamper the overall mission. The main research question is based on this observation.

The main research question is:

> *How can the exchange of information between the PSE and the PRT be improved?*

In order to answer this question the following sub-questions have been formulated:

1. *What instrument for analysis can be developed (based on information management theory) to assess the exchange of information?*
2. *What are the characteristics and working-methods of the PRT and the PSE?*
3. *How can the instrument for analysis (formulated in the answer to sub-question 1) be applied in the case of the PRT and the PSE operations between March 2009, when the PRT became civilian led, and March 2010?*
4. *How is the internal management of information between March 2009 and March 2010 being assessed by those directly involved?*
5. *How is the exchange of information (the external flow of information) between March 2009 and March 2010 being assessed?*
6. *What recommendations can be made based on the analysis of the internal and external management of information in order to improve the exchange of information?*

1.4 Research strategy and approach

This study is based upon the case of the PRT and PSE as part of the Task Force Uruzgan between March 2009 and March 2010. In order to conduct this research I have first developed an instrument in order to analyse the exchange of information. The existing literature on information management has been the main source for an information sharing model. A combination of models from both military and civil information management is used to design a chain of processes that can be used to analyse the current situation.

Next, I have identified how the PRT and PSE operate. In order to apply the model a thorough understanding of the organization of these elements was needed. Official documents together with information from those who worked in these elements provided that information. This data is used to see how the information management model can be applied to the situation (i.e. the exchange of information between the PSE and PRT). In addition to this model, I have used the experiences of the persons involved in both the PSYOPS Support Elements (PSEs) and the Provincial Reconstruction Teams (PRTs) that I collected through interviews.

The interviews were semi-structured. This allowed the researcher a reasonable amount of freedom to ask additional questions that have not been anticipated at the beginning of the interview, to give explanation, ask for clarification if the answer is not clear or to prompt the respondent to elucidate further if necessary. The group of experts that I have consulted to gather the information in order to draw a picture on the actual cooperation on the exchange of information consists of both PSE and PRT members, together with staff members of Regional Command South (RC-S) and Task Force Uruzgan (TFU) who served from March 2009 till March 2010.

The organization and structure of the two elements, together with the experiences of former members have formed the basis on which the model can be applied. The differences between the model and the process in practice were used to formulate recommendations.

1.5 Social and scientific relevance

In one of the previous paragraphs a couple of practical problems were introduced. These range from leaving an unorganised impression on the local population by posing the same questions over and over up to severely hampering each other's activities. All because of bad communication. The actors were not properly informed on each other's objectives and apparently did not share information that was collected previously. By studying the exchange of information between two of the central players in so-called hearts-and-minds operations, efficient use of these COIN methods can be improved: the success of individual operations can be enhanced and in the end the mission as a whole (now and in the future) can become more efficient, effective and successful. However, not only the military will benefit from these improvements. Eventually all involved in a counterinsurgency situation (the local population, the local government, NGO's and IO's etc) will benefit from close cooperation and an efficient partner.

Although there has been some research on the subject, most studies only dealt with parts of the problem or focussed on foreign military forces[61]. A study that focuses on information exchange between Dutch military actors exclusively will therefore enrich the knowledge already existing. It will not only test the applicability of the existing (information management) theories in a specific military environment, it will hopefully also adjust these theories where necessary and enrich the existing knowledge on what forms the foundation of military cooperation.

1.6 Validity and reliability

The external validity of this study is guaranteed by applying method and data source triangulation. During research, two methods for collecting information were used: documentation and interviews. Information acquired through written sources could be validated with the help of interviews and vice versa. In order to secure the validity and reliability of the information sources multiple interviews with different people about similar

[61] See for example: Sebastiaan J. H. Rietjens et al., "Inter-Organisational Communication Iin Civil-Military Cooperation During Complex Emergencies: A Case Study in Afghanistan," *Distasters* 33, no. 3 (2008).

subjects and different written sources on the same subjects resulted in data source triangulation.

By applying these methods the outcomes of this study will be applicable to not only the members I have interviewed, but to the Dutch Provincial Reconstruction Teams and Psychological Support Elements that operated in Afghanistan between March 2009 and March 2010 in general.

1.7 Demarcation of the study

In this research I will study the exchange of information between the PSYOPS Support Element (PSE) and Provincial Reconstruction Team (PRT) as the primary representatives of CIMIC and PSYOPS from March 2009 until March 2010. This time span is chosen because the PRT became civilian led as from March 2009. From that moment on, the Provincial Reconstruction Team is being led by a civilian representative (CIVREP): a civil servant from the Dutch Ministry of Foreign Affairs. The PSE remained part of the military led TFU. As I will show in much more detail later, the official organizational structured changed significantly. Instead of a sub-unit, the PRT became a coordinate unit, right next to the Task Force Uruzgan.

I will also make an important distinction between the concept of civil-military cooperation and the provincial reconstruction team: the PRT is not CIMIC and CIMIC is not a PRT. Civil-military cooperation can be one of the activities of a PRT, but a PRT can also be tasked with other activities that are not directly related to establishing good civil-military relations. The civil section (i.e. the political advisor, development advisor etc.) of the PRT will therefore not be part of this research, nor will the Police Mentoring Team.

1.8 Research structure

In the next chapter I will introduce the PRT. The concept, purpose, structure, management and implementation of the a PRT will be taken up, according to both NATO's concept and the Dutch policy. In Chapter 3 the PSE and the concept of psychological operations is discussed. Again, key definitions are offered and the structure of the PSYOPS Support Element is provided.

In Chapter 4 the theoretical model that I will use to map and analyse the internal and external information flows, within and between the PRT and PSE, will be introduced. However, before this model can be created a short introduction to information and information management will be provided. Key concepts like data, information, knowledge, intelligence and communication will be defined.

Next I will introduce the case for applying the information management model: the Dutch PSE and PRT from March 2009 till March 2010. The information from the previous chapters, combined with the results of the interviews the communication (i.e. the exchange of information) and cooperation between the PRT and PSE will be described. At the same time the model, designed in Chapter 4, will be applied to the situation. The outcomes of this comparison between theory and practice will be presented at the end of the chapter.

The result from Chapter 5 will be further discussed and based on this discussion, recommendation on how to improve the exchange of information between the PRT and PSE will be made. This concluding chapter also sums up the most important conclusions and presents ideas for future research.

2 PROVINCIAL RECONSTRUCTION TEAM

> *The PRT is scaffolding – it is an interim structure designed to support Afghan government and security structures build their capacity to govern and deliver essential public services, such as security, law and order, justice, health care, education, development and so on.*[62]

The purpose of a Provincial Reconstruction Team is well illustrated by the quote from the ISAF PRT Handbook. However, to fully grasp the idea of the PRT we need to take a closer look at the concept. In this chapter I will show the guiding principles and the purpose of a PRT, the role of civil-military cooperation and the way a PRT is managed and structured.

Because the Dutch approach to a PRT is embedded in both international principles and Dutch policy frameworks, I will start by introducing the PRT concept as publicized in NATO's ISAF PRT Handbook. This handbook contains the main international guiding principles for all NATO PRTs in Afghanistan. Thereafter I will describe the Dutch PRT characteristics in more detail.

2.1 NATO's PRT

The PRT concept was developed and first used by U.S. forces during Operation Enduring Freedom (OEF) in Afghanistan in 2002. Its objectives were to create security and stability, to expand the reach of the Afghan authorities and to support reconstruction and development.[63] Since then, NATO copied the idea of a PRT, and its member states integrated it into their military organizations. Although the OEF PRTs were used as short term, non-kinetic military instruments to counter an insurgency, NATO's PRTs are different. According to NATO a PRT has a slightly bigger role to play: PRTs should help to extend the reach of the Afghan government. As of March 2010 there are 27 PRT in Afghanistan operated by more than a dozen different nations (some operating on more than one PRT at a time). In order to make sure that these PRTs were based on a consistent and coherent approach, NATO decided to come up with an ISAF PRT handbook. By introducing this manual it seeks to ensure a set of common objectives and increased convergence between the activities of all PRTs.[64] It thus provides us with some useful concepts and guidelines in order to get an idea of what a PRT should look like.

2.1.1 Concept and Purpose

When we look at the definition of a PRT as given by the ISAF handbook, we can immediately identify it as an organization dominated by civil-military relations: "A PRT is a joint, integrated *military-civilian* organization, staffed and supported by ISAF member countries, operating at the provincial level within Afghanistan [italics added]".[65] The contact between the military and its civilian counterparts is described in more detail in the mission statement of the PRT as it is stated in the ISAF Operational Plan:

[62] International Security Assistance Force, *Provincial Reconstruction Team Handbook* (Kabul: International Security Assistance Force,, 2009), 8.

[63] Ministerie van Defensie, "Joint Doctrine Bulletin 2008/01: "Provincial Reconstruction Teams" Inzet in Afghanistan," ed. Ministerie van Defensie (The Hague2008), 1.

[64] International Security Assistance Force, *Provincial Reconstruction Team Handbook*, 1.

[65] Ibid., 4.

> *[PRTs] will assist The Islamic Republic of Afghanistan to extend its authority, in order to facilitate the development of a stable and secure environment in the identified area of operations, and enable Security Sector Reform (SSR) and reconstruction efforts.*[66]

A PRT should create an environment that is stable enough for the government authorities, international organizations (IOs), non-governmental organizations (NGOs) and civil society to start the political transition process, the reconstruction and development work and economic development.[67] By doing so, it is almost unavoidable to run into civilian actors such as local authorities, national or international organizations. Therefore the PRT's initial task is to merge civilian and military efforts to enable security, governance and development. Furthermore, a PRT can offer to mediate, initiate meetings and share information with the civil actors. A civil-military 'hub' around which the PRT can operate is provided by CIMIC and CIMIC trained officers.

Now when should a PRT enter the scene? In the early stages of a conflict, the security situation might not allow a reconstruction team in the area seriously compromising its freedom of movement. Without a relatively secure situation, a PRT cannot fulfil its objectives. Then again, on the other side of the spectrum, in an environment that is secure enough for IOs, NGOs and other development agencies to do their work independently from the military, a PRT is unnecessary. As Figure 3 shows, the best moment to introduce a PRT is in-between these situations.

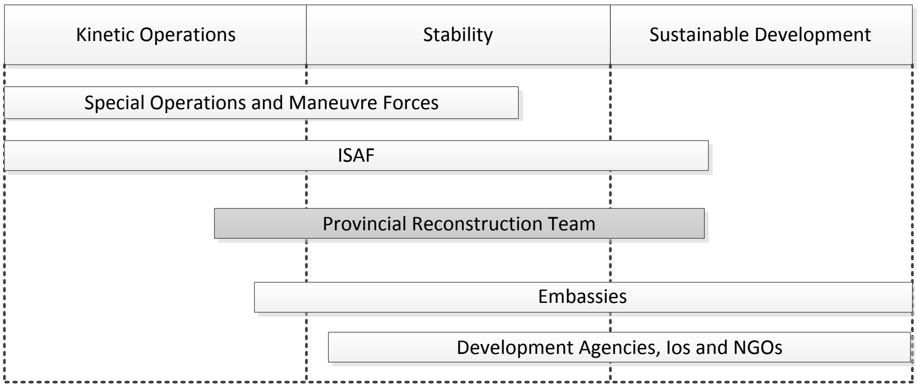

Kinetic Operations
Stability
Sustainable Development
Special Operations and Maneuvre Forces
ISAF
Provincial Reconstruction Team
Embassies
Development Agencies, Ios and NGOs

Figure 3 Spectrum of Intervention[68]

Based on the knowledge of the civil-military component, one can easily argue why a PRT should be established during the stability phase: this is the time when civil organizations and institutions enter the scene. In order to for example coordinate joint activities or avoid duplication of efforts, a relatively large amount of civil-military communication is necessary.

2.1.2 PRT's Structure

In 2003, when only three (Operation Enduring Freedom) PRTs were active in Afghanistan, these teams consisted mainly of military personnel. However, best practices show that the most successful PRTs involve both a civilian and military component.[69] According to the PRT Handbook, a team should have an integrated command group,

[66] Ibid., 3.
[67] Ibid., 4.
[68] Ibid., 5.
[69] Ibid., 272.

composed of senior military and civilian officials. “Without an integrated command group, a PRT will be unable to harmonise the diplomatic, economic and military lines of operation and will fail to act with unity of effort”.[70] And indeed, in the years following, most PRTs became more and more civilian. The size of both the military and civilian component however could vary based on for example the security situation, the effectiveness of governance institutions or the status of reconstruction.

In addition to an integrated command group, a PRT can include key leaders such as a diplomatic officer, a development officer, a police officer, other civilian experts. A deputy commander and a chief of staff are part of the integrated military command. The specific composition of PRTs differ however, according to which lead nation (LN) commands them. Nevertheless, the general structure includes civilian experts and a small group of security forces in order to provide force protection. The next paragraph shows the Dutch interpretation.

2.2 The Dutch PRT

In addition to the abovementioned international documents, the Netherlands’ approach to its PRT operations is embedded in Dutch policy frameworks. In those frameworks, the so-called 3D approach is key. All activities in the field of Defence, Diplomacy and Development should be coordinated as closely as possible to maximize unity and minimize duplication of efforts.[71] The 3D approach will therefore be a returning concept.

2.2.1 Dutch PRT Policy

Starting point for all ISAF operations (including the Dutch) is the JFC Brunssum Operation plan (OPLAN) 30302. The NL CHOD OPLAN 11415 lays down the plan for the execution of the operation by the Netherlands. Yet a more comprehensive document is the 2006 Civil Assessment on Uruzgan province, prepared by the Royal Dutch Embassy in Kabul. In the assessment, the Dutch approach is defined by five key elements. The immediate objective of the Dutch intervention is “to develop positive relations with the leaders and population at large in the Uruzgan province” to build a secure environment, to achieve visible development results and to create a stable institutional environment. Therefore all reconstruction and development should be aimed at promoting Afghan ownership, improving central, provincial and district governments and enhancing legitimacy. Next, aid and humanitarian assistance must be delivered on the basis of established needs. At the same time the PRT needs to make sure that infrastructure work should not enable insurgents to undermine the security. Last, all interventions should be formulated in dialogue with different partners and at different levels: the Afghan security forces, provincial and district administrations, government institutions, village committees, tribal elders, civil society, NGOs and other actors in the province.[72]

The mode of operation of the PRT is based on the 3D approach (activities in the field of Defence, Diplomacy and Development) and the five key elements from the civil assessment. For example, in the area of Diplomacy the emphasis is on the improvement of governance. Priorities include support for governmental programmes and activities, assistance to increased co-operation and dialogue between the different levels of authority, support to implementation

[70] Ibid., 22-23.

[71] Ministry of Defence, "The Netherlands' Approach to Its Prt Operations in Afghanistan?," (The Hague: Ministry of Defence, 2007), 2.

[72] Royal Netherlands Embassy, "Civil Assessment Urzugan Province, Afghanistan Executive Summary," (Kabul2006), 5.

of reform measures, formulating and implementing provincial policy and increased communication with the population of Uruzgan on ISAF and the PRTs.[73]

In the field of Defence the focus will be on establishing stability through the formulation of a long term strategic security plan with ISAF, the ANSF, ANA and the provincial government and the preparation of institutional arrangements and physical facilities for detainees.[74]

The activities in the field of Development are aimed at poverty alleviation. Priorities include:

- "... support of strategically important zones where improvements in security and governance will create conditions conducive to socio-economic development"
- Support of productive activities and income generation through the creation of an enabling private sector
- Development of capacity ("both inside and outside the government"), in order to establish improved prospects for the youth of Uruzgan
- Facilitation of the development of the health sector
- Establishment of increased involvement of communities and local authorities in developmental activities
- The support of the implementation of national programmes.[75]

2.2.2 The PRT in Practice

The first Dutch PRT (2004) was a so-called 'independent PRT', in the city of Pol-el-Komhri, in the Afghan province of Baghlan.[76] In this area, the local population, the local authorities and the local security forces allowed and supported the Dutch team to fulfil its mission. This so-called 'permissive environment', made it possible to operate the PRT as an independent organization, not embedded in a larger military setting. The PRT was composed out of a command group, a staff, three mission teams, operational support, force protection and combat support service.

The security situation in the province of Uruzgan however, did not permit a PRT to operate on its own. Instead, it got integrated into the Task Force Uruzgan (TFU). In this situation (as shown in Figure 4) the PRT could rely on the support of the other Task Force elements (for example a Battle Group and Special Forces).

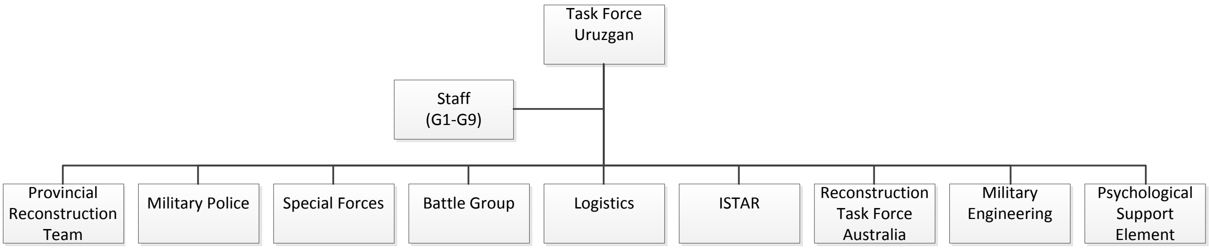


Figure 4 Task Force Uruzgan (until March 2009)

I will come to the composition of the TFU in more detail when I discuss the case that this thesis is based on in Chapter 4. At this point however, I want to focus on the structure of the Dutch PRT before April 2009: until then the PRT was under military command.

[73] Ibid., 3.
[74] Ibid., 4.
[75] Ibid.
[76] The Baghlan PRT was handed over to Hungary in 2006.

2.2.3 PRT under Military Command

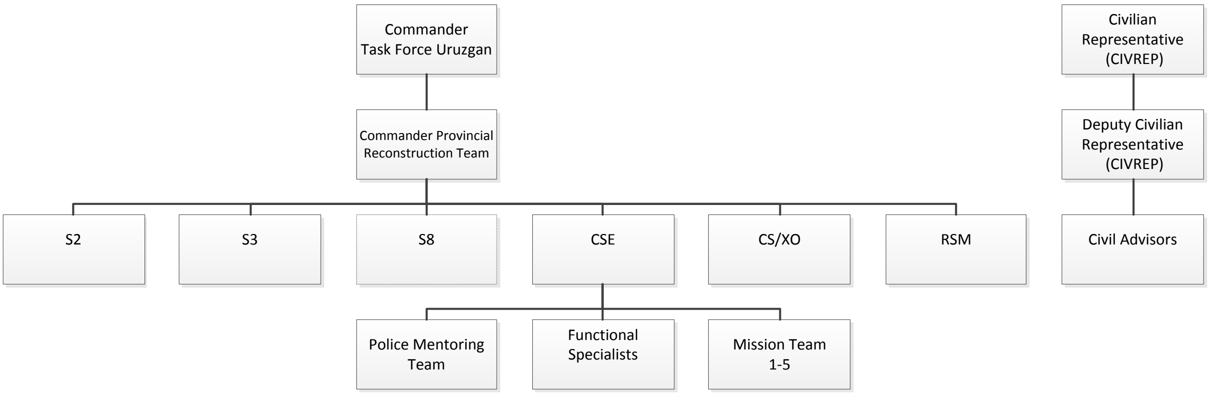


Figure 5 PRT structure (until March 2009)

Up until March 2009, the PRT resided under the lead of the TFU commander (COMTFU). The Commander of the PRT (COMPRT) directs the Provincial Reconstruction Team. He is supported by his staff, comprised of the following functions and sections.

- A Deputy Commander (XO)
- A Chief of Staff (CS), coordinating the different staff sections.
- An intelligence and security section (S2), with a primary task to support the commander by advising him on the use of intelligence and different aspects of (operational) security.
- An operations section (S3), with a primary task to direct the planning of current and future operations.
- A finance section (S8), with a primary task to advise the commander on financial issues.
- A CIMIC Support Element (CSE), responsible for civil-military cooperation and development projects
- A Regimental Sergeant Major (RSM), with a primarily responsibility to maintain standards and discipline as well as being the representative for all personnel ranked Warrant Officer and lower to the commander.

Besides their primary tasks, most sections have additional duties that, viewed in the light of this thesis’ topic should be mentioned. Especially the intelligence and security section is an important player. According to the description of its tasks, a S2 officer should direct the flow of information between the PRT and the TFU, make formats for reports and assessments and produce standard reports on intelligence and security to higher command. But he is also responsible for: the Information Operations of the PRT, providing intelligence needs, planning information collection, processing information to intelligence, disseminating intelligence, processing intelligence from higher level command to PRT level and reading and analysing reports for new information.

The Mission Teams (residing under the CSE) are responsible for identifying, starting, monitoring and evaluating projects that should help the District authorities function. Therefore they coordinate with civil authorities in the area and report and assess on district level. Because of their contacts with local authorities during their patrol the MT is able to collect a lot of information that could improve the situational awareness of the PRT and the overall TFU.

Notice that besides the military commander, there is the Civilian Representative (CIVREP). This officeholder is responsible for advising the PRT commander, guiding the employees from the Ministry of Foreign Affairs, the Ministry of Development Cooperation, the Development Cooperation Advisor and the Tribal Advisor. He also directs the functional specialists (FS). The CIVREP also has a direct link to the local diplomatic representation, the Dutch embassy in Kabul. His role became much bigger when, in March 2009, the PRT was placed under his direction.

2.2.4 PRT under Civilian Direction

As from March 1, 2009 a 'management board' is established, after the example of the British and the Canadians. From that moment on PRT is put under the lead of the CIVREP, together with the civil structure that was already led by the CIVREP. Not only did the security situation allow civilian direction, it also gave the Ministry of Foreign Affairs (the major financier of the reconstruction activities) a more direct saying in the PRT's activities.

Both the commander of the TFU (COMTFU) and the CIVREP have a seat in this coordinating organ and are responsible for directing the military and civil activities. However, COMTFU remains ultimately responsible for security related issues and the TFU. The CIVREP, representing the Royal Netherlands Embassy in Kabul, coordinates all the non-military activities in Uruzgan.

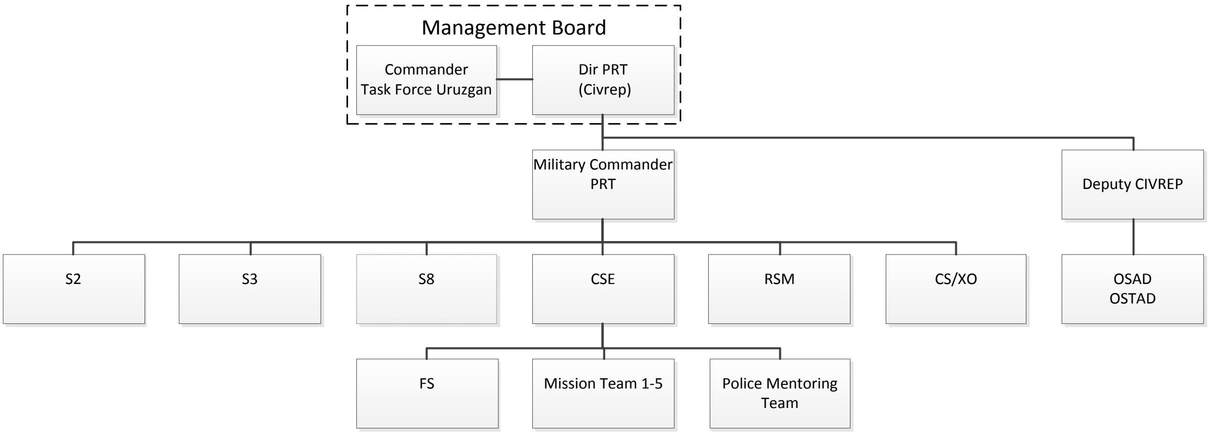


Figure 6 PRT structure (as from March 2009)

Both the COMTFU and the CIVREP are responsible for coordinating civilian and military activities in their area of responsibility. As a former CIVREP said: "He [the COMTFU] could not do anything without my signature and I could not do anything without his".[77]

Besides the newly installed management board, the structure of the PRT changed little. The military part of the PRT was placed under the direction of a military commander, while the Deputy CIVREP took over the civilian part of the PRT. The staff remained untouched as were the other parts of the team.

The table in Appendix III gives an overview of the PRTs between March 2009 and March 2010.

[77] Interview PRT2

3 PSYOPS SUPPORT ELEMENT

In this chapter I will discuss the PSYOPS Support Element (PSE), the smallest unit of the Task Force Uruzgan (TFU). Less than 20 people were involved in a rather big mission: to influence the posture, perception and behaviour of the Afghan population in Uruzgan.

Before I turn to the PSE, its organization and its functions, I want to take a look at the definition of PSYOPS as expressed by NATO and the Royal Netherlands Army.

3.1 Psychological Operations

Since 2002 there have been two NATO Allied Joint Publications (AJP) on Psychological Operations. The first one, AJP 3.7, and AJP 10.1. The most recent one describes PSYOPS as:

> *Planned psychological activities using methods of communications and other means directed to approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives.*[78]

The Dutch Army Doctrine Publication (ADP) II-C defines PSYOPS according to the previous NATO description (used in AJP 3.7).[79] However, in a 2006 document on Dutch PSYOPS policy, the 'new' NATO definition is used. As indicated in paragraph 1.1.6, I will refer to the current NATO definition for the rest of this thesis.

3.2 PSE Organization

Since the start of the TFU, the PSE has been part of the organizational structure of the task force as is shown in Figure 7.

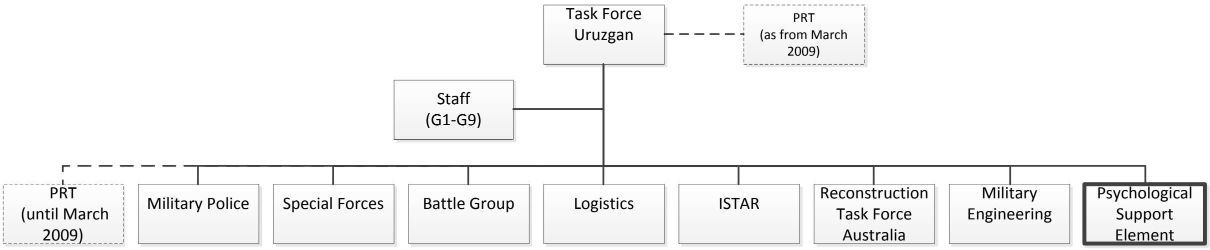


Figure 7 PSE as part of the TFU

Notice that until March 2009, the PRT and the PSE were positioned on the same organizational level. Both resided under the lead of the (military) COMTFU.

The PSE itself is constructed out of four basic elements (Figure 8): the commander, his staff and two Tactical PSYOPS Teams (TPTs).

[78] ———, "Mc 402/1 Nato Military Policy on Psychological Operations," 2.

[79] "... planned psychological activities in times of peace, crisis and war, directed at hostile, friendly and neutral parties with the intention of influencing the attitudes and behaviour which affect the established political and military objectives". Royal Netherlands Army, "Combat Operations Adp Ii - Part C: Combat Operations Againts an Irregular Force," 687.

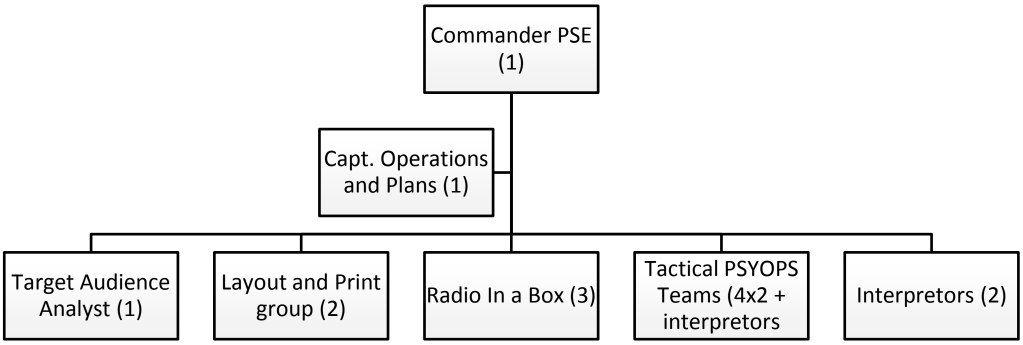

Commander PSE (1)
Capt. Operations and Plans (1)
Target Audience Analyst (1)
Layout and Print group (2)
Radio In a Box (3)
Tactical PSYOPS Teams (4x2 + interpretors
Interpretors (2)

Figure 8 PSE structure

The Commander of the PSE, a major, is tasked with directing his PSYOPS Support Element. He is supported by a deputy commander who handles the planning and execution of PSE campaigns. The Planner is basically tasked with the planning of activities. In this role he should have frequent contact with other units like the PRT in order to coordinate each other's activities and coordinate the cooperation between for example the MTs and TPTs. There is also a group responsible for making handbills and posters as well as a so-called Radio In A Box (RIAB) that transmits radio messages.

Besides making analyses of potential audiences, the Target Audience Analyst (TAA) is the key figure when it comes to information management. He is a member of the All Source Intelligence Centre (ASIC), where information from all kinds of sources is collected and processed. The TAA is also responsible for storing the information collected by the TPTs into digital database such as iBase.

The TPTs consist of a Commander, a Deputy Commander, two Drivers and an Interpreter. These teams are the eyes and ears of the PSE outside the gate of the base. They go on patrols, talk to the local population and spread the PSYOPS messages. Most of these patrols are carried out together with other units such as the PRT and the Battlegroup (who offers force protection).

The table in Appendix III gives an overview of the different PSEs between march 2009 and March 2010.

4 INFORMATION EN COMMUNICATION

In this chapter the model that is used to analyse the exchange of information between the PRT and the PSE will be introduced. First, however, the concept of 'information' should be defined. Together with information, related concepts like data, knowledge and intelligence will be defined.

Next I will introduce the model that describes the internal process of information management. Although this study focuses on external process of exchanging information between two separate units, it is vital to understand the internal processes. The different phases will be described and the models, on which this instrument for analysis is based will be discussed briefly.

By combining two of the models that describe the internal processes, a combined model comes into being. It will become clear that the storage of information and the 'organizational memory' or database, plays an important and central role. Different types of information (consisting of both digital and hardcopy information, as well as 'knowledge') should be stored within a central database.

4.1 Data, Information, Knowledge and Intelligence

Before presenting the information management cycle, a basic understanding and a clear definition of 'information' is needed. Information starts however with data.

According to a commonly held view, data is raw numbers and facts.[80] Information is data that has been given meaning by processing it and putting it into a certain context through ways of relational connection.[81] One could describe the difference between data and information referring to symbols. Data is about symbols and it "simply exists and has no significance beyond its existing".[82] For example, the symbol in Figure 9 has no specific meaning without a context. It is nothing more than a set of lines. However, when this symbol is put into a military context it is given meaning: infantry unit.

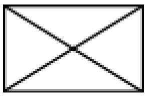


Figure 9 Symbol

A third concept that is frequently used in this context is knowledge. Knowledge is defined as information together with some kind of human involvement.[83] It is information combined with "experience, interpretation and reflection".[84]

The reason for adding the definition of knowledge to this paragraph is that, beside information, there is a similar concept that is used frequently in the military context: intelligence.

[80] Maryam Alavi and Dorothy E. Leidner, "Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues," *MIS Quarterly* 25, no. 1 (2001): 109.

[81] Ibid.

[82] Gene Bellinger, Durval Castro, and Anthony Mills, "Data, Information, Knowledge, and Wisdom," Systems Thinking, http://www.systems-thinking.org/dikw/dikw.htm.

[83] Lisa Krizan, "Intelligence Essentials for Everyone,"(1999).

[84] Development Concepts and Doctrine Centre, "Information Management," ed. Ministry of Defence (Swindon: Ministry of Defence, 2006), 3.; Alavi and Leidner, "Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues," 109.

> *Intelligence is more than information. It is knowledge that has been specially prepared for a customer's unique circumstances [...] Intelligence collection systems produce... data, not intelligence; only the human mind can provide that special touch that makes sense of data for different customers' requirements.*[85]

By defining intelligence as "the product of collecting and *processing data* [italics added]" the intelligence guideline from the Royal Netherlands Army basically states that intelligence is similar to information (at least according to the abovementioned definition of information). However, intelligence is much more that information.[86] The NATO Glossary of Terms and Definitions, agrees on this: intelligence is "the product resulting from the *processing of information* [italics added] concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations".[87]

Data remains a fundamental building block for creating information and includes basic facts and statistics. The meaning that individuals give to data, presented in a context, is information. That information, combined with experience, interpretation and reflection, generates knowledge or (if it concerns information on adversaries and areas of operation) intelligence. In the case of a PRT, collected data could be the number 23,000. By adding meaning to this number ("inhabitants of a city"), information is created. When this information is reflected upon, by comparing it to previous information on the number of inhabitants ("50.000 inhabitants"), the produced knowledge suggests that more than half of the people that used to live in this city are now gone. When this knowledge concerns the inhabitants of a certain area of operations, it could be classified as intelligence.

4.2 The Information Management Model

Since the idea of information is clear, the instrument for analyzing the internal management of information can be introduced. In this paragraph the individual phases of the cycle (Figure 10) will be described. The model is however largely based on a couple of other (both military and non-military) models that can be found in Appendix I. When describing the different phases I will occasionally refer to these models.

4.2.1 Information Goal

The information management cycle starts with an information goal. This first process is easily overlooked when constructing an information management model: the information goal is not explicitly mentioned in the basic intelligence cycle used by the Royal Netherlands Army nor in the information life cycle form the British Armed Forces (see for both cycles Appendix I). The phase of formulating information goals is also lacking in some non-military models that I studied (see for example the models by Choo and Krizan in Appendix I). Nevertheless this phase remains critical, especially in a (hierarchic) military organization where goals are set and orders are given. Weggeman however starts his model with a phase in which mission, vision, goals and strategy are identified.

It should be clear what goals have to be met, what mission has to be accomplished. Therefore I added this phase to the model that will be used to assess the situation in

[85] William S. Brei, "Getting Intelligence Right: The Power of Logical Procedure,"(1996).

[86] Royal Netherlands Army, "Leidraad Inlichtingen," ed. Ministery of Defense (The Hague: Royal Netherlands Army, 2006), 10.

[87] NATO, "Aap-6 Nato Glossary of Terms and Definitions."

Afghanistan. The next phase, the identification of information needs is largely dependent on a clear information goal.

4.2.2 Information Needs

The information goal is used as the input for determining the information needs or requirements. Questions like: what kind of information is needed? Where can this information be found? How can this information be collected? Who will collect this information? This process is basically about identifying needs but also about planning and tasking. Although Weggeman included the determination of existing information to this particular phase, I added this process to the collection of information.

4.2.3 Information Collection

The collection of information is about acquiring information according to the needs that were identified in the previous phase. The information needed might exist both inside and outside the organization. Therefore, I made the determination of existing information part of the collecting phase (see 4.2.2): the information that is already present within the organization is determined in this phase. Some kind of database that contains the internal information is a necessity. Without it, an organization cannot store its acquired information. This database will therefore be the main source for acquiring existing information and knowledge.

Notice that in this phase communication between the own unit and other units starts playing a role. I will describe this communication process in more detail when I connect two Information Management Cycles in the next paragraph.

4.2.4 Information Organization

When necessary information is collected, it should be organized. Because information can be provided by all sorts of different sources, the diversity of information and its formats can be huge. In order to keep the information accessible, controlled and structured the collected information needs to be organized. In some situations information should be extracted from certain media. In other cases information needs to be translated (sometimes literally) into a useful format.

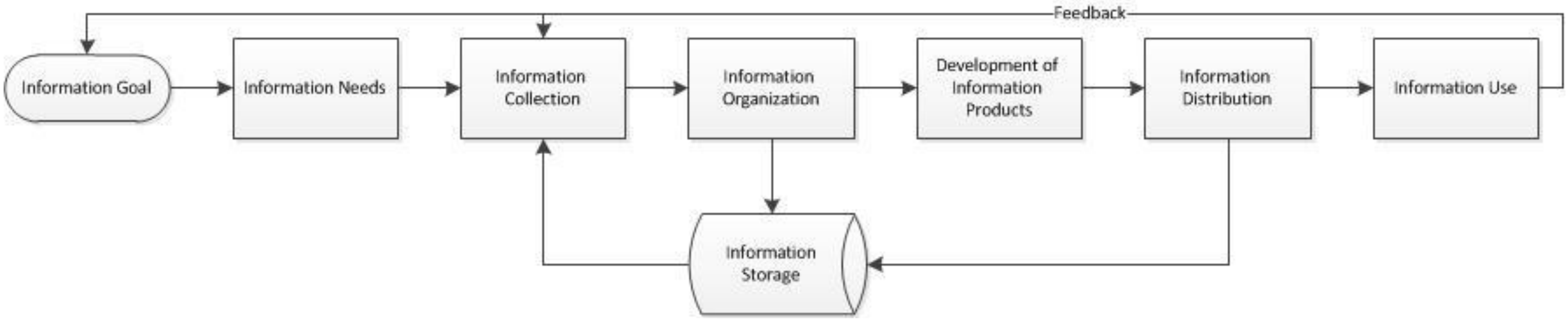
4.2.5 Information Storage

As soon as the information is organized, it should be stored in order to create an “organizational memory that is the active repository of much of the organzation’s knowledge and expertise”.[88] Information can be stored in roughly three ways: in digital form, as a hardcopy or in the human brain (where it becomes knowledge). These three types of storage all have their own advantages and disadvantages: one can think of, for example, accessibility or security issues.

Information that is stored in one of the abovementioned three ways becomes part of the organizational memory or database.

[88] Chun Wei Choo, "Information Management for the Intelligent Organization: Roles and Implications for the Information Professions," in *Digital Libraries Conference* (Singapore1995).

Figure 10 The Information Management Cycle



4.2.6 Development of Information Products

When the information is collected, organized and stored, the organization (i.e. the military unit) can start to develop information products. In this phase presentations, electronic messages, hardcopy reports, videos and briefings can be made. The information presented in these products or services should meet certain criteria. It should be accessible, timely, objective, relevant, accurate, accountable and secure. Only when these criteria are met, the final information product can be of use to the initiator of the information process.

4.2.7 Information Distribution

Next, the final product needs to be distributed. The information should be disseminated to other relevant actors and added to the database (or organizational memory). Notice that the distribution process is a phase in which communication with other units is key. As with the collection phase, the database is of great importance. As I will show in the paragraph where I will combine two of the Information Management Cycles (

Figure 12), it is this database that can play a very important role in sharing information.

4.2.8 Information Use and Feedback

When the information is distributed, it can be applied at the different levels. This will result in new information and possible adjustments of the information goal: it is a constant process of altering and adjusting the goals in order to get the information that is needed.

However, the feedback loop also links to the information collection phase. This is done based on the information management cycle by Choo (Appendix I). The use of the collected information itself produces new information that should be acquired by the organization and stored in its organizational memory (i.e. the ‘database’).

4.2.9 Disposal of Information

Something that is not included in the model, although it is mentioned in the British information life cycle, is the disposal of information. When collected information is being processed, some information may be lost. For example, when a lot of information has to be compressed into a brief report, data and thus information will be lost: details will be left out and only the most important information will be presented. Although in principle all information should be stored (after being organized), there will always be some loss of information because of intentional or unintentional selection or interpretation at every phase of the model. Because of this I have not added one or more disposal phases into the information management model. It would make the scheme unnecessarily complex.

4.3 A Combined Model

This study is about the communication of information between the PRT and the PSE. Therefore only one internal cycle will not be sufficient to capture all the processes going on. In fact, what is needed is a combined management system that covers both the internal and the external information processes. When combining two of the internal information management cycles (Figure 10), we get a new cycle that is presented in (Figure 12). Notice the central role of the information storage process. It is this phase that basically links the two units together.

However, the cycles remain individual in the sense that each unit works on its own processes. During the collection phase both units can acquire information from the database that has previously been collected by one of them. At the same time the database can be filled with raw but organized information from both units, and can contain finished information products.

The introduction of a central database solves an important communication problem. When information travels along the hierarchical lines of the organization, information is being compressed and (seemingly unimportant) details are lost. Only the relevant parts of tactical (or operational) reports will be discussed on a strategic level. Information that is unrelated to that level will not be reported. It is therefore not always possible to distribute information through the hierarchical organizational structure to all remote corners of the organization.

By using a shared database like the one in Figure 12 the information not only gets distributed along the hierarchical (vertical) lines, both also ‘horizontally’, crosscutting the organizational structure (Figure 11).

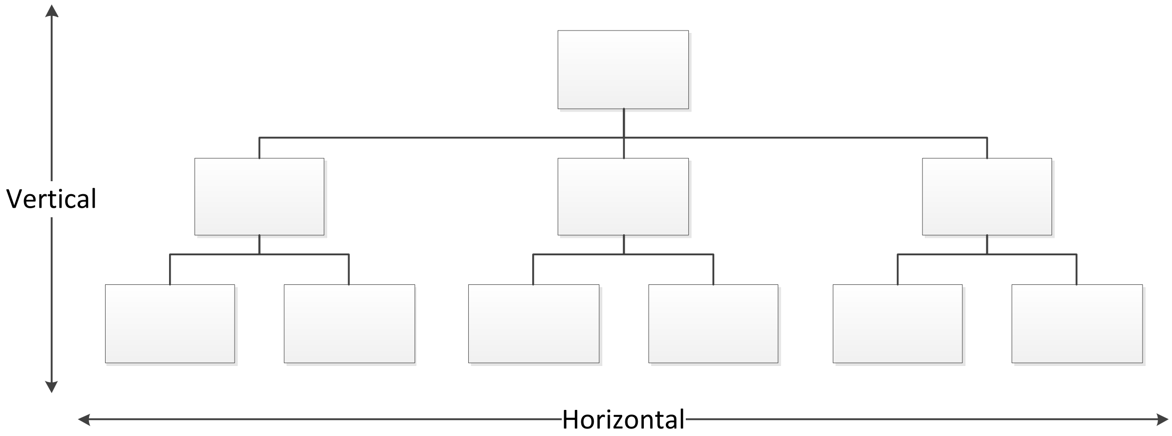
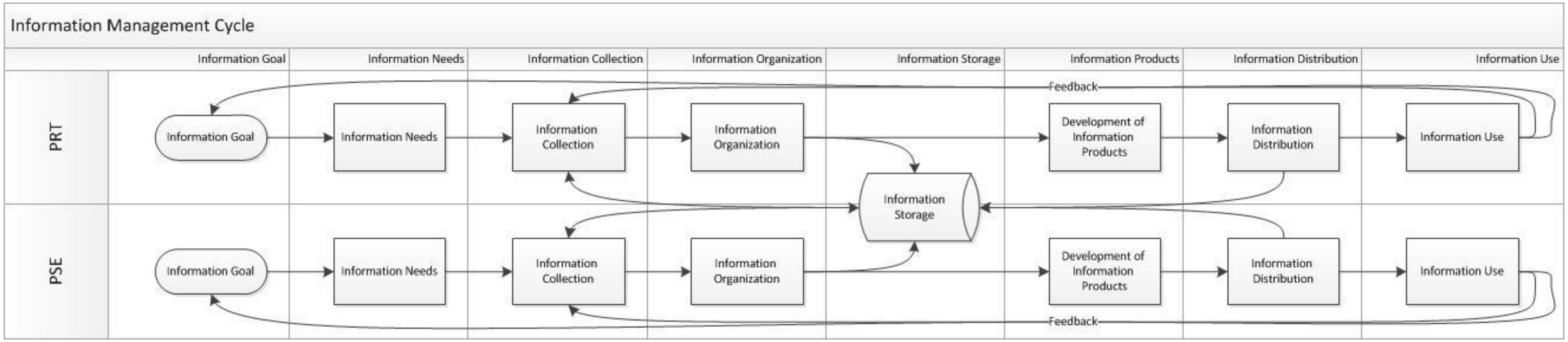


Figure 11 Ways to exchange information

Figure 12 Combined Information Management Cycle



Although a shared database may solve the problem of exchanging information between several units, the linking of the individual types of information storage (digital, hardcopy or knowledge) pose some new challenges: Not all sources are equally accessible.

A closer look at what we might call the heart of the information exchange process, gives us a model as is presented in Figure 13. In this figure the types of information storage are introduced and linked with the sources from the other unit.

Figure 13 demonstrates two things. First of all, it shows that knowledge, hardcopy and digital information can be transformed into each other. Within the PRT and PSE, the information available to the individual members of the unit (i.e. their knowledge) can be transformed into hardcopy documents or digital database records. Documents can be digitalized, or stored as knowledge in the human brain. Digital documents can also become a part of human knowledge or can be printed and stored as hardcopy.

Second, the internal information flows can be connected by linking the ways of storage. Knowledge can be linked by (and eventually exchanged through) interpersonal contact (e.g. meetings, face-to-face conversations, conversation over telephone, etc.). Entrance to each other's digital documents or database can be done by exchanging digital documents via electronic mail or by linking or even merging two digital database into a single database. Hardcopy documents can be exchanged by physical exchange.

What I would like to add to the idea of knowledge exchange (information that has been processed and combined with human involvement), is that knowledge becomes information when it is shared: it leaves the mind and thus loses its connections with the individuals interpretation. The British Joint Doctrine Note on Information Management states that "one individual's knowledge becomes another's information, and thus information and knowledge, when presented, require managing through the same IM [information

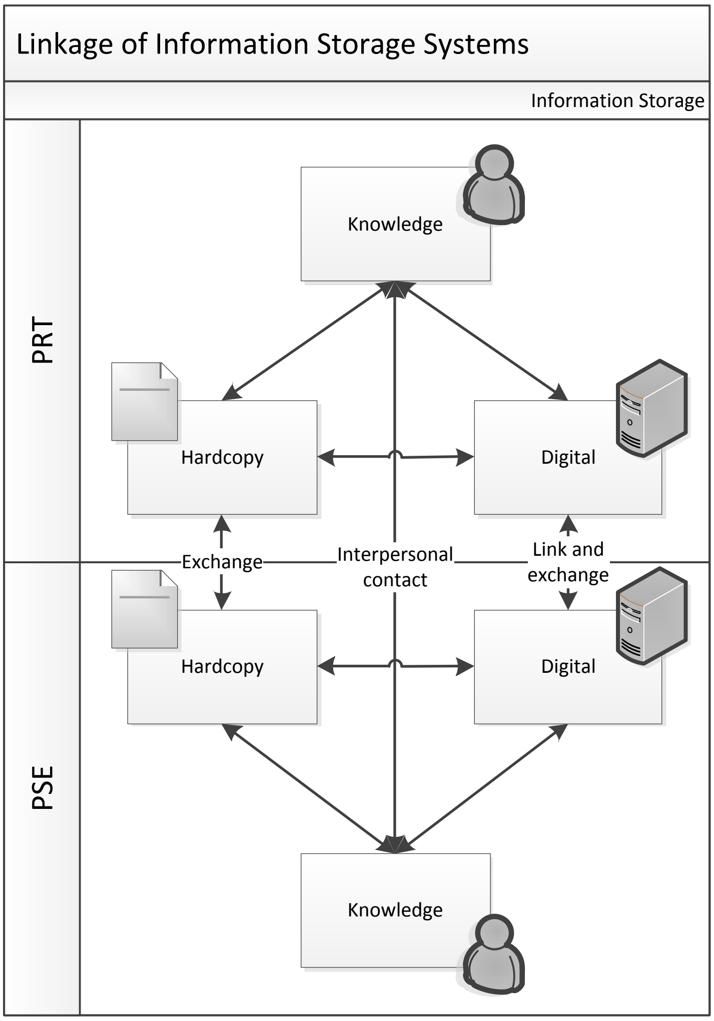


Figure 13 Linkage of Information Storage Systems

management] processes”.[89] As soon as knowledge leaves one’s mind, it is becomes separated from one’s experience, interpretation and reflection and thus becomes plain information again.

The linking of the information storage systems, the hub in the combined information management cycle, should be studied to analyse the actual exchange of information. The three ‘intra-organizational’ links (interpersonal contact, linking and exchanging of digital documents, and exchanging hardcopy documents) therefore are keys when analyzing the exchange of information in the coming chapters.

Before turning to the case of Afghanistan and the exchange of information between the PRT and the PSE, I would like to briefly touch upon the definition ‘exchange of information’, or communication.

4.4 Exchange of Information

In a counterinsurgency environment, a common base of understanding and a shared situational awareness is key to effective collaboration. Therefore communication between actors is one of the most critical conditions for success.

[89] Development Concepts and Doctrine Centre, "Information Management," 3.

The most well-known communication model comes from Shannon & Warren (Figure 14). The model consists of an information source, that sends out a message through a transmitter that converts the message into a signal. This signal is then send through a channel (or medium) to a receiver that turns the received signal back into a message. During this linear process, the signal can be influenced by a noise source, for instance a technical obstacle that can interfere with the signal. The feedback loop is used by the receiver to respond to the message. It is through this mechanism that the received information (and interpretation of the receivers) can be checked.

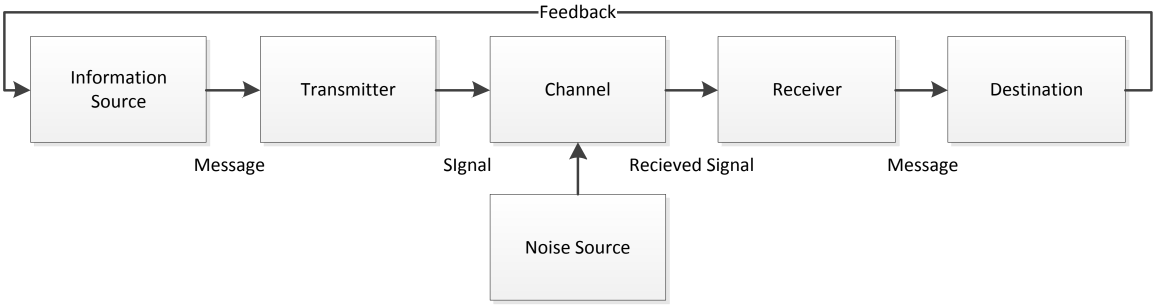


Figure 14 The Shannon & Weaver mathematical model[90]

By using this model, a certain understanding of communication is implied. It is basically a linear process by which information is transferred from a source to a receiver. However, communication can be perceived through a whole range of definitions and concepts. It his article 'The Concept of Communication' Frank Dance describes 15 conceptual components of communication, accompanied by definitions. Communication is defined as "the verbal interchange of thought or idea" or even "the mechanism by which power is exerted".[91] Communication can be thought of as something about symbols, understanding, interaction, transfer, stimuli, etc.

From all of these definitions and concepts a central thought can be deduced: communication is about transmission from a source to a recipient. Ayer describes this process as "something's being transferred from one thing, or person, to another [...]. He adds that "In many cases, what is transferred in this way continues to be shared", it does not necessarily 'leave' the source.[92] In this thesis that "something" that is being transferred is information.

Especially during interpersonal contact, the communication model by Shannon & Weaver provides an insight in how this process works. In order to effectively communicate knowledge, the sender transforms his knowledge into information by sending a message, through a certain channel. That message is then received by a recipient.

The exchange of digital information follows roughly the same steps: a message containing the information is transmitted via signals through a digital medium (the Internet or a local network) and is then received by the other party.

In both cases during the transmission of a message, an external noise source can interfere. Therefore it is necessary to check if the received information is equal to the information that has been send.

The exchange of hardcopy documents follows a different way. One could argue that information that is available in hardcopy is already in the 'channel' phase of the model. The

[90] Claude Elwood Shannon, "A Mathematical Theory of Communication," *The Bell System Technical Journal* 27(1948); Claude Elwood Shannon and Warren Weaver, *The Mathematical Theory of Communication* (Champaign: University of Illinois Press, 1963).

[91] Frank E.X. Dance, "The "Concept" Of Communications," *The Journal of Communication* 20, no. 2 (1970): 204-08.

[92] A.J. Ayer, "What Is Communication?," in *Studies in Communication*, ed. A.J. Ayer, et al. (London: Martin Secker & Warburg, 1955), 12.

information is already put down, transcribed into a certain message. The only thing left to do for the recipient is to ‘decode’ the message (that is to read it).

4.5 Instrument for Analysis

It is the combined model in Figure 12, including the (detailed) model of the relations between the different types of information storage as depicted in Figure 13, that will be used for analyzing the exchange of information between the PRT and the PSE. Based on the different phases, the relations between them and the actions taken in each phase, the semi-structured interview is designed (Appendix II).

The questions follow the different phases of the information cycle. It touches on the information goals of the PRT and PSE: what assignments did they have? From whom did they receive their assignments? The information needs, collection, organization, storage, development, sharing and information use are also discussed. The answers to these questions not only help to ‘map’ the flow of information within the PRT and PSE but also the various opportunities for information exchange between these units. The efficiency and quality of information exchange can then be based on these outcomes.

The result of the interviews will be presented in the next chapter.

5 THE URUZGAN CASE

The case which the model (Figure 12) from the previous chapter will be applied to, is the presence of the Dutch Task Force in Uruzgan, Afghanistan from March 2009 until March 2010. This particular period of time is chosen for several reasons, of which the most important one is that in March 2009, the Dutch PRT became civilian-led. Other reasons include the possibility to collect fairly recent and accurate information and the possibility to extend the study across more organizational levels. A previous study by Den Boer, for example, focussed only on the exchange of information on the 'tactical' mission team/tactical PSYOPS team level.[93] This thesis will also incorporate the exchange of information on the level of the PRT and PSE staff, all the way up to the Management Board.

The results of applying the model to the case will be presented in twofold. First the information cycle within the PRT will be discussed. During the interviews it became clear that two distinct but intertwined cycles are present, a mid- to long-term cycle on a staff level and a mid- to short-term cycle on the tactical level. Both cycles will be discussed. The same thing goes for the PSE information cycle.

Together with a description of the information flow within the units, the exchange of information will be discussed.

5.1 The PRT Information Life Cycles

When the information model is applied to the PRT's information flows, it shows that two distinct but intertwined cycles can be distinguished. The first one is what I shall call the mid- to long-term staff cycle. This flow of information almost entirely takes place within the PRT staff. The information that is collected during this phase is nearly always acquired by consulting internal sources: digital databases and knowledge that is available within other elements.

The second cycle focuses on the tactical level and the role of the mission teams: the information is collected from sources outside the organization. This is why this cycle will be called the tactical information cycle.

In the next paragraphs these flows of information will be discussed as well as the moments and processes of communication between the PRT and the PSE.

5.1.1 Staff Cycle

Although the organization chart does not indicate a hierarchical relation between staff TFU and PRT, the Provincial Reconstruction Team is treated as a subordinate element of the TFU.[94] This means that long term orders are issued by the Staff to direct the PRT in the long run. Therefore the first process, the definition of the information goal, is done by the TFU staff. After issuing the order, it will be examined by the PRT and the units that are closely linked, such as the PSE. During this stage, the involved actors talk over the individual tasks in order to reach a common understanding.

Next, the PRT staff will formulate the information needs required to produce the effects that are described in the order. This is where the S2 officer of the staff comes in. In his role as intelligence officer he is able to identify the required information in close cooperation with the other staff members. Moreover, he has access to the most current intelligence and

[93] Jelmar Den Boer, "Informatie-Uitwisseling Tussen Het Mission-Team, Tactical Pys-Ops Team En Het Field Humint Team" (Nederlandse Defensie Academie, 2008). As the title of this thesis implied, Den Boer also included the field humint team into his analysis.

[94] Interview PRT1

information available on the intelligence drive on the network. He therefore can collect the information needed to carry out the order.

However, the other staff member will also collect information for example through knowledge that is available at the other units. During formal and informal conversations information exchange takes place. After the information is organized by the S2, it can be stored.

During PRT 7 a lot of information has been stored through collators from the 2 section (intelligence and security) at the TFU staff because the PRT did not have its own collator capacity (red line in

Figure 15).[95] This resulted in a fragmentized database, called iBase, in which reports were stored as single entities and individuals were known under several different names.[96] A couple of months after PRT 8 arrived, they started filling and correcting iBase themselves (green line in

Figure 15). This resulted in over 2000 new entries.[97] After the database was 'back on track', the collators from the TFU staff took back over. However, this time reports that had to be added to the database were prepared in such a way that the collators could not make the same mistakes again.

After the information was stored the intelligence officer made his information products (summaries, presentations, briefings etc.). These were then, depending on the classification, distributed among the other parts of the PRT (mission teams, staff) and other elements of the TFU (staff, other units, iBase).

Based on the interviews I had with PRT members, I could not identify a specific feedback loop or evaluation process for this process. A clear evolution of the whole process is therefore not included in

Figure 15.

[95] Interview PRT6
[96] Interview PRT7
[97] Interview PRT7

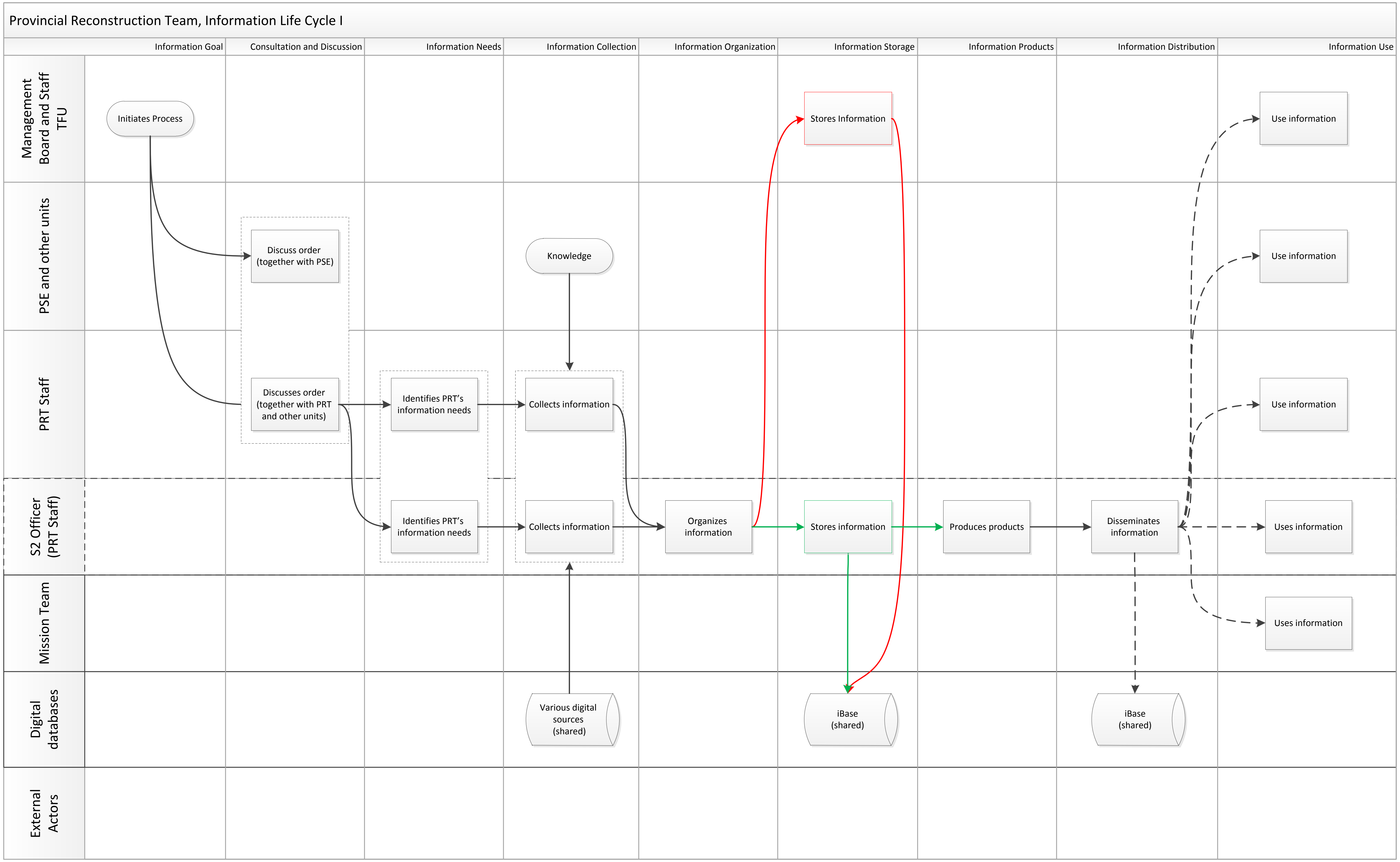


Figure 15 PRT Information Life Cycle I

5.1.2 Exchange of information

Exchange of information between the PRT and PSE takes place at several different moments. First, there is the examination of the order issued by the TFU staff. At this point staff members of the PRT and PSE (together with other units involved, such as the Battlegroup) sit together to discuss the order and the role that each of the units could play in order to reach the desired end state. According to the interviewees that were present these meetings were held in a cooperative way. However, as a former PRT commander told me, he noticed that after these meetings the different actors went their own way again.[98]

The collection of information required to prepare and execute activities were gathered by staff members through informal networking and were heavily depending on interpersonal relations and knowledge about the whereabouts of information. Digital databases established indirect communication: information shared by other units could be found in for example iBase.

5.1.3 Tactical Cycle

The tactical cycle focuses on the processes that take place when the mission teams are tasked to gather information. The cycle starts when the military commander of the PRT orders an MT to go on patrol. Most of the time however, especially on the more remotely located bases, the MT commander itself decides when he goes on patrol. A decision like this is taken in close cooperation with the PSE and the unit that delivers force protection. If the intelligence officer of the PRT staff (S2) has some additional information need, he can provide the mission team with a list of questions.

During their patrol the MT will gather all sorts of information about the area where they operate: the attitude of the population, social ties between tribal leaders, basic needs etc.

The information that is collected is then put into a patrol report. Notice that in Figure 16, this report is put in the Information Organization stage, because it is raw information that is not processed yet by for example an intelligence officer.

The report will then be send to the S2 officer in Tarin Kowt, the main base in the area. For those mission teams that were not located on the military base in Tarin Kowt, the report was send to the S2 via the intelligence officer located on the bases in Chora en Deh Rawod.

The S2 stores the product in the digital database. As said before, previous to PRT 8 the storage of reports was done by collators working at the TFU staff (red line in Figure 16). The intelligence section of PRT 8 however, took care of collating the reports themselves for quite some time during their tour.

After the information has been stored, the intelligence officer can produce his own information product (for example an intelligence summary, a briefing or an analysis). After the product is finished, it will be distributed, depending on the classification, to a database or other units.

As with the first cycle, there is no clear feedback loop present in this information life cycle.

[98] Interview PRT3

5.1.4 Exchange of information

During this cycle information exchange is taking place between the PRT and the PSE at various moments. However, the amount of exchange heavily depends on the type of patrol and the base where the MT is located.

On the more remote bases such as Deh Rawod, the Mission Teams and Tactical PSYOPS Teams worked more closely together, largely because of the smaller size of those bases compared to the main base in Tarin Kowt. A lot more informal information exchange took place for example, because a deputy TPT commander shared a room with a MT commander.[99]

However, during the preparation phase both the TPT and MT in Tarin Kowt as well as the teams on the other bases sat together in order to discuss the goals of the patrol, the places they would like to visit and the people they would like to meet. Because the TPT is not targeting a specific local leader or elder (as the MT often does), but instead talks to the local population in general, they could easily adapt to the more specific wishes of the MT.

When the patrol was a joint undertaking, the exchange of information between the MT and the TPT was obvious: the two teams worked closely together for several days, they visited the same places and they discussed their observations.

Afterwards the TPT and MT patrol reports are placed on the local network (in the case of the more remote bases) and thus shared. The reports were also send to the S2 in Tarin Kowt who placed them on iBase and used them to make his own information products. These products were then shared with other units depending on the classification.

[99] Interview PSYOPS4

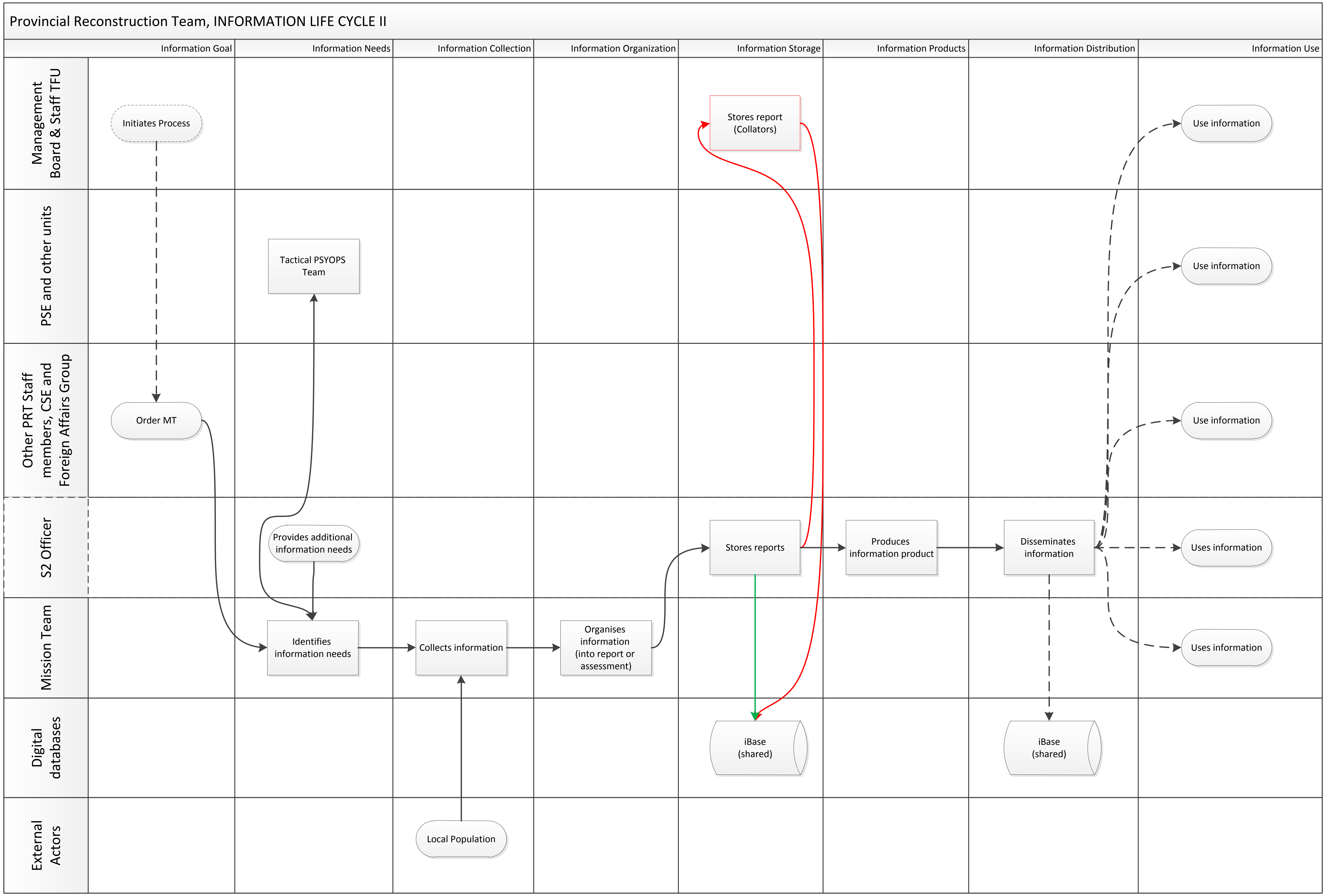


Figure 16 PRT Information Life Cycle II

5.2 The PSE Information Life Cycles

As with the PRT, two different but interlinked information cycles can be distinguished inside the PSE. The first one starts when an order is issued by the staff of the TFU and concerns the preparation stage of a certain (long term) operation. In this stage the PSE will focus on collecting information necessary to prepare actions and produce annexes to orders.

A second process starts when the order is issued and a TPT goes on patrol. During these patrols the members of the TPT will be confronted with information that needs to be gathered, organised and processed. This cycle results in the production of a patrol report.

5.2.1 The Staff Cycle

The first cycle I want to discuss is the Information management model depicted in Figure 17. This cycle is mainly an internal process; it does not incorporate external actors such as the local population or governmental or non-governmental organization or institutions.

The steps in this cycle are basically aimed at supporting the tactical teams and producing annexes to orders that are issued by the TFU staff. Most of the information that the PSE will produce during this stage is based on information that has been acquired previously. The database that contains this information and knowledge is therefore of great importance.

In this stage the PSE will not send its tactical PSYOPS team for collecting information. The only sources that are used are the internal digital databases and knowledge that is present within the PSE and other units such as the PRT or the Battle Group.

The process is depicted in

Figure 17. The different stages will be explained in the next paragraphs.

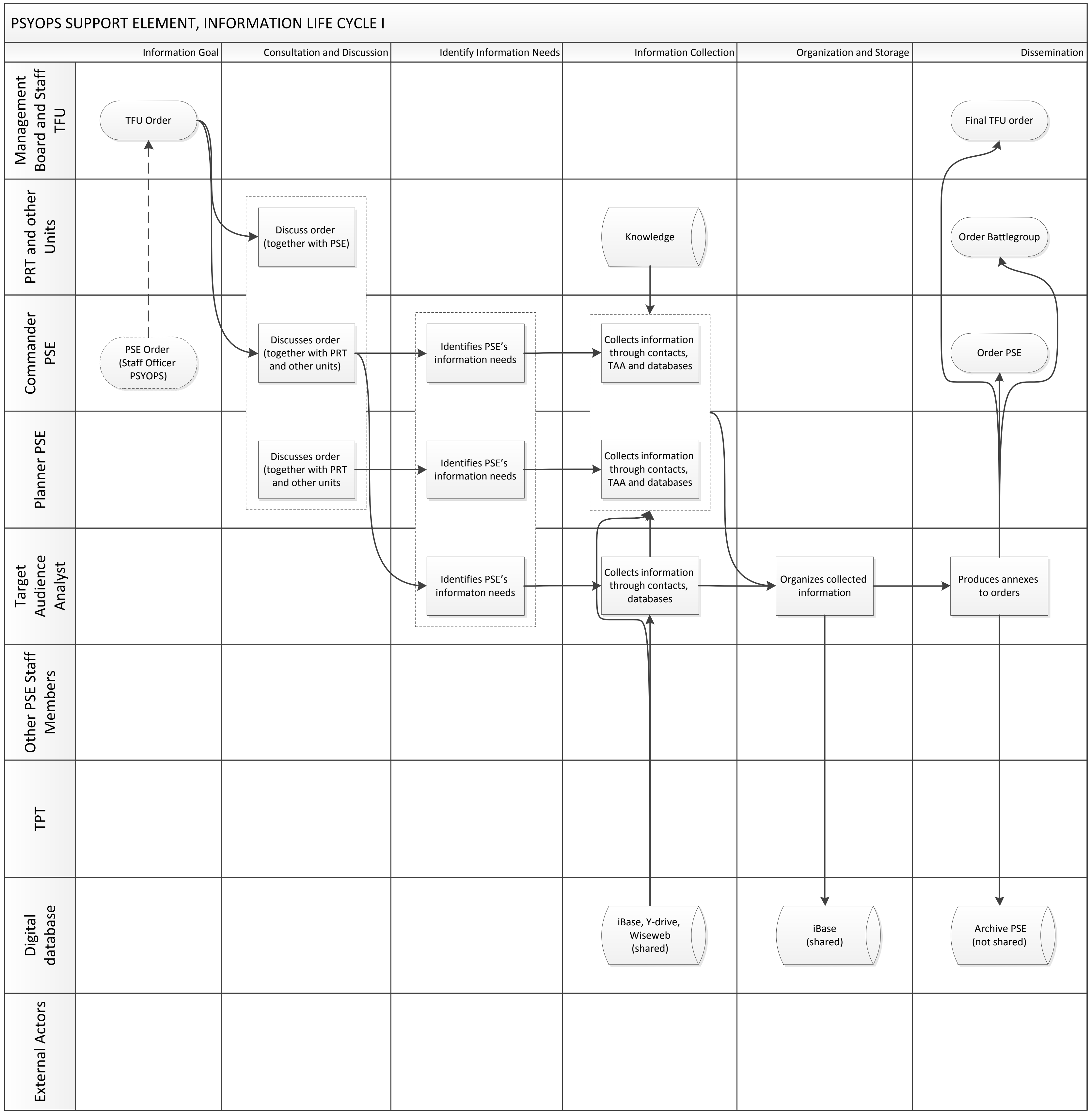

PSYOPS SUPPORT ELEMENT, INFORMATION LIFE CYCLE I
Information Goal
Consultation and Discussion
Identify Information Needs
Information Collection
Organization and Storage
Dissemination
Management Board and Staff TFU
PRT and other Units
Commander PSE
Planner PSE
Target Audience Analyst
Other PSE Staff Members
TPT
Digital database
External Actors
TFU Order
PSE Order (Staff Officer PSYOPS)
Discuss order (together with PSE)
Discusses order (together with PRT and other units)
Discusses order (together with PRT and other units
Identifies PSE's information needs
Identifies PSE's information needs
Identifies PSE's informaton needs
Knowledge
Collects information through contacts, TAA and databases
Collects information through contacts, TAA and databases
Collects information through contacts, databases
Organizes collected information
Produces annexes to orders
Final TFU order
Order Battlegroup
Order PSE
iBase, Y-drive, Wiseweb (shared)
iBase (shared)
Archive PSE (not shared)

Figure 17 PSE Information Life Cycle I

The information goal is formulated in an order issued by the staff of the TFU and will be the starting point of the information cycle. Notice that the staff officer responsible for psychological operations happens to be the same person as the PSE commander. He is therefore actively engaged in writing staff orders. To make things even more complicated, the C-PSE does not have a superior officer within the TFU. He gets his orders directly from Regional Command South (RC-S) in Kandahar, which gets its orders from ISAF headquarters in Kabul (Figure 18).

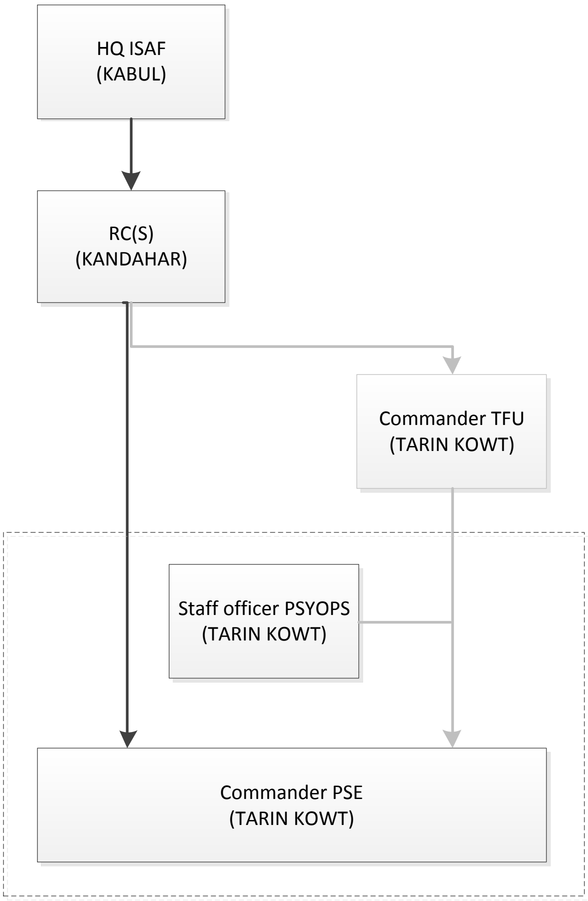


Figure 18 Command structure PSYOPS

Figure 18 shows this command structure. The two functions boxed by the dotted line are filled by the same individual. This construction means that the PSE Commander more or less "writes his own order".[100] Nevertheless, these orders should of course fit in with the overall TFU guidelines.

The order from the TFU staff does not read as a clear assignment but is formulated in terms of desired effects: "This is the effect we would like to achieve in order to reach that end state".[101] This order is then send to the PSE commander and the other units that might be involved. These units have to concretize this order in close cooperation and coordination. Thanks to these joint meetings the other units (including for example the PRT) become familiar with the order and the capabilities of the other units involved.[102]

One of the interviewees, a former PSE Planner, added that although the order is officially given by the staff of the TFU, it is often initiated based on information that is acquired at the

[100] Interview PSYOPS2
[101] Interview PSYOPS1
[102] Interview PSYOPS1

lowest level.[103] When for example, during a patrol a TPT finds out that in some areas the attitude towards the coalition forces is unfriendly or even hostile, the information will be communicated through patrol reports to the PSE staff or commander and the TFU staff. This means that the PSE is well posted on the content of a coming order.

After the order from the TFU staff is talked over with other relevant units and the role of the PSE is defined, the information needs can be determined. This is done by the commander and two members of the PSE staff: the Planner and the Target Audience Analyst (TAA). Because the order is often known before it is officially issued, some preparatory work has already been done.

The TAA collects information from digital databases, known as iBase, WiseWeb and the intelligence drive. Additional information then needs to be collected by both the commander and the planner.[104] They will try to collect information that is 'stored' (as knowledge) inside other elements of the TFU (for example the PRT). The TAA then organizes the collected information. He will also store the information in the iBase database. The TAA will also produce annexes to the final TFU order. These orders are shared with the TPTs, the Battlegroup and the TFU and stored in the PSE's own unshared archive.

The use of information takes place during the operation, for instance by the Tactical PSYOPS Teams. After their return the TPTs will be debriefed by a member of the staff (for example the Planner) and are able to express their feedback. However, there is no extensive evaluation that focuses on the entire life cycle as is depicted in

Figure 17.

5.2.2 Exchange of Information

During the preparatory information cycle, there are some moments where the PSE and PRT meet, for example when the order by the TFU staff is issued. When information is collected (internally) the C-PSE and his Planner might also contact the PRT in order to gather the necessary information. These relations, as almost all of the interviewees said, heavily depend on personal relations.

Besides direct contact between the PSE and other units they also communicate through the shared databases. Indirect contact takes place when the C-PSE, Planner or TAA consult these sources or when the TAA stores the collected information in these digital databases.

5.2.3 The Tactical Cycle

The other process that can be identified within the PSE is the tactical information life cycle. This cycle revolves around the TPT and its information gathering activities.

The cycle starts with an order from the PSE commander. He gets his directives from the staff officer PSYOPS. The C-PSE in fact issues his own orders with respect to the instruction from ISAF headquarters (ISAF HQ) in Kabul and Region Command South (RC-S) in Kandahar.

The C-PSE then orders the tactical PSYOPS team to go on a patrol in order to collect information or to spread a message. Besides standard questions the TAA may have identified additional information needs which he communicates to the TPT.

During its patrol a TPT will try to collect relevant information (for instance about living conditions, attitude towards to coalition forces) by observing and communicating with the local population. These patrols can be joint: most of the times a PRT Mission Team will join

[103] Interview PSYOPS1

[104] Interview PSYOPS1

the TPT (or vice versa). Especially on the remote bases the cooperation between the TPTs and the MTs was very close.

During the patrol itself the information can be organised and stored thanks to an armoured laptop. However, the final reports were written after the TPT returned back to the base. The patrol report, the information product, will then be distributed to the TAA who stores it in the iBase database and uses the information for his target audience analyses. Because iBase is a shared database, other units can also use the information gathered by the TPT to fulfil their own information needs.

As with the preparatory cycle, there is again no real feedback loop to identify in this process. The TPT does not receive feedback on the information they gathered. Nor do they receive feedback from other units.

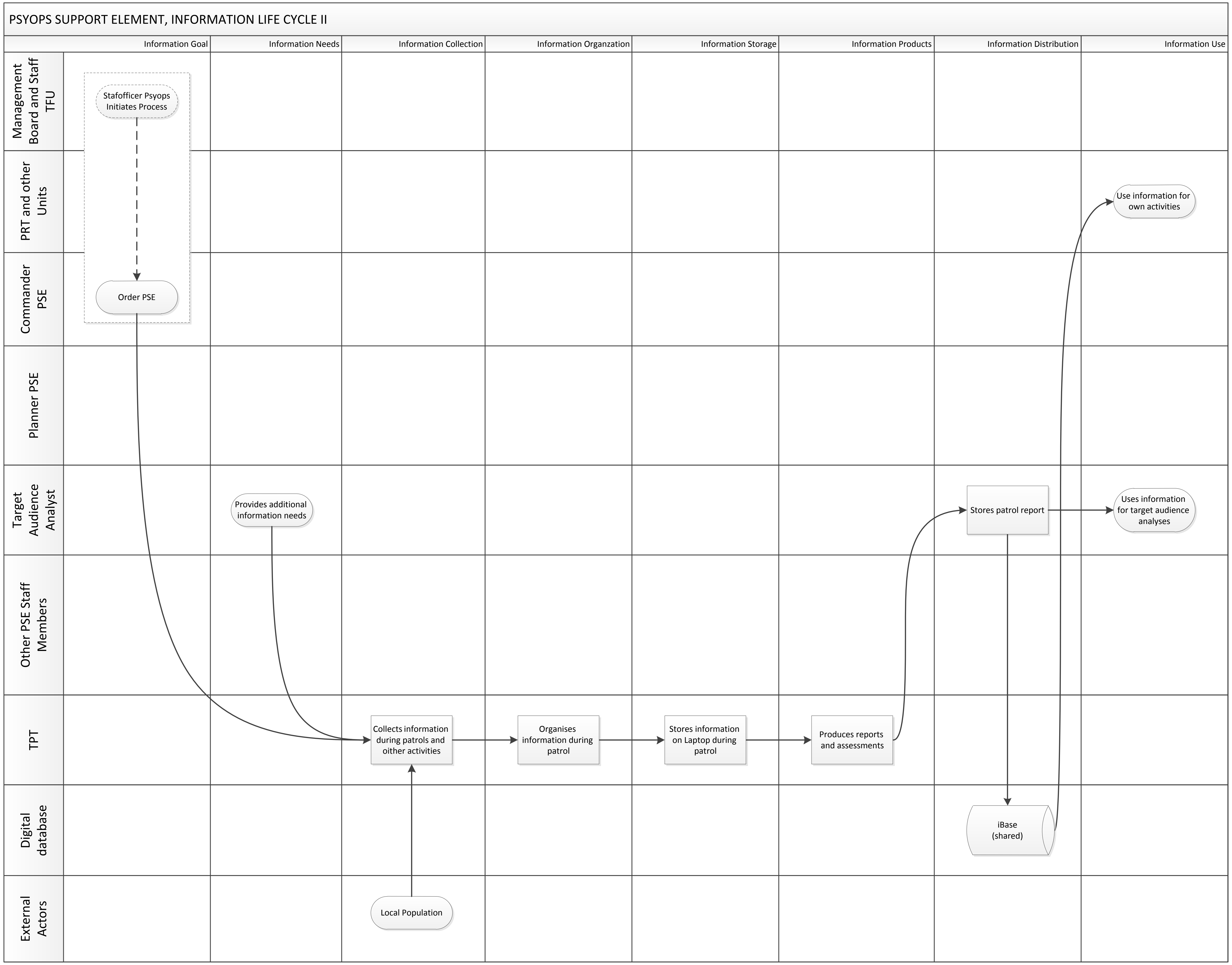

PSYOPS SUPPORT ELEMENT, INFORMATION LIFE CYCLE II
Information Goal
Information Needs
Information Collection
Information Organzation
Information Storage
Information Products
Information Distribution
Information Use
Management Board and Staff TFU
PRT and other Units
Commander PSE
Planner PSE
Target Audience Analyst
Other PSE Staff Members
TPT
Digital database
External Actors
Stafofficer Psyops Initiates Process
Order PSE
Use information for own activities
Provides additional information needs
Stores patrol report
Uses information for target audience analyses
Collects information during patrols and other activities
Organises information during patrol
Stores information on Laptop during patrol
Produces reports and assessments
iBase (shared)
Local Population

Figure 19 PSE Information Life Cycle II

5.2.4 Exchange of information

In the tactical cycle the exchange of information depends on what kind of patrol is ordered. If a MT joins a TPT (or vice versa) the collection of information is a joint activity. Therefore a lot of information is exchanged during the patrol (since they can last up to several days). However, if a TPT goes on patrol alone, the only contact between a TPT and the PRT is indirect: patrol reports are placed on iBase or a local network drive. There is, however, some exchange of information that takes place in informal conversations, during lunch, sport activities etc. Again, these informal contacts heavily dependent on personal relations.

5.3 Challenges

The interviews revealed that the main obstacles for intensive communication can be categorized in five groups: interpersonal relations, need-to-know versus need-to-share, lack of feedback, private databases, and capacity problems. I will briefly discuss them before I turn to the next chapter were I will elaborate on them in order to draw my final conclusions.

First of all, interpersonal relations play a major role when it comes to information exchange. As I indicated before, this is not necessarily a bad thing. On the contrary, via face-to-face communication a more direct and complete type of communication can take place: one can ask for additional information, see the other's response etc. This is recognized by the respondents: informal meetings were a characterized as a great source of information. However, interpersonal relations are heavily dependent on the people involved and their stance towards each other or each other's unit. Therefore the amount and quality of interpersonal relations changes with every rotation. Also trust proved to be an important factor for informal communication.

Together these influences caused all kinds of informal ad-hoc based, get-togethers that illustrate the existence of a 'need to know' culture. Information is shared, but only when the 'owner' of that information thinks it might be relevant for the other unit. This implies that one needs to know what the other's information need is. Since the PRT and PSE were not properly informed about each other's activities and there was hardly given any feedback when information was shared it is hard to believe that this 'need to know' based communication was effective; in fact, it was not.

The interviews also revealed that some tactical teams used private databases to store their information. Although this was done because of a lack of information infrastructure (access to the shared database), keeping information for oneself will of course not improve the communication at all.

Also a lack of collators hampered the information sharing process. Information was added to the shared database in a number of ways, ultimately leading to a confusing environment.

6 CONCLUSION

In some cases the cooperation between the PSE and the PRT during the period from March 2009 up until March 2010 was very close. Especially on the more remote bases the Mission Teams and the Tactical PSYOPS Teams were directly involved in each other's activities. Several former staff officers admitted, however, that cooperation and exchange of information on their level can be improved. In this chapter I elaborate on the challenges that have been identified in the previous chapter, draw some final conclusions and presents recommendation on how to improve the exchange of information.

6.1 Outcomes

In the previous chapters I systematically tried to answer the six questions I posed in paragraph 1.3. The answers, when put together, should answer the main question of how to improve the exchange of information between the PSE and the PRT.

First I found an instrument for analysis that is used to assess the exchange of information. A combination of models from military and non-military information theory resulted in what I called a combined model (Figure 12). It includes two models from the Netherlands Army and the British Army as well as three non-military cycles that represent a more general information management theory. These models complement each other in different ways and each one adds a unique characteristic to the combined model from Figure 12.

The instrument itself, however, had to be applied to the information flow within and between the Provincial Reconstruction Team and PSYOPS Support Element. Therefore these two organizations were discussed in chapters 2 and 3. The characteristics and working methods of both units will have their effect on their information management.

As it turned out it was not easy to apply an abstract model to a real life situation. I therefore had to make a distinction between two kinds of processes: a staff cycle and a tactical cycle. The first one focuses on the preparatory phases of the second and are therefore linked. It is needless the say that in both situations (preparatory or tactical) information plays a vital role.

The internal management of information and the exchange of information are interdependent. The questions on these topics are therefore answered together in chapter 5. Several challenges were then identified in paragraph 5.3. In this paragraph I would like to elaborate on these findings, draw final conclusions and present my recommendations to enhance the communication between the PRT and PSE during future missions.

6.1.1 Interpersonal Relations

Most of the former PRT or PSE members stated during the interviews that good interpersonal relations are very important for effective and efficient exchange of information.[105] Especially informal meetings were considered useful. Examples of informal meetings mentioned during the interviews include places like the 'coffee corner' near the offices of the PRT staff members, the gym and the mess hall. Former PRT intelligence and security officers said that they frequently walked in-to the office of for example the Human Factor Analyst (HFA) or the Senior Analyst from the Military Intelligence and Security Service (both members of the All Source Intelligence Centre or ASIC), to discuss urgent matters.

[105] Interview PRT4, PRT5, PRT7, PRT8, PSYOPS1, PSYOPS4, PSYOPS5, PSYOPS6, PSYOPS7

The same thing goes for the members of the PSE. The editor for example had to setup a relation with the PRT's chief of staff himself in order to get information about upcoming events. Most of these contacts were based on one's own initiatives.

Although the communication was never severely hampered by the rotation of 'counterparts' some of the interviewees explicitly said that they did experience a difference in the amount and quality of the information exchange.[106] One of the PRT intelligence officers for instance, said that he had a lot of contact with the ASIC through the HFA who visited the PRT regularly.[107] However, the exchange of information with the successor of this HFA was less frequent. Notice that, although the HFA is considered the PRT representative within the All Source Intelligence Centre[108], he officially is not (because he is part of the intelligence and security sector of the TFU staff). Nevertheless, this informal relationship illustrates that all kinds of unofficial organizational structures occurred.

A lot of contacts were organized on one's own initiative. A PSE editor for example told that he contacted the PRT's Chief of Staff (CoS) because he simply felt that this would improve the exchange of important information.

Although some meetings institutionalized (for example the meetings between the PRT and PSE when TFU orders were issued) many of the other 'get-togethers' remained informal. There were almost no standards for 'official' meetings. Information was therefore shared on an ad-hoc basis.

The informal relations depended heavily on trust, an important condition for exchanging information and cooperation. An issue that might have influenced the amount of trust between the PSE and the PRT was the way in which the PRT contributed to iBase. Although the PRT did fill iBase (through the TFU Staff), some PSE members were convinced that the PRT did not contribute to the collective database: "The PRT kept the information for themselves".[109] So, although the PRT made real efforts to share information, it was not perceived by the other units as doing so.

6.1.2 'Need to Know' versus 'Need to Share'

In the previous paragraph the importance of one's own initiatives and ad-hoc information-pull indicates the 'need to know' culture that is still dominant. Although a part of the available information is added to a shared database, an important part is kept unshared. That is why all these informal relations were set-up.

There are, however, some serious difficulties with this 'need to know' mind-set. It assumes that it is possible to know, in advance, who will need to use the information. But as some of the former members declared the PRT was not properly informed about the PSE's information and vice versa and hence the units did not push information towards each other.[110] During the interviews various former members told for example that the activities of the PRT were not (extensively) discussed during the preparation phase of a new PSE was send to Afghanistan.[111] The same thing happened during the preparation phase of the PRT: there was no attention paid to PSYOPS and the PSE.

In practice this means that potential opportunities for the PSE are not recognized by the PRT and associated information is thus not shared: for instance a list of PRT projects or upcoming events (the opening of a hydro-electric power station) were not shared with the

[106] Interview PRT4, PRT7, PSYOPS4, PSYOPS5, PSYOP6, PSYOPS7
[107] Interview PRT7
[108] Interview PRT6
[109] Interview PSYOPS2, PSYOPS5, PSYOPS6
[110] Interview PRT4, PRT8, PSYOPS1
[111] Interview PSYOPS1

PSE.[112] On the other hand, a former PRT intelligence officer stated that the messages from the PSE did not match the intent of the PRT.[113]

In order to enable an environment in which the units can share their information on a need to share basis, they need to be fully informed about each other's activities, working methods, tasks and goals.

6.1.3 Lack of Feedback

In chapter 4 the information cycles within the PRT and PSE have been depicted. Almost all processes that are part of the model were found in the actual cycle, except for a feedback loop.[114]

Without a feedback loop the process cannot be adjusted when things can be improved because the processes cannot be evaluated. According to the information gathered through the interviews, the lack of a feedback loop is mainly due to a lack of time. As one of the interviewees said, there basically is no time for an extensive evaluation of the whole process.[115]

At least one of the interviewees, a former TPT commander, asked for feedback on the outcome of the process he was involved in himself.[116] However, a PRT mission team deputy commander stated that he never received feedback from the staff on his patrol reports and assessments.

The debriefings back in the Netherlands were used as an opportunity to evaluate the tour. Although there is some attention paid to information exchange, during the debriefing a new PSE or PRT is already in place.

6.1.4 Private Database

Besides the shared databases (e.g. iBase) there were also private databases used by, for instance the mission teams of PRT 6 and PRT 7.[117] During PRT 8 this situation has changed. The mission teams were no longer allowed to work exclusively with their own private database. They got linked to iBase (except for the teams in Deh Rawod).

When parts of information are not even shared through a collective database within the own PRT, it is unlikely that this information reaches the PSE staff.

6.1.5 Capacity Problems

A lack of collator capacity at TFU staff level caused a confusing digital (iBase) environment.[118] The PSE had access to iBase through its own Target Audience Analyst. The PRT however had to fill iBase through the TFU staff. At some point PRT 8 even choose to fill iBase themselves because the TFU collators added the fragmented information.

PRT 8 also managed to link the mission teams to iBase by giving the teams 'reading rights'. [119] Only the intelligence and security section (S2) from the PRT had the right to 'write' information to the database.

[112] Interview PSYOPS6
[113] Interview PSYOPS7
[114] Interview PRT2, PSYOPS1, PSYOPS2, PSYOPS3
[115] Interview PRT2, PRT 5
[116] Interview PSYOPS3
[117] Interview PSYOPS6, PRT6, PRT7
[118] Interview PRT6, PRT7
[119] See Appendix III for an overview of the PRTs and PSEs in time

Unfortunately the TPTs and MTs in Deh Rawod had no access to iBase because this base was not linked due to security and technical reasons. In order to keep each other up to date, there was contact through telephone. However, these conversations did not suffice. Face-to-face conversations seem to have a lot of advantages that written information exchange lacks: one can express ones feeling for instance through non-verbal communication. The conversation over telephone were assessed as ineffective and time consuming.[120] Although he had frequent contact with the main base in Tarin Kowt, one of the interviewees stated that when he visited the base itself he and his colleagues experienced an ‘information boost’.

6.2 Recommendations

The abovementioned outcomes indicate that some improvement of the information exchange between the PSE and PRT seems to be in place. Therefore I return to the main question of this thesis: How can the exchange of information between the PSE and the PRT be improved? What recommendations can be made based on the analysis of the internal and external management of information in order to improve the exchange of information?

The results of the interviews indicate that although parts of Network Centric Warfare as discussed in Chapter 1 are already incorporated in the military organization (e.g. infostructure and information management) it seems that the PRT and PSE can improve their cooperation and exchange of information much further in order to reach a state of shared awareness. Therefore I will only concentrate on the first three stages of the NCW model: the infostructure, information management and shared awareness (see also Figure 2). The last two stages (self-synchronizing forces and increased combat effectiveness) will be mere results of an effective implementation of the first three.

6.2.1 Infostructure

The technology for implementing a robust ‘infostructure’ is available: virtual databases are accessible and fast, digital lines of communication are used. However, the information infrastructure has some important weaknesses.

One of the most striking examples of a failing infostructure is the lack of access to the shared database iBase. Without sharing the knowledge available within the organizations as a whole, the more distant units cannot get a clear overview of information needs or information that might influence their area of operations. Although they have tried to close this communication gap by daily telephone calls, interviewees indicated that this did not solve the problem.

The use of private databases by tactical teams is related to the requirement of access to shared databases. If parts of the TFU or parts of the PRT (the MTs from PRT 7) use their own unshared databases to store information, that information is kept from the other parts of the organization. In this respect it is quiet similar to the shared databases that were inaccessible to distant units. Private (unshared) databases pose the same threats to a well-functioning information infrastructure and the number of these databases should therefore be reduced. As one of the interviewees said, a single database would be the best solution. Of course such a database would cause all kind of technical challenges, but it would centralize all the available information.

Another major threat to a robust infostructure has been the lack of collators, resulting in poorly filled databases. Collators are a vital part of the infostructure. They are responsible for filling the databases with the information they are provided with. Without enough capacity or

[120] Interview PRT8

training, they cannot fulfil their jobs as good as a well-built information infrastructure demands.

As Figure 2 indicates, infostructure is the basis for NCW. Without a solid foundation, the implementation of network like cooperation will not succeed. Therefore the first recommendation will be to invest in the information infrastructure.

> **Recommendation 1**: Invest in a solid information infrastructure: provide (secured) access to shared information to all units involved; reduce the number of unshared databases; invest in collator capacity so that information reaches the database and is added in a reliable way.

6.2.2 Organization

Much of the NCW related work done by the military has been in technological and operational domains.[121] The Australian Department of Defence published an important report on the human and organizational factors. When it comes to the organizational point of view it seems that the Dutch military organization, at least in Uruzgan, is at a turning point. Historically the military has been organized hierarchically. However, during the mission in Afghanistan informal social networks between the PRT and PSE (but also between other units) emerged almost spontaneously; according to Warne et al. a typical sign of a network centric environment.[122] So instead of working along the hierarchical lines, stove-piping is already prevented by setting up informal ad hoc networks.

The previous paragraph already mentioned that almost all of the interviewees said that cooperation and the exchange of information depends on interpersonal relationships and informal connections between one or more actors. In most cases the exchange of information was based on own initiatives and informal networks that were created during the mission. These kind of relations are useful but they depend on a willingness to cooperate and exchange information, not to mention trust, knowledge about each other's speciality and organizational and physical distance. Although both units are trained and prepared for their duties, not much is spend on each other's field of work. Until the final exercise, the units work in complete isolation of each other. By establishing close cooperation during the preparatory phase, people get the change to know each other and know each other's activities. This will lead to a better understanding of the each other's responsibilities, build trust and more powerful intra organizational networks.

> **Recommendation 2**: Members of both the PRT and PSE should be provided with a thorough understanding of each other's activities during their preparatory phase. This could be done by introducing each other's field of work and combined exercises.

A supportive organizational culture and an good understanding of their systems and the capabilities present in the battlespace are basic needs for a "warrior" operating in a network centric environment that could improve and support the informal networking.[123]

As far as support goes, there are already some signs of improving the organizational environment. In December 2009, the 'Operationeel Stafconcept Taskforce' published the first part of a new concept for the operational staff that describes a network-like environment. In

[121] Warne et al., *The Network Centric Warrior: The Human Dimension of Network Centric Warfare*, 5.
[122] Ibid.
[123] Ibid., 13.

this concept six cells are introduced: a mission environment cell, mission design & assessment cell, a plans cell, a current cell, a mission support cell and an information management cell.

The mission environment cell contains all elements that focus on external influences and the effects of operations on the environment. It will be tasked with the initiating, collecting, processing and disseminating of information and knowledge on the environment in order to support the commanders situational awareness.[124] It is very likely that besides the CIMIC activities PSYOPS will also be incorporated in this cell in order to combine their individual knowledge about the operational environment.

> **Recommendation 3**: The military organization should (continue its effort to) support a networking organizational culture, for example by placing related actors (physically and organizationally) together

Although the network oriented developments are promising, there are also cases known in which the PSYOPS and CIMIC capacity merged into a single (tactical) team. The Austrians, Hungarians, Belgians and Canadians for example operate in this way, combining the two units in highly specialised teams.

6.2.3 Evaluation

When the Information flow model was applied to the information cycles of the PRT and PSE, it appeared that no feedback loop was in place. This means that no standardized system of evaluation is used. There are no indications that the process of information gathering, organizing, storing and dissemination are assessed. No feedback is given on information provided by the own tactical teams, nor is there any response given to information that was provided by other units.

Because of a lack of feedback, no organizational learning can take place. Without an evaluation phase the military organization in general, and the units involved in particular cannot improve their information flows in terms of efficiency and effectiveness. Only afterwards, when the units had returned to The Netherlands, a debriefing took place that evaluated the operation as a whole. This situation leaves almost no space for assessing the information cycle within the PRT or PSE, let alone the exchange of information between them.

The main reason, as suggested by one of the respondents, might be a lack of time. However, feedback and evaluation can increase the efficiency of the information flow: communicating the value and significance of the information offers the provider of it with useful instructions for future information sharing.

> **Recommendation 4**: Introduce a consistent form of feedback to the information flows within and between units.

6.2.4 Platform-centric versus Network-centric

All things considered I would argue that the Dutch military organization has arrived at some sort of transitional phase in which a hierarchy is confronted with networking capabilities. As the previous chapter and the aforementioned paragraphs indicate, there is a strong information technical development that enables but also forces the organization into a

[124] Operationeel Stafconcept Taskforce, "Operationeel Stafconcept," (2009).

new kind of structure. The information infrastructure with its shared databases and digital communication has a lot to offer in terms of efficiency and effectiveness, but the military needs to adjust its organization in order to fully use its potential.

As the case of the exchange of information between the PRT and PSE indicate the ‘infostructure’ is used, but the organization (i.e. the military men and women) often revert to hierarchical procedures, resulting in organizational stovepipes.

Hierarchical lines, especially in the military, are very important. However, now that information technology offers networking capabilities that could increase the situational awareness, the military organization can no longer ‘deny’ the need for organizational adjustments.

In the current situation information exchange takes place, but on an incidental basis. Minor adjustments in the preparation phase, a solid information infrastructure, together with introducing information flow evaluations and a supportive organizational structure, could lead to an growing amount of effective and efficient information exchange and thus an increasing situation awareness.

6.3 Future research

These recommendations should further improve the awareness of (military) organizations in general. Though, as I hope to have indicated through my introduction, an improved situational awareness is especially needed when operating in a counterinsurgency environment. It is in these chaotic conflicts that an accurate overall view is necessary.

In this study I focussed my attention to only two important actors on the side of the military. However, future research could also include other actors that are involved in similar practices on the side of military organizations. Information is of course not only gathered by the PRT or PSE. There is in fact a whole range of teams that influence the battlespace awareness: from the regular (military) intelligence agencies to the single rifleman.

I realize that a study that includes more of these actors could very well grow exponentially: every new actor introduces numerous new links to other organizations not to mention the internal information process that needs to be analysed.

On the other hand, one could decide to study the implementation of network-centric warfare or another cluster-like organizational structure, and its effect on the efficiency of constructing a clear view on the battlespace. How do individual clusters communicate? How does a decentralized structure mix with an hierarchic military organization? How do people adapt to these new circumstances?

It is my hope that the answers to these questions, together with the results of the study that lies before you, will eventually make it a lot easier to eat soup with a knife.

BIBLIOGRAPHY

Alavi, Maryam, and Dorothy E. Leidner. "Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues." *MIS Quarterly* 25, no. 1 (2001): 107-36.

Alberts, D.S., J.J. Garstka, and F.P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington: CCRP, 2000.

Alberts, D.S., and R.E. Hayes. *Power Top the Edge: Command... Control... In the Information Age*. Washington: CCRP, 2003.

Ayer, A.J. "What Is Communication?" In *Studies in Communication*, edited by A.J. Ayer, J.Z. Young, J.B.S. Haldane, R. Wittkower, Colin Cherry, T.B.L. Webster, Geoffrey Vickers, Randolph Quirk, D.B. Fry and B. Ifor Evans, 11-28. London: Martin Secker & Warburg, 1955.

Bellinger, Gene, Durval Castro, and Anthony Mills. "Data, Information, Knowledge, and Wisdom." Systems Thinking, http://www.systems-thinking.org/dikw/dikw.htm.

Brei, William S. "Getting Intelligence Right: The Power of Logical Procedure." (1996).

Brocades Zaalberg, Thijs W. "'Hearts and Minds' of 'Search and Destroy'." *Militaire Spectator* 176, no. 7/8 (2007): 288-301.

Brown, S.L., and K.M. Esienhardt. *Competing on the Edge: Strategy as Structured Chaos*. Boston: Harvard Business School Press, 1998.

Choo, Chun Wei. "Information Management for the Intelligent Organization: Roles and Implications for the Information Professions." In *Digital Libraries Conference*. Singapore, 1995.

Daft, R.L., and A.Y. Lewin. "Where Are the Theories for The "New" Organizational Forms? An Editorial Essay." *Organzation Science* 4 (1993): i-vi.

Dance, Frank E.X. "The "Concept" Of Communications." *The Journal of Communication* 20, no. 2 (1970): 201-10.

Den Boer, Jelmar. "Informatie-Uitwisseling Tussen Het Mission-Team, Tactical Pys-Ops Team En Het Field Humint Team." Nederlandse Defensie Academie, 2008.

Department of Defense. "Joint Publication 3-24 Counterinsurgency Operations." edited by Department of Defense. Washington: Department of Defense, 2009.

Department of the Army. "Field Manual 3-24 Counterinsurgency." edited by Department of the Army. Washington: Department of the Army, 2006.

Development Concepts and Doctrine Centre. "Information Management." edited by Ministry of Defence. Swindon: Ministry of Defence, 2006.

Galula, David. *Counterinsurgency Warfare: Theory and Practice*. London: Pall Mall, 1964.

Hall, Micheal T., and Stanley A. McChrystal. *Isaf Commander's Counterinsurgency Guidance*. Kabul: International Security Assistance Force, 2009.

International Security Assistance Force. *Provincial Reconstruction Team Handbook*. Kabul: International Security Assistance Force,, 2009.

Jones, Seth G. *Counterinsurgency in Afghanistan*. Vol. 4, Rand Counterinsurgency Study. Santa Monica: RAND Corporation, 2008.

Kilcullen, David. "Counterinsurgency Redux." *Survival* 48, no. 4 (2006): 111-30.

———. "Three Pillars of Counterinsurgency." In *U.S. Government Counterinsurgency Conference*. Washington, 2006.

Koninklijke Landmacht. "Leidraad Inlichtingen." edited by Ministery of Defense. The Hague: Koninklijke Landmacht, 2006.

———. "Vs 2-1353 Handboek Cimic." edited by Ministerie van Defensie. The Haque: Koninklijke Landmacht, 2002.

Krizan, Lisa. "Intelligence Essentials for Everyone." (1999).

McCormick, Gordon H. "Things Fall Apart: The 'Endgame Dynamics of Internal Wars'." RAND.

Ministerie van Defensie. "Joint Doctrine Bulletin 2008/01: "Provincial Reconstruction Teams" Inzet in Afghanistan." edited by Ministerie van Defensie. The Hague, 2008.

Ministry of Defence. "The Netherlands' Approach to Its Prt Operations in Afghanistan?". The Hague: Ministry of Defence, 2007.

NATO. "Aap-6 Nato Glossary of Terms and Definitions." edited by NATO Standardization Agency. Brussels: NATO, 2009.

———. "Ajp-3.7 Nato Psychological Operations." edited by NATO. Brussels: NATO, 2002.

———. "Ajp-9 Nato Civil Military Co-Operation (Cimic)." edited by NATO. Brussels: NATO, 2003.

———. "Ajp-9(a) Nato Civil Military Co-Operation (Cimic)." edited by NATO. Brussels: NATO.

———. "Mc 402/1 Nato Military Policy on Psychological Operations." edited by North Atlantic Military Committee. Brussels: NATO, 2003.

———. "Mc 422/1 Nato Military Policy on Information Operations." edited by North Atlantic Military Committee. Brussels: NATO, 2002.

———. "Mc 457 Nato Military Policy on Public Information." edited by North Atlantic Military Committee. Brussels: NATO, 2001.

Operationeel Stafconcept Taskforce. "Operationeel Stafconcept." 2009.

Opleidings- en Trainingscentrum Operatiën. "Doctrinebulletin 07/02: Counter Insurgency (Coin) En De Militaire Bijdrage." Amersfoort: Opleidings- en Trainingscommando, 2007.

Rietjens, Sebastiaan J. H., Kirsten Verlaan, Thijs W. Brocades Zaalberg, and Sirp De Boer. "Inter-Organisational Communication Iin Civil-Military Cooperation During Complex Emergencies: A Case Study in Afghanistan." *Distasters* 33, no. 3 (2008): 412-35.

Royal Netherlands Army. "Combat Operations Adp Ii - Part C: Combat Operations Againts an Irregular Force." edited by Ministery of Defence. The Hague: Royal Netherlands Army, 2003.

———. "Leidraad Inlichtingen." edited by Ministery of Defense. The Hague: Royal Netherlands Army, 2006.

Royal Netherlands Embassy. "Civil Assessment Urzugan Province, Afghanistan Executive Summary." Kabul, 2006.

Schraagen, Jan Maarten, Mirjam Huis in 't Veld, and Lisette De Koning. "Information Sharing During Crisis Management in Hierarchical Vs. Network Teams." *Journal of Contingencies and Crisis Management* 18, no. 2 (2010): 117-27.

Shannon, Claude Elwood. "A Mathematical Theory of Communication." *The Bell System Technical Journal* 27 (1948): 379-423, 623-56.

Shannon, Claude Elwood, and Warren Weaver. *The Mathematical Theory of Communication*. Champaign: University of Illinois Press, 1963.

Tiggelman, P.J.J. "Psychologische Operaties: Treffers Zonder Met Scherp Te Schieten." edited by Koninklijke Landmacht. Utrecht: Koninklijke Landmacht, 2006.

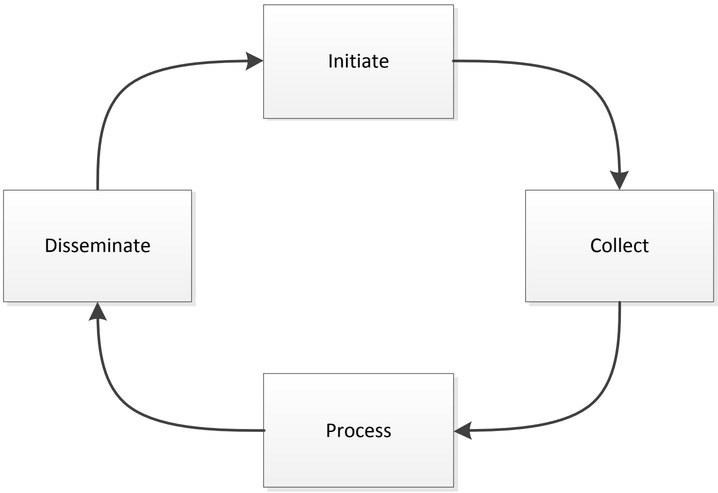
Van der Woerdt, J. "Toelichting Op De Rol Van Cimic in Militaire Operaties." edited by Ministerie van Defensie. The Hague: Ministerie van Defensie, 2007.

Warne, Leoni, Irena Ali, Derek Bopping, Dennis Hart, and Celina Pascoe. *The Network Centric Warrior: The Human Dimension of Network Centric Warfare*. Edinburgh: DSTO Information Sciences Laboratory, 2004.

Weggeman, Mathieu. *Kennismanagement: Inrichting En Besturing Van Kennisintensieve Organistaties*. Schiedam: Scriptum, 1997.

APPENDIX I

The Royal Netherlands Army Intelligence Cycle[125]



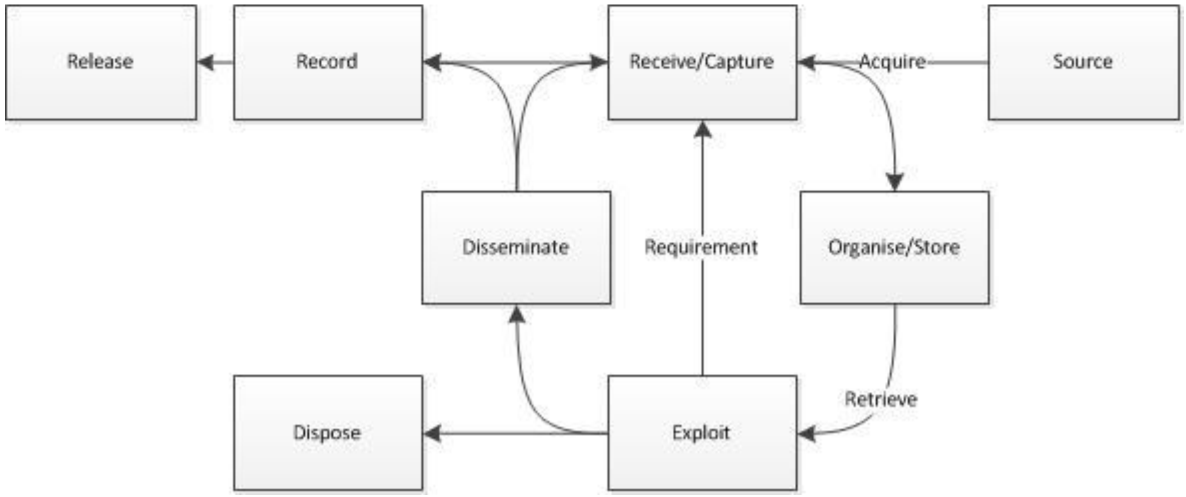
The basic Intelligence Cycle described in the intelligence handbook comprises of four basic steps: an initiation phase, a collection phase, a processing phase and a dissemination phase. Although the cycle seems rather basic, each phase contains sub-processes.

In the initiation phase, the commanders formulates his information need, a schedule is made and assignments are issued to those who collect the information. During the second phase, the information is collected, checked and delivered according to the schedule made during the initiation phase. The processing phase is where information becomes intelligence. The collected information from the previous phase is “collated, evaluated, analysed, integrated and interpreted”.[126] When the intelligence is produced, the end-product is disseminated, either actively (push) or passively (pull). The commander, who initiated the intelligence cycle will be presented with an intelligence product. Based on this product and additional information needs the cycle can be reinitiated.

[125] Koninklijke Landmacht, "Leidraad Inlichtingen," ed. Ministery of Defense (The Hague: Koninklijke Landmacht, 2006), 41.

[126] Ibid.: 52.

The British Information Life-Cycle[127]



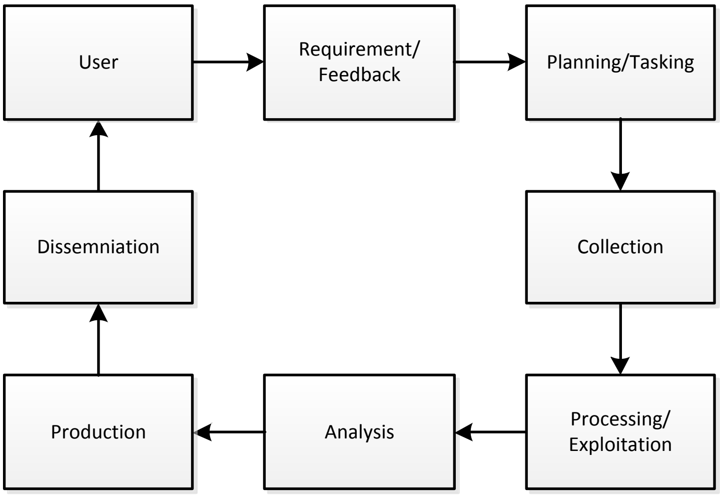
The Joint Doctrine Note on information management of the British Development Concepts and Doctrine Centre does not elaborate much on the steps in the Information Life-Cycle. However, it adds some important phases to the abovementioned intelligence cycle. The information life cycle adds a disposal and record phase. Although I have not included the disposal phase in the model I have used in this study (because information or intelligence can be lost throughout the information cycle, that is during each individual process), I do see the need for a storage phase. "The cycle is not complete until information is discarded, archived or released into the public domain".[128]

Instead of placing this record or storage phase at the 'end' of the cycle (as if there is something like an end to a cycle), I placed the storage phase in the 'middle' of it, accessible to both the collectors of information as well as those disseminating the end-product. By doing so recorded information or intelligence can be used as a source to fulfil future information needs.

[127] Development Concepts and Doctrine Centre, "Information Management," 4.

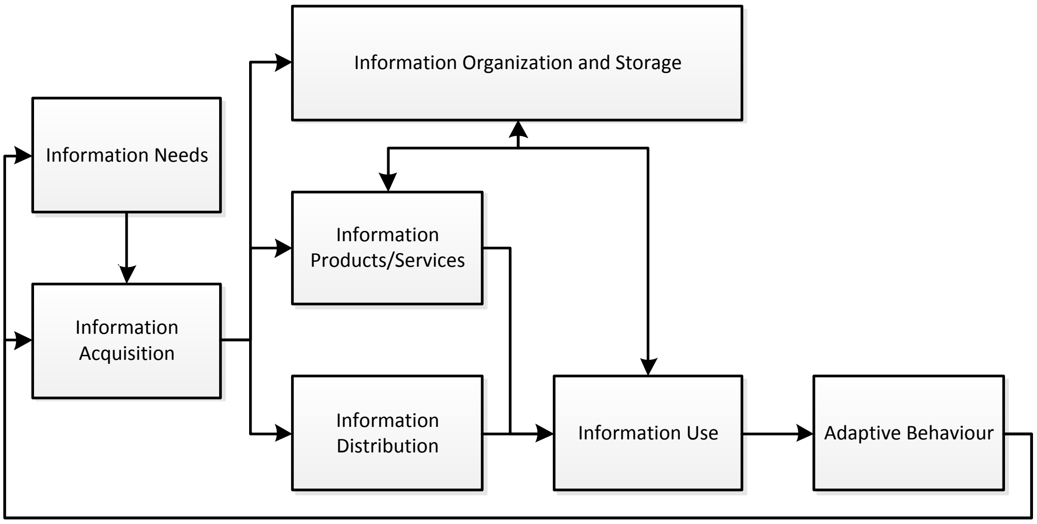
[128] Ibid.: 4.

Krizan's Process of Intelligence Creation and Use[129]



Krizan agrees with the model of the Royal Netherlands Army that the production of intelligence follows a cyclical process. In the model that she presents a lot of the previously mentioned phases can be recognized. Again, an information need has to be formulated (requirements), the collection, production and dissemination activities need to be planned and people or groups of people need to be tasked with them (planning/tasking). Next information needs to be gathered, processed, analysed (in order to turn it into intelligence) and turned into a product that can be disseminated to various users of that intelligence. Based on their experience, feedback will be provided in order to improve the process or start a new cycle.

Choo's Information Management Cycle[130]

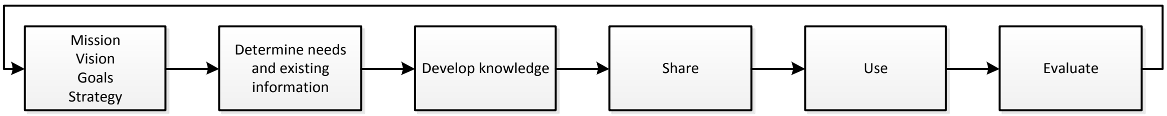


In Choo’s information management cycle one can recognize a lot of phases that are described in the abovementioned models. However, what this particular model made me decide to include it is the central role for information storage that I mentioned when I described the British information life cycle.

[129] Krizan, "Intelligence Essentials for Everyone."
[130] Choo, "Information Management for the Intelligent Organization: Roles and Implications for the Information Professions."

Again, the process starts with a certain information need, that triggers the acquisition of information. Next Choo chooses to organize and store, produce and distribute the information. Note that this model does not include a processing phase as the intelligence cycles do. However, the information storage functions as a database that can be used to make products or provide services (that can be stored in the same database). Also note that the adaptive behaviour phase indicates a form of feedback in order to improve the cycle as a whole.

Weggeman's Knowledge Chain Model[131]



Weggeman’s chain model does not add that much to the previous models, but includes a phase in which mission, vision, goals and strategy are defined. Especially in a military environment the information needs will be based on a broader strategy and goals other than collecting information or intelligence. The end-product will be used to plan new strategies, missions and activities.

[131] Mathieu Weggeman, *Kennismanagement: Inrichting En Besturing Van Kennisintensieve Organistaties* (Schiedam: Scriptum, 1997).

APPENDIX II

In order to avoid the loss of any meaning (intended or unintended) and to give the most accurate image of the questions asked, they are presented in the language they were posed.

Information Goal

1. Wat voor soort opdrachten ontving uw eenheid gedurende uw uitzending?
2. Van wie ontving uw eenheid deze opdracht?
3. Hoe duidelijk waren de opdrachten die u ontving?
4. Hoe uitvoerbaar waren de opdrachten die u ontving?
5. Waren de opdrachten van het PRT/PSE bij u bekend?

Information Need

1. Wie stelde binnen uw eenheid vast welke informatie noodzakelijk was om de opdrachten te vervullen en het gestelde doel te bereiken?
2. Hoe werd die informatiebehoefte kenbaar gemaakt?
3. Sloot de gestelde informatiebehoefte aan op het informatiedoel?
4. Welke vragen kreeg een patrouille (standaard) mee?
5. Bleek uit de gestelde informatiebehoefte voldoende welke informatie moest worden vergaard?
6. Was u op de hoogte van de informatiebehoefte binnen het PRT/PSE?
7. Hoe verliep het overleg met het PRT/PSE en andere eenheden?

Information Collection

1. Welke onderdelen van het PSE/PRT waren actief bezig met het verzamelen van informatie?
2. Welke interne bronnen werden bij het verzamelen van informatie geraadpleegd (interne databases, informatiesystemen, andere eenheden)?
3. Wie heeft toegang tot iBase/WiseWeb? (alleen TAA of ook C-PSE en Planner?)
4. Welke externe bronnen werden bij het verzamelen van informatie geraadpleegd?
5. Is er bij het verzamelen van informatie contact geweest met het PRT/PSE? Zo ja, in welk mate?
6. Werd informatie actief (dat wil zeggen zonder directe informatievraag vanuit uw PSE/PRT) aangeleverd door het PRT/PSE?
7. Bent u obstakels tegengekomen bij het onderhouden van contact met het PRT/PSE?
8. Heeft u achteraf het idee gehad dat er door uw PSE/PRT informatie is verzameld die reeds binnen de organisatie beschikbaar was? Waar is dit aan te wijten?

Organizing and Storing Information

1. Wie was binnen uw eenheid verantwoordelijk voor het organiseren van verzamelde informatie?
2. Wordt verzamelde informatie door TPT tussentijds geordend/georganiseerd voordat een patrouille rapport of civil assessment geschreven wordt?
3. Wordt ruwe informatie tussentijds opgeslagen of komt alleen het (eind)rapport in iBase terecht?
4. Wie slaat het civil assessment op WiseWeb op?
5. Sloot de informatie afkomstig van het PRT/PSE (qua *format*, medium, taal, taalgebruik) aan op de informatie zoals die binnen het PSE/PRT beschikbaar was?
6. Is er digitale informatie gedeeld met het PRT/PSE?
7. Hoe frequent is informatie op deze manier gedeeld?
8. Zijn er problemen geconstateerd tijdens deze manier van informatie overdracht?

9. Werd informatie opgeslagen in een (centrale) database? Zo ja, was deze database gedeeld met andere eenheden (waaronder het PSE/PRT)?
10. Heeft u informatie gedeeld via intermenselijke contacten (*face-to-face,* telefonisch)?
11. Hoe frequent is er op deze manier contact tussen het PRT en het PSE geweest?
12. Zijn er problemen geconstateerd met betrekking tot deze contacten?
13. Zijn er *hardcopy* documenten gedeeld met het PRT/PSE?
14. Hoe frequent is er op deze manier contact geweest tussen het PRT en het PSE?
15. Zijn er problemen geconstateerd met betrekking tot deze contacten?
16. De TAA is los van de rest van het PSE geplaatst binnen het ASIC. Heeft dit voor problemen gezorgd?

Development of Information Product

1. Wie was binnen uw organisatie verantwoordelijk voor het opstellen van informatieproducten (rapporten, briefings etc.)?
2. In welke taal werden deze producten opgesteld?
3. Werden patrouillerapporten volgens een bepaalde standaard opgemaakt?
4. Werden deze producten opgeslagen in een (gedeelde) database? Zo ja, voor wie was deze database toegankelijk?

Information Sharing

1. Wie was binnen uw eenheid verantwoordelijk voor het verspreiden (delen) van informatieproducten?
2. Beschikte u over de juiste (technische) middelen om informatie(producten) te verspreiden?
3. Werd informatie op een (gedeelde) database beschikbaar gesteld aan derden?
4. Wordt informatie op iBase volgens een vast *format* aangeleverd (taal, zoektermen, gebruik van namen etc.)?
5. Naar wie werd het door u geproduceerde informatieproduct verspreid?
6. Deelde u eindproducten met het PRTPRT/PSE?

Information Use and Feedback

1. Was de informatie verzameld door uw eigen PSE/PRT, aangevuld met informatie vanuit het PRT/PSE, bruikbaar?
2. Werd het informatieproces binnen het PSE/PRT geëvalueerd?
3. Werd de uitkomst van het evaluatieproces gedeeld met het niveau waarvandaan u de opdracht ontving?
4. Wordt er door de TAA feedback gegeven op de verzamelde informatie door TPT?
5. Bestaat de mogelijkheid om via iBase of WiseWeb feedback te geven op verzamelde informatie?
6. Kreeg u anderszins feedback op verstrekte informatie aan het PRT/PSE?

APPENDIX III

PRTs and PSEs in time

	2008		2009												2010		
	nov	dec	jan	feb	mar	apr	may	jun	jul	aug	sep	oct	nov	dec	jan	feb	mar
PRT	PRT 6					PRT 7						PRT 8					
PSE		PSE 8				PSE 9				PSE 10				PSE 11			

Interviewees CIMIC/PRT

ID	Function	Date
PRT1	Staff Officer CIMIC CSE	15-05-2010
PRT2	Director PRT (CIVREP)	27-05-2010
PRT3	Commander PRT	09-06-2010
PRT4	Chief of Staff PRT	09-06-2010
PRT5	Chief of Staff PRT	10-06-2010
PRT6	S2 officer PRT	09-06-2010
PRT7	S2 officer PRT	10-06-2010
PRT8	Deputy Commander MT	15-06-2010

Interviewees PSYOPS/PSE

ID	Function	Date
PSYOPS1	PSYOPS Planner	11-05-2010
PSYOPS2	Commander PSE (staff officer PSYOPS)	31-05-2010
PSYOPS3	Commander TPT	31-05-2010
PSYOPS4	Deputy Commander TPT	25-05-2010
PSYOPS5	Target Audience Analyst	31-05-2010
PSYOPS6	Editor	31-05-2010
PSYOPS7	Editor	02-06-2010