The Battle for the Information Domain

By Major Rob Sentse[1] Bachelor. Infantry, Royal Netherlands Army and Major Arno Storm, Bachelor. Infantry, Royal Netherlands Army

(This publication has been written on our personal title and does not reflect the opinion of the Royal Netherlands Army.)

"I've learned that people will forget what you said, people will forget what you did, but people will never forget how you made them feel."

–Maya Angelou (American Poet, b.1928)

Influencing Behaviour: The basic principle for education, training exercises and operations

In this paper we cover the need for exchanging and broadening international insights and expertise on Influence Operations as a whole and Information Operations in particular. We describe the way to operate in an expanding technology and communication era and we will conclude with a description on how to organize exercises starting from complementary factors of influence. This paper describes the way military forces could operate in the current and expanding communication and technology era.[2]

We would like this paper to fuel discussions regarding the viability of line staff organizations, the way we should organize our armed forces and the way we should arrange our training and exercise programs. While we do not have a solution to the many challenges in this field, we hope that this paper will contribute to the creative minds working on these issues.

The communication and technology era influences the way we relate to politics, populations, society and the media. To be specific, this technology era influences:

a) The positions the population and government take in the area of operations;
b) The positions the population and government take in the countries which relate to the conflict;[3]
c) The positions the population and the government take in countries contributing troops to international missions.

Future conflicts will be complex and non transparent, which will require a nation's military to respond with flexibility, creativity and speed. Our traditional military way of thinking has evolved into an interagency[4] way of acting in which the armed forces are to shape the conditions for development, security and diplomacy.

In our present and future areas of operations it will be hard to find a clear distinction between permissive, semi-permissive and non-permissive elements, as these three concepts tend to emerge at the same moment. The primary behaviour we would like to influence is in urban areas. Future conflicts arise in part from the need for political freedom, power, water, food, energy and living space. The interagency environment is not well supported by the current line staff organization, an organization type that often leads to internal conflicts, competition and containment of networks in favour of personal ambition instead of organizational goals.

The limits of present line staff organization require changes be made. One solution may be a process organization consisting of modular units. One of the positive effects of this model would be a decrease of restraints whilst solutions and creativity will be magnified causing desired effects immediately.[5] A modular process organization could be the answer to current line staff organization difficulties.

Surviving and Living at the Speed of Information

It is conceivable that future conflicts will occur in that part of the world where 70 percent of the world population lives at 30 percent of the earth's surface. Asia (1.2 billion in China and 1.1 billion in India) will suffer the consequences of the ever-growing world population. [6] Due to the many failed and failing states in Africa, it should be closely monitored as well.[7]

Population growth is a major concern to be reckoned with, also and maybe particularly in Africa, the population at this continent has grown up to 1 billion. Specialists estimate a 9 billion-world population density by 2050, resulting in a massive increase of urbanized areas and a huge demand for food, water and energy. [8]

Influencing the behaviour of people and of the other parts of the information domain is fundamental and the armed forces have a role in this interagency approach. Developing awareness of the broad area of activities necessary to influence behaviour requires creative and pro-active minds. It is not simply about "every soldier a rifleman" nor is it about "every soldier a sensor." It could best be summarized as: "every soldier is a tool of influence."

Get to know your opponent and change him into your companion. [9] To achieve this, we have to develop an emphatic mind concerning the ethics, values, norms and culture in the area of operations (AO) and in the areas that influence the AO. This requires a well thought coordinated and synchronized approach of all behavioural aspects to control the information domain in its broadest sense.[10]

For instance, the "developed" countries perspective towards the problems in the Middle East is far different from the perspective of the governments and people living in those nations.

The human quality to perceive worldwide problems from its own values and norms is one of the very few characteristics in which "we" recognize ourselves. The freedom and democracy "we" like to bring to "them" is something "they" experience quite differently. The "killing," and "battle," which happens in moral, cultural, and psychological spheres is far stronger than any physical or kinetic harm inflicted.

Powerful nations fight a different kind of war than their opponents do. This problem leads to a question we should ask ourselves: In whose perceptions is it the opponent and, above all, WHY is it the opponent? [11] The following terms relate to our unique perception: terrorists, resistance, guerrillas, criminal gangs, freedom fighters; labelling refers to the "ally" or to the "enemy." Still, they all have one thing in common. They are all (in different ways) supported by a part of the local population and/or (a foreign) government or governments.

The opponent is not recognizable as such and has the initiative as one of its most typical aspects. [12] Our opponents use continuous technological developments to their advantage. An instrument, often employed by insurgents, is to play to the perceptions of opponent policymakers and audiences, throughout the media, to convince their enemy that their goals are unachievable or too costly.

> *"…any sound revolutionary war operator (the French underground, the Norwegian underground, or any other European anti-Nazi underground) used small-war tactics – not to destroy the German Army, of which they were thoroughly incapable,* but to establish a competitive system of control over the population. *To do this…they had to kill some of the occupying forces and attack some of the military targets. But above all they had to kill their own people who collaborated with the enemy."*[13]
>
> -Bernard Fall

In such an environment many variables influence the outcome of our actions. One thing is clear; the way, in which democratic countries choose to deal with insurgents and terrorists, is related to the increase or decrease of support for this issue from their policy makers and their troops. One needs to take this into account and try to positively influence the perceptions of the local population, potential supporters of the insurgents abroad, allies and neighbouring countries; thus increasing resilience against insurgents to ensure support for our own efforts. [14] Dealing with different variables in a concerted manner requires a balanced approach to coordinate how efforts and information flows are to be organised. [15]

If this is not done correctly it will lead to a situation that is prone to producing efforts that are counter-productive to the political and strategic goals. Furthermore, efforts can be counterproductive for other parts of the organisation or its partners. The challenge is to seek methods to reduce undesirable outcomes. Establishing a common starting point for planning and action is fundamental in a battle in which perception is more important then facts. The "opponent" seems to achieve their goal with 15% violence and 85% by controlling the information domain and "we" as the military respond to that with 85% violence and 15 % control of the information domain, leading us to the question: "Who is effective here?" [16-17]

In such an environment there is no space for stove piped visions like "kinetic elements" or "non-kinetic elements" as the interconnection and the mutual influence of these concepts are fundamental in a coexisting permissive, semi permissive and non permissive environment. [18]

> *"It is obvious that the media war in this century is one of the strongest methods; in fact, its ratio may reach 90% of the total preparation for the battles."*[19]
>
> -Osama Bin Laden

Influencing Behaviour and the Information Domain: Two mutually reinforcing concepts

In the aftermath of the elections in Iran in June 2009, "Twitter" turned out to be a powerful medium to activate, inform and influence. [20-21] Obtaining and maintaining influence is no longer solely a military capacity and has evolved into a symbiosis of the information domain with the military instruments of influence.[22] This international challenge needs more attention from other armies.

In December 2008, a conference was held at the Netherlands Institute of International Relations, Clingendael, in The Hague. This conference was named, "*Challenging uncertainties, the future of the Netherlands Armed Forces,*" in which the effects of the "Information and Communication era" were explored. [23] Professor Alex Schmid, Director of the *Centre for the Study of Terrorism and Political Violence* at the University of St. Andrews in Scotland addressed the fact that the success of terrorist actions depends on their access to technological means of communication. This principle is important to our consideration and practice of Influence operations and Information Operations, which can complement each other in the information domain. There is a great deal of room for improvement in this area.

To describe the RLNA's perspective of Influence Operations we would first like to consider the views of some NATO partners. Influence Operations, as terminology in the RNLA is non-existent whilst Information Operations as part of Influence Operations is still under construction, not only in the Netherlands but also in the USA and the UK. The American Armed Forces and the Armed Forces of the United Kingdom have made a great deal of progress on

Influence Operations. Within the UK Army's doctrine, Information Operations is a component of Military Influence, which, on its part, contributes to Influence Operations.

The following illustration is part of the "*UK Influence Doctrine 2009*," among the cadre of Influence activities, the term Information Operations can be seen. Within brackets you see: "coord." The Information Operations officer is responsible for synchronization and coordination.

According to the UK definition, Information Operations are: *"A military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capability of audiences, consistent with a UK Information Strategy."* [24]

The UK Army's doctrine is advanced, both in their vision and policy when it comes to influencing behaviour. UK "Influence Campaigns" are conducted by several ministries. At the level of the Chief of Defence Staff, the Targeting and Information Operations (TIO) office coordinates and synchronises the MoD actions within an interagency environment. TIO consists of a Targeting, Policy & Capability and an Info Ops desk. The Targeting desk also consists of an Intelligence Support Team. [25]

Also the US Army has a well-developed vision of Influence Operations, although it seems that the execution of it does not entirely relate to the well thought-over documents about the important subject. According to the American non-profit think-tank, *RAND*, Influence Operations are: "*the coordinated, integrated, and synchronized application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviours, or decisions by foreign target audiences that further interests and objectives."[26]*

Another US Military document is the *Allied Joint Doctrine for Information Operations*, Ratification Draft 1 (AJD-3.10 RD1). This document uses the same definition as NATO document MC422/3 (NATO Military Policy on Information Operations): *"Info Ops is a military function to provide advice and coordination of military information activities in order to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other NAC approved parties in support of Alliance mission objectives. Information activities are actions designed to affect information and or information systems. They can be performed by any actor and include protective measures."*

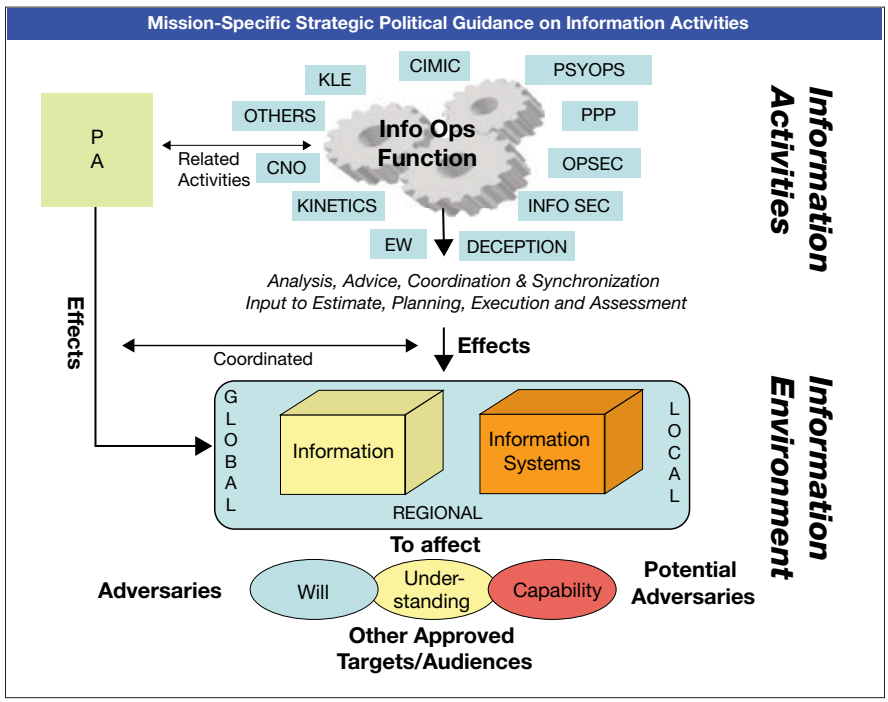
The AJD-3.10 RD1 also mentions the Information Operations Coordination Board (IOCB). This is the forum for the implementation of Information Operations (Info Ops), collective coordination and advice. This board, chaired by the Chief of Information Operations, meets as a subset of the Joint Coordination Board (JCB). It will convene as necessary in the Headquarter decision cycle and during non-operational activities. Ideally the IOCB is part of the decision cycle at every level and at every moment. This board should contribute to the militaries mindset, (and to other governments) to plan and execute operations.

Besides the AJD.3-10 RD1; the American Joint Publication 3.13 "*Information Operations(IO)*" describes IO as: *"Information operations (IO) are described as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own."*

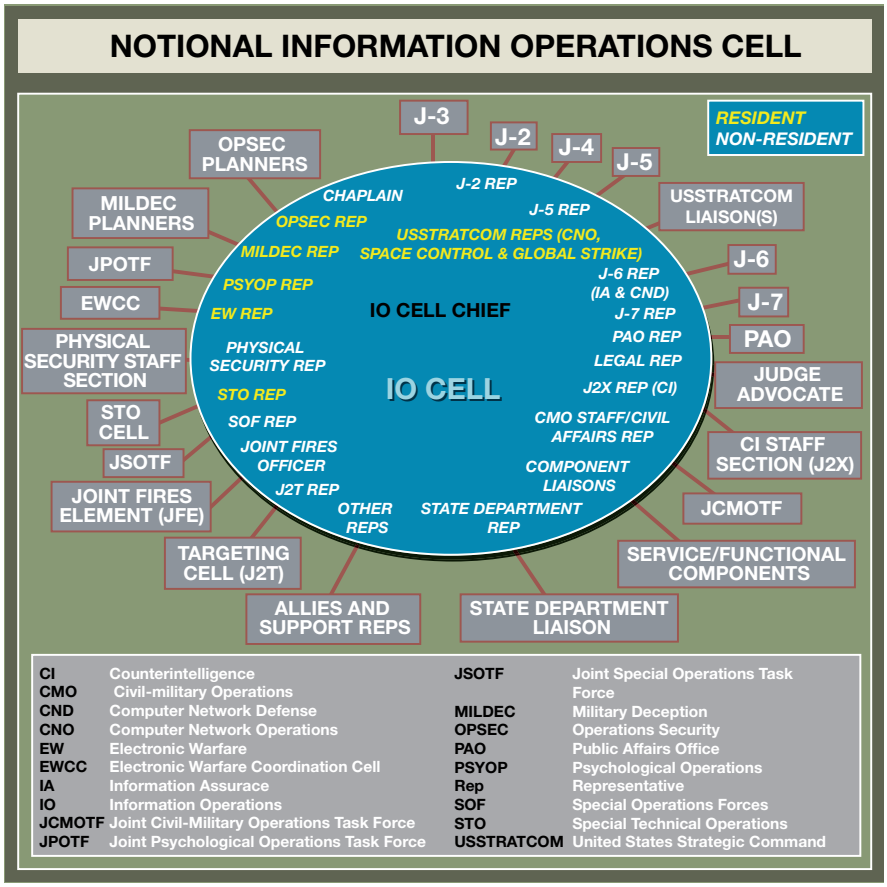
This document refers to the "Notional Information Operations Cell" (page IV-5); ideally this should be the design used at headquarters. Although advisable to implement; this proposed layout has to be established by experience. One of the advantages is that all core "tools" of influence will be together permanently with the opportunity to consult their subject matter experts.

Within the RNLA; Influence Operations is not staffed as such and Information Operations is still under construction. The authors of this article recommend the conceptualization of a common understanding designed toward influencing behaviour as a whole. In the RNLA the functionality "Staff officer Information Operations" is foreseen at the brigade level. The RNLA consists of two manoeuvre brigades (13th and 43rd), one air mobile brigade (11th) and one support brigade. A brigade headquarters will, amongst others, consist of three staff officers, two Information Operations and one for Psychological Operations.

The RNLA has chosen a policy in which officers and NCOs are multi-purpose, which creates another problem: there are some specialized units but the manning changes every 3 to 5 years. The desired balance between costs and effects leads to the situation that there are no specialized units neither



This illustration summarizes a part of the AJD-3-10 RD1.



AJP 3.13

supporting the Influence Operations domain nor supporting the Information Operations domain. For instance, PsyOps is not regarded as a specialism in the RNLA; it is an additional function for personnel of the Air Defence unit. In the Netherlands Influence Operations as a whole and Information Operations in particular remain an evolving trade. Several documents have been written regarding the way commanders should deal with InfoOps as a means of coordination rather than a specific capacity.

Within the RNLA the following definition is used: *"Coordinated activities aimed at influencing the opponents' decision cycle and supporting the politica/ military targets of an operation by striking the opponents' information systems, decision-making processes and supporting processes whilst defending our own."*

It remains to be seen that much attention is required for the defensive side of InfoOps. It seems the message is that InfoOps is to be seen as a coordination mechanism to create a complementary environment for the military and non-military areas of attention.

One thing is clear; there are a lot of perspectives on Influence operations and Information operations which makes it all a bit diffuse, to say the least.[27] The RNLA has chosen for a limited approach to InfoOps. The Netherlands Defence Doctrine 2005, which is largely derived form the British Defence Doctrine, correctly argues that attention to the necessity of harmonization and integration of activities is needed. Reports by former commanders of Task Force Uruzgan have emphasized the necessity of InfoOps.

Computer Network Operations (CNO)

In the RNLA CNO is one of the elements of InfoOps, which could get more attention. CNO plays a major part in the battle for the information domain and is one of the fundamental elements to influence behaviour and stems from the increasing use of networked computers and supporting ICT infrastructure systems by military and civilian organizations.

CNO is divided into Computer Network Attack (CNA), Computer Network Defence (CND), and related computer network exploitation (CNE) enabling operations. [28] CNA consists of actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CND involves actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and computer networks. [29] CND actions not only protect systems from an external adversary but also from exploitation from within, and are now a necessary function in all military operations. CNE is enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

The increasing reliance of "unsophisticated" adversary and terrorist groups on computers and computer networks to pass information to C2 forces reinforces the importance of CNO in InfoOps planning and activities. As the capability of computers and the range of their employment broaden, new vulnerabilities and opportunities will continue to develop. CNO should be an essential part of our operations.[30]

Adversaries also know how to play their part in the information battle. [31] The Taliban, for instance, obtain parts of their information via Twitter and Facebook.[32] All Facebook and also Hyves profiles are partially accessible for others. Some prominent intelligence chiefs in the Netherlands[33] and in the UK[34] noted that fact to their great dissatisfaction.

Investigating Networks and other means of ICT can lead to a massive amount of information which can be used to study feelings, emotions, similarities and differences within the indigenous population and governmental institutions.

Nationalism and political failures can be used and implemented as part of the information domain is exploited. Content generated by extremist organizations, their use of online tools, especially online forums, provide snapshots of their activities, communications, ideologies, relationships, and ongoing developments. [35] These snapshots provide invaluable data sources for researchers and experts,

with which they can better study extremist movements. However, several problems, such as information overload and the covert nature of the "Dark Web," prevent effective and efficient mining of "Dark Web" intelligence. Due to these problems, no systematic methodologies have been developed for "Dark Web" collection and analysis. A collection has been created of 110 U.S. domestic extremist forums containing more than 640,000 documents. The extremist forum collection, could serve as an invaluable data source to enable a better understanding of extremist movements.[36]

Adversaries manage their conflicts using the digital battle space and this knowledge should create more awareness than it does right now. [37] This part of the information domain is a major strategic element to be reckoned with. The information and communication era is absolutely boundless.[38] Coordination and synchronization of operations that influence behaviour is of great importance to create clarity and to produce order in the chaos of information flows.

Obvious and Applicable: Integration of Influence Operations in education, training and exercises

For that reason we need to coordinate and synchronise the influence of behaviour in the planning and implementation of operations at strategic, operational and tactical levels. The endless possibilities of the information and communication era obliges far more attention to the influence of emotions, perceptions, feelings, convictions, attitudes and behaviour. [39] With this in mind, influencing behaviour dominates the complete operational spectrum and is coordinated and synchronised at exercises and training in which the desired end state and the intent of the commander are normative. In the long run it is conceivable that an interagency approach for training, exercises and operations will be the standard; this will require commitment, eagerness and dedication of other relevant departments.

As we speak army units try their utmost to implement exercises in complex environments (including in matters of time and category). Force enablers like Provincial Reconstruction Teams (PRT), Civil Military Cooperation (CIMIC) and Psychological Support Elements (PSE) are deployed in a modular mode together with manoeuvre elements to present exercises with a higher level of reality. Such exercises have been executed for the past two years by the 13th Mechanized Brigade in order to train and prepare units for their mission.

To make this point more tangible we will give an example for an integral (interagency) exercise with an initial entry as a starting point. The point of departure for the scenario will be an initial entry in the port of Vlissingen in Zeeland which is a Netherlands province. From this town the operation will be executed via the southern parts of Brabant (province of The Netherlands) to Oirschot where 13th Mechanized Brigade is located.

In 2010 the 13th mechanized Brigade will provide a brigade staff for the European Battle Group (EUBG). The following main objective has been formulated: "The EUBG is to be trained to operate in several scenarios in which units have to respond flexible in a complex and dynamic environment in many areas." [40] In preparation of the exercise the brigade staffs are to execute an integral country study including a Computer Network Exploitation. In advance we have to consider how the local population should be informed regarding the operation (exercise). In a targeting meeting we can determine what kind of resources we have to influence the target audience.

It has been decided to send a Reconnaissance Squadron in advance to conduct deep reconnaissance supported by a Psychological Support Element and a PRT mission team in order to create a positive mindset within the local population for the forthcoming deployment of NLD Forces. To achieve a positive mindset some meetings *(Key Leader Engagement)* with the Mayor, police chiefs and district administration will be executed.[41] Several media outlets will be used, like news papers whilst regional radio and TV messages will explain the reason for executing exercises or operations like these. In addition the population will be asked to cooperate with this exercise (for example by participating in a roadblock).

This will be followed by manoeuvre elements, which will enter the area while engaging the opponent physically (which will be executed at a training area) simultaneously performing an open approach regarding the population to influence their hearts and minds in a positive manner. (For example, by organizing static shows in the vicinity of a school.) At the same time a lift operation will be prepared. A reconnaissance unit will be inserted to carry out close target recce, for example, in a house in front of a pub occasionally visited by a Medium Value Individual (role players). Besides that, others assets will be deployed, such as Human Intelligence and Unmanned Arial Vehicles. After the observation stage, followed by a positive identification Special Forces will conduct a lift operation to capture the MVI. In accordance to this an intensive media campaign will be launched.

It is interesting to note that the Belgian army performed a similar exercise to certify EUBG units in 2009. In 2010 the RNLA will train to be lead nation for the EUBG ready to be deployed in 2011 and is now planning an exercise in which all modular elements will execute an exercise in urbanized areas in combination with training areas. [42]

More options can be established to train units in which each soldier has to be aware of the results and consequences of their behaviour. In the preparation phase of an exercise we can plan and execute social patrols at markets and streets. We can identify Quick Impact Projects and carry out those projects (for example repairing a neglected playground). Former inhabitants of the potential area of operation, currently living in The Netherlands, could be able to participate as an adviser and as role players. Role play can be performed by military personnel (National Reserves) to perform the role of adversaries or military opponents. Civilian drama actors from an academy of dramatic art could perform certain civilian roles supported.

Public Relations and a consistent marketing strategy is an important element of such modular organised exercises using combined urbanised/exercise

terrain. The own population will see and experience how and why their army trains and exercises which creates commitment and understanding.

Moving Ahead

This paper covered the need for the exchange and broadening of insights and expertise on Influence Operations as a whole and Information Operations in particular. We described the way to operate in an expanding technological and communication era. We also questioned the viability of line staff organizations. Should we not be organized as we operate? Discussions of this may result in a modular process organization.

As we are all tools of Influence we have to set the conditions to train in urbanized terrain mixed with exercises at training areas. The basic principle is to train in a complex environment with modular organised units to prepare for our operational role in an interagency structure. [43] Over the past few years we have executed our operations with modular organized units. Currently we bring together several elements of manoeuvre units, CIMIC battalions, ISTAR battalions etc. into a module tailored for the operations. When we are "back home" we then fall back in the "known pattern" of line-staff organized units. We should consider organizing our armies into a permanent modular organization.

Instead of deriving units from a battalion or a company we then derive strike power from a module. Although, a modular organised army may seem to be one step too far.[44] This would mean that every brigade sized unit will exist of all units taking part in a module; working, practicing and training together and that will have consequences for the current line-staff army organisation and its employees.

According to us (the authors of this article), a modular organised army will be able to embed influence operations more fluently thus being better prepared for the growing battle for the information domain.[45] The centre of gravity in present and future operations aims at influencing the capabilities, will and understanding of all elements and actors and we have to adapt our mindset and organization towards that purpose. Influence Operations and Information Operations as a component of it, apply to a systematic and targeted approach to ensure that an opponent has the information we want him to have and which will lead him to make the decisions which act in our favour and to his disadvantage.

This illustration embodies the complex environment of our operations and shows the importance of well thought-out Lines of Influence to interconnect an interagency approach.

Furthermore we realize that the increasing population growth, combined with an ever-expanding urbanisation, will have a decreasing effect on manoeuvre space for traditional warfare. [46] The control of the information domain will be one of the important targets.[47] Influencing perception might be more important then facts in the future fight for energy, water, food and living space. In such a perception there is no space for stove piped visions like "kinetic elements" or "non-kinetic elements" as the interconnection and the mutual influence of these concepts are fundamental in a coexisting permissive, semi permissive and non permissive environment.

In current and future conflicts we will most likely find ourselves in a fight which is put up against a hardly determinable opponent who uses a tuned combination of political/economic activities, criminality, conventional activity and terror to accomplish desired objectives.

This is an environment in which alliances exist, by the day, between legitimate and illegitimate organisations – alliances which apparently are not linked but at the same time seem to find each other at corresponding areas to achieve common goals.[48]

One of the common goals is the control of the population, a control that is achieved differently by legitimate and illegitimate organisations. In such an environment Computer Network Operations plays a major part. The increasing reliance of "unsophisticated" opponent and terrorist groups on computers and computer networks to pass information to C2 forces reinforces the importance of CNO in planning and executing operations. As the capability of computers and the range of their employment broaden, new vulnerabilities and opportunities will continue to develop. One thing is sure; not only are our opponents managing their conflicts using the digital battle space; every actor in the conflict does. There should be a bigger role for CNO in our operations.

The broad spectrum of Influence Operations, and Information Operations as a component of it, directs our individual perception of a society is this boundless information and communication era. [49] Coordination and synchronization of operations is therefore of great importance to create clarity and to produce order in the chaos of information flows. We have to acknowledge that the critical success factor of operations lies in analyzing and steering opinions and convictions. The question here is how to obtain and sustain uniformity about Influence Operations, Information Operations and Strategic Communication within NATO's (Military) terminology and explanations, and to bring this into practise in operations and exercises. I would be strategically valuable for us to have a common understanding of these important subjects in this new era.

Perhaps the first step ahead could be exploring the possibility of organizing our armies into a permanent modular organisation instead of composing modules from battalions and companies.

> *"You [and "they"] are the embodiment of the information you [and "they"] choose to accept and act upon.*
>
> *To change your [and "their"] circumstances you need to change your [and "their"] thinking and subsequent actions."*[50]
>
> Adlin Sinclair

Major Rob Sentse, *B-SW, is a Royal Netherlands Army Infantry Officer. Serving at several branches, he worked, amongst others, as an intelligence analyst, as a trainer in leadership and educational skills and as a project officer implementing Field Humint in the RNLA. Currently he works as an Information Operations officer for 13th Mechanized Brigade.*

In 2006 he was deployed to the Canadian lead RC-S HQ in Kandahar as J2PLANS where he implemented the Fusion Cell. (http://www.jmss.org/2008/spring/articlesbody2.htm). www.linkedin.com

Major Arno Storm *is a Royal Netherlands Army Infantry Officer who is currently Branch Chief G5/Plans within the 13th (NLD) Mechanized Brigade in Oirschot. He was commissioned a second lieutenant within the Infantry upon graduation from the Royal Netherlands Military Academy in August 1998. He started his career at 17th Mechanized Infantry Battalion, in Oirschot, as a mechanized infantry platoon leader. www.linkedin.com*

Endnotes

1. Rob Sentse is staff officer Information Operations and Arno Storm is G5PLANS, both work for the 13th Mechanized Brigade, Royal Netherlands Army (RNLA), at the RvS Barracks, Oirschot , The Netherlands.
2. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA478337&Location=U2&doc=GetTRDoc.pdf
3. http://www.time.com/time/world/article/0,8599,1871487,00.html
4. http://www.sfcg.org/Documents/CPRF/CPRF-Summary-090414.pdf
5. http://www.nytimes.com/2009/06/23/world/americas/23military.html
6. http://www.prb.org/pdf04/04WorldDataSheet_Eng.pdf
7. http://www.africom.mil
8. http://www.un.org/apps/news/story.asp?NewsID=13451&Cr=population&Cr1
9. The "Strength through Peace program" as adopted by the Karzai government in 2005 gives the possibility to reconcile opponents and to include them in society making them important for progress thus splitting the few hardliners from the many followers (who follow by belief, hate or intimidation). If this is in the Popalzai interest seems to be questionable. Until now the "program" has not been implemented.
10. http://www.army.mil/aps/09/information_papers/cyber_operations.html
11. http://smallwarsjournal.com/blog/journal/docs-temp/216-guvendiren.pdf
12. http://www.captainsjournal.com/category/information-warfare/
13. "The Theory and practice of Insurgency and Counterinsurgency," Naval War College Review, April 1965.
14. Balancing the emotive ("hearts") component and the cognitive ("minds") component.
15. http://fas.org/irp/doddir/army/fm3-24-2.pdf
16. http://www.coldtype.net/Assets.04/Essays.04/Miller.pdf
17. http://www.guardian.co.uk/world/2009/mar/29/china-computing
18. In a Conventional Maneuver the Objective is defined in terms of terrain & enemy. In a Counterinsurgency Maneuver the Objective is defined in terms of population & perception.
19. http://www.jeffersoncomm.com/documents/strategiccommunications-bewarethejabberwockv2.pdf
20. http://www.mapchannels.com/twittermap/iranelection.htm
21. http://www.washingtonpost.com/wp-dyn/content/discussion/2009/06/17/DI2009061702232.html
22. http://www.cfc.forces.gc.ca/papers/csc/csc27/buck.pdf
23. http://www.clingendael.nl/cscp/events/20081216/
24. http://ics.leeds.ac.uk/papers/pmt/exhibits/2270/jwp3_80.pdf
25. http://www.fas.org/irp/eprint/index.html
26. http://www.rand.org/pubs/mongraphs/2009/RAND_MG654.sum.pdf
27. http://www.au.af.mil/info-ops/influence.htm#definitions
28. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf
29. http://www.securecomputing.net.au/News/114202,uk-ministry-of-defence-to-bolster-internet-intelligence.aspx
30. http://www.crisisgroup.org/home/index.cfm?id=5589
31. http://www.fas.org/irp/eprint/mobile.pdf
32. http://www.washingtonpost.com/wp-dyn/content/article/2009/04/08/AR2009040804378.html
33. http://www.expatica.com/nl/news/local_news/Dutch-news-in-brief_-Wednesday-8-April-2009_51439.html?ppager=1
34. http://laurelpapworth.com/facebook-mi6-wifes-photos/
35. http://www.sipri.org/blogs/Afghanistan/taliban-communication-skills-increase-mullah-omar-speaks-with-confidence-and-awareness
36. http://www2.computer.org/plugins/dl/pdf/proceedings/hicss/2007/2755/00/27550070c.pdf?template=1&loginState=1&userData=anonymous-IP%253A%253A127.0.0.1
37. http://www.govcom.org/about_us.html
38. http://www.potomacinstitute.org/media/mediaclips/2009/YAwatimes_a-kinder-gentler073009.pdf
39. http://www.d-n-i.net/fcs/lawrence_27_articles.htm
40. According to the authors of this article there is no space for stove piped visions like "kinetic elements" or "non-kinetic elements" as the interconnection and the mutual influence of these concepts are fundamental in a coexisting permissive, semi permissive and non permissive environment.
41. It is essential to build a robust network with representatives of organisations participating in the conflict, also to identify their possible role in reconstruction and development.
42. Example: A patrol walking at a market sees four men turning around whilst walking away from the approaching patrol. The patrol member then must have the awareness to create an observation report with relevant personal description, once executed they can contact the nearby police station (part of the scenario) to identify the individuals.
43. http://www.wiltonpark.org.uk/documents/conferences/WP919/pdfs/WP919.pdf
44. http://www.blueskybroadcast.com/Client/Army_Stratcom/docs/printable.slides.pdf
45. http://www.upiasia.com/Security/2009/07/17/chinese_and_us_lead_information_warfare/8629/
46. http://www.StrategicStudiesInstitute.army.mil/ State and Nonstate Associated Gangs: Credible "Midwives of New Social Orders," Dr. Max G. Manwaring.
47. http://www.forsvaret.dk/fak/documents/fak/publikationer/the_talibans_information_warfare.pdf
48. http://www.potomacinstitute.org/publications/Potomac_HybridWar_0108.pdf (December 2007).
49. http://influenceops.wordpress.com/2007/03/08/changing-perspectives-enhanced-%E2%80%98influence-operations%E2%80%99-in-conflict/
50. Text in brackets by authors.