INFORMATION OPERATIONS
Ideas for a strategic approach within a small country

Brigadier Dipl. Ing. Alois A. J. Forstner-Billau
Landsverteidigungsakademie - Wien

ABSTRACT

Just like other countries, Austria is confronted with the increasing dynamics of the development of Information and Communication Technology (ICT). Both the public sector, including defence, and the private sectors are depending on ICT. Discussing conflict scenario's, one has to discern international activities within the framework of a crisis response or peace support operation, and a military assault to a country. If Austria should be attacked it could theoretically be by an equally capable or by a far superior power. In this last case, it is like David and Goliath. This article introduces the idea to study 'associative communication' to arm David.

PREFACE

The general theme of the publication for the NL Royal Military Academy Symposium on 'Information Operations' is a real temptation for an author. He may try to find the best technically oriented approach to the general theme. In view of the enormous dynamics in scientific development of all related technologies, I will try to withstand this temptation. I will concentrate more on a, if I am permitted to use the expression, general (`s) approach. The following reflects my personal opinion and in no way should be regarded as an official Austrian political or military position. Nevertheless it is quite evident that more or less personal ideas of key personnel can and do influence the official view of organisations.

INTRODUCTION

Some of the key features of the Information Age are: the quantity of available information, the nearly unlimited access to this information and the resulting speed of activities of maintaining them.

All of these are and, over time, will increasingly be essential factors, that decide about the efficient combination of the traditional production factors: Labour, Money and Property, in a world of ICT-based processing. Computer aided decision-making has to guard and facilitate the different processes.

The information infrastructure, which is the vital backbone of our modern society, is unacceptably vulnerable to, intentional and pinpointed actions by terrorists, criminals and/or hostile organisations and governments. But not only by them. In the world of economy and business even competitors could try to use illegal means of intrusion into the data – and therefore knowledge bases - of another competitor. The vulnerability of today's ICT-systems in general is a serious problem and offers a tempting, rather inexpensive and very simple alternative for pinpointed intrusion or more likely assaults.

The ‘Superpowers’ in the world of today have recognised these threats and have therefore started to establish means and procedures to maintain ‘Information Superiority’ as a strategic objective to reach ‘Information Dominance’. Russian authors discussing this, have stated the following:

‘We are now seeing a tendency towards a shift in the centre of gravity away from traditional methods of force and means of combat, towards non-traditional methods, including information. Their impact is imperceptible and appears gradually. It is less burdensome economically and is not dangerous ecologically (....) Thus today information and information technologies are becoming a real weapon. A weapon not just in a metaphoric sense but in a direct sense as well.“[1]

In a report by the U.S. Centre for Strategic and International Studies, one finds the conclusion that the U.S. is aware that it is exposed to a host of new threats to society as a whole. This is because of the immense complex information infrastructure, being based on insecure foundations. The weapons of information warfare can outflank and circumvent military establishments and compromise the shared foundation of both the U.S. military and civilian infrastructure.[2]

As one can easily see, both views are more or less focused on the military part of Information Operations and are the source and background for mainly offensive concepts which might be indicated as ‘Strategic Information Warfare’.

The ‘Superpowers’ invest heavily in intellectual, scientific, and economic efforts and last but not least, invest vast amounts of money to be ahead in a global race for ‘Information Superiority’ with the objective to reach ‘Information Dominance’. For us, the authorities and citizens of the ‘Small Powers’, or shall I call them the ‘Powerless’ it is of high relevance as Campen makes us aware that:

“The information age world is one where geography, time, distance and space are irrelevant; where threats are diffused and obscure; **where Allies can also be non-traditional adversaries; and where Industrial Age laws and agreements among sovereign nation states have limited relevance“** [3]**.**

This means that in the ‘Information age’ one cannot fully rely on ‘friends & partners’ anymore. You either belong to a ‘club’ or your don’t. In the latter case everybody might threaten you, everywhere, and at anytime.

The national efforts in ‘Information Operations’ in general are based on three pillars: **‘Private Information Infrastructure’,** the **‘Federal Information Infrastructure’** and, within both information infrastructures as a subset, **’Defence related Information Infrastructure’**

THE PRIVATE INFORMATION INFRASTRUCTURE

In the early days of the implementation of Information Technology (IT), this technology was about the single user. Only highly qualified personnel and experts were able to run and

maintain these systems. IT was not of vital importance to the user respectively his organisation.

There was hardly any connection between one system and another. Data and information had to be printed out for use. For the manipulation and the possible abuse of data, one had to look for a direct, physical entry into the system. With physical barriers only, one could provide a high level of security. With the increasing upcoming of standardisation, the connection of networks and the recent dramatic growth of the worldwide interconnection via 'Internet', the 'solitude' in IT-privacy of the old days is over. It is now ICT, the combination of Information and communication that counts. 'Internet' is becoming increasingly essential for the economic survival of business organisations.

For a small country and its 'Private Information Infrastructure' this 'Globalisation' and ICT-supported 'Interworking' is, giving its opportunities, more of a challenge than a danger!

Within international partnerships of co-operating as well as competing business units, it is of mutual concern to fight the threats resulting from the application of modern information and communication technologies and their potential abuse by 'non- partners'. Small countries on the one hand, as well as small businesses on the other, cannot afford the full range of necessary investments of complex and expensive Research and Development (R&D) activities, to counter a wide variety of ICT-related threats and possible assaults.

Due to the vital interests of the 'Powerful', they will have to take care that the 'Powerless' (or 'Less powerful') have access to that kind of technology which maintains a required minimum standard and capability of protection against possible threats.

So what could the policy of the 'Less powerful' be? They have to bring required quality products and services to the market, in such a way that even the 'Superior' are interested and find so many benefits that they want the 'Less powerful ' as partners. Then, they will take all the measures to let the 'Less powerful' join the international 'Information Infrastructure'. That is what happens for example to and in the Middle and Eastern European (MEE)-countries at this particular time.

THE FEDERAL INFORMATION INFRASTRUCTURE

The particular political situation in Austria before we entered the European Community (EC), nowadays European Union (EU) was, and to some extent still is, that we do not have a real government. What we had and still have is a board of independent ministers who's political actions are limited only by a, what is called, coalition pact as a 'framework' of constitutional and legal rules. Therefore, from the very beginning of the ICT-age the implementation of an Information Infrastructure to support the public administration was of a rather unique design within each of the single ministries and other agencies.

By the time and, stemming from the demands for an increasing, mutual co-operation within the public administration, based on modern ICT-Infrastructure, a co-ordination board for ICT-matters was created under the lead of the Federal Chancellery. This co-ordination Board (KIT^4) tries to apply, on a more or less voluntary basis for the member organisations and agencies, common rules for ICT-hardware implementations, software applications and (i.e.

security -) procedures. Furthermore, this Board co-ordinates all the ICT-relevant matters with and to the EU-bodies as well.

Modern Internet-technologies nowadays provide the opportunity to overcome the former standardisation deficiencies between the different federal organisations and agencies and, step by step, the 'Federal Information Infrastructure' becomes more interoperable and homogeneous.

The fact that Austria is now a full member of the EU, requires that we stick to the common rules and directives for the ICT-based administration with and within the EU-bodies on the one hand, and for the relationship with the other member States on the other.

Besides this, the 'Federal Information Infrastructure' shares with its political and business partners the common 'year 2000-problem' (Y2K). The Y2K problem is a real nation- and worldwide testbed to address other issues, like handling large scale inter- agencies and inter-government processes and, last but not least, an opportunity for improved ICT-security. The first of January 2000 will prove if we have succeeded or failed. As far as these Y2K-issues are concerned, it is my strong belief that in general terms, the predicted catastrophic events will not occur. But we must be prepared to face rather minor but nevertheless unexpected problems, and there may be 'painful', and 'odd effects' of the Y2K-problem.

THE DEFENCE INFORMATION STRUCTURE

According to the existing Austrian 'National Defence Plan', based on the constitutional obligations for the national defence in general, homeland defence itself comprises the military and militia organisations as well as different federal agencies and civil emergency management organisations. The historical development after the Second World War of these different organisations, combined with their widely distributed responsibilities for management and operations, as well as their Information Infrastructure are unique and therefore different as well. As mentioned for the private and federal sector of information infrastructure, Internet technology facilitates the connection and interoperability of these different systems right now.

Combined endeavours and missions of this integrated Defence Organisation to handle peacetime tasks, like national disaster relief operations, are therefore not a real problem for the interoperability of the different information infrastructures.

Joint training, monitoring and control centres, and a common understanding, make sure that in case of national- or worldwide catastrophes, relief can be provided and maintained very efficiently.

TASK END MEANS

Missions require a partnership approach to Information Operations. Sometimes an 'environment' results in a high probability that Information Operations will occur. Sometimes one can be sure that this environment in general can be indicated as having a friendly and co-

operative nature. Extensive precautions to counter possible hostile attacks against the Information Infrastructure of relief units are therefore in most of the cases not necessary.

As far as crisis response (CR) and peace support operations (PSO) is concerned, given the pure military character and the actual political (neutral) situation in Austria, one has to differentiate between two scenarios:

1. International – trans-national crises and conflicts – PSO engagement within a UN-, OSCE - and/or Partnership for Peace (PfP) – framework.

   In such cases, Austrian military units take part as 'sub'-units of other military units and hardly in a „Lead Nation" role and responsibility. Therefore the information infrastructure, fielded with an Austrian military contingent, will serve primarily for contingent-internal and 'reach back' functions. For the interoperability with higher echelons of command in the crisis theatre, the 'Lead Nation' in charge has to take care. The more national information infrastructure is interoperable with the 'outside' world, the less the logistic burden for the 'Lead Nation'.

   So it is our national intention to follow, as far as possible, international standardisation processes. Already in peacetime we are highly interested to take part in ICT-related, comprehensive projects and programmes, following international military partners and participating in joint and combined ICT-training and -exercise events.

2. The least probable case – military assault directed against Austria.

   In such a case, Austria has to rely only on its own military capabilities and try its best to face the conflict. As far as the „Information Operations" within a, (at the moment in a conceptual stage), national command and control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) capability is concerned, one has to differentiate between an assault by an equally capable opponent or by a far superior hostile military power.

In the first case I assume that we would be able to run our own ICT-infrastructure and therefore 'Information Operations' in a rather secure and successful way.
In the second case, one has to analyse what has happened in earlier conflicts between rather small countries and, relatively lager power adversary countries or organisations.
In all these cases, the Armed Forces of the small countries were hardly able to operate their 'electronic' equipment in a systematic manner. To secure the 'Defence Information Infrastructure', the only thing they could do was to switch them off most of the time. However 'Dormant' systems are no systems'.

So, what to do to maintain a minimum C2-capability which is necessary to resist a military attack? What to do, yet to be able to command one's remaining (remotely deployed) military units?

To go for very expensive and risky programmes to develop, produce and implement highly sophisticated technical systems in order to secure a certain fraction of one's ICT-infrastructure, is, in my opinion, in most of the cases a 'dead end' approach. A small country can hardly outdo 'Superpowers' in highly sophisticated technical solutions. And, if I look at

the budgets we spend on R&D in general and on military research in particular, we might just as well even forget to try.

So what else to do? Let me remind you of the story where a prisoner shouts a certain number and all the other prisoners start laughing. On the question of a visitor, what was going on, a guard answered, that a particular joke has a certain number and just by calling that number, all other inmates remember the full joke and therefore start laughing.

ASSOCIATIVE THINKING

The lesson to be learned from this story is that the challenge of an 'Less powerful' military power is to use intelligent solutions, which do not require extensive economic and industrial resources and investments. But smart ideas, a high level of training and bright trainees. With a minimum of data transfer and therefore a minimum of information infrastructure, which minimises the effects of hostile countermeasures too, one can and one has to achieve a maximum of, what I would call '**associative'** information content.

Communication, based on **'associative'** thinking and not just on 'listening and/or viewing' – that is the challenge for the 'Less powerful'! If you can communicate, you can command! If one further pursues this idea, one should - for example - revive the efforts of scientific research on paranormal phenomena, like telepathy etc., to use the possible results for military purposes. '**High Tech**' can be mastered by '**High Intel**.

CONCLUSION

Goliath was not defeated by another Goliath, but by little smart David!.So the only way to survive in wartime as an IT-David, is to be smarter than the IT-Goliath is!

NOTES

1 Yevgeniy Korotchenko and Nikolay Plotnikov, 'Information is also a Weapon: About what should not be Forgotten When Working wit Personnel', *Krasnaya Axezda,* 17 february 1994, p. 2.

2 *SIGNAL*, June 1999, offical publication of AFCEA p. 65

3 Col. Alan D. Campen, USAF (Ret.)

4 **K**oordinationsgremium für **I**nformations **T**echnologie (KIT)