

**Submission Number 1-135**

**12<sup>th</sup> ICCRTS  
“Adapting C2 to the 21th Century”**

**Critical Decisions Approach to C2**

**Track 1: C2 Concepts, Theory and Policy  
Jan Foghelin**

**FOI, The Swedish Defence Research Agency  
(Gullfossgatan 6), 164 90 Stockholm, Sweden**

**+46 8 55 50 37 45  
[jan.foghelin@foi.se](mailto:jan.foghelin@foi.se)**

## **Critical Decisions Approach to C2**

### **Abstract**

The Network Centric Warfare (NCW) concept is essentially derived from civilian systems and a basic assumption that more information (shared) will result in better quality of decisions. A major driver of the concept has been a technology-push. After criticism concerning not taking the enemy, the human-factor etc. into account modifications have been made in the NCW-concept. The concept remains however fundamentally the same.

As a complement (not a substitution) it would be useful to look at the decision problem from another perspective. The steps could be the following:

- Select scenarios (generic) of important future conflicts.
- Derive key decisions from these scenarios.
- Describe the decisions (time constraints, need to know, countermeasures...)
- Analyse suitable decision supports which result in a robust decision.

This concept can be characterized by:

- Demand – pull (instead of technology – push)
- Need to know instead of all information.
- Takes into account the operational context.

### **Introduction**

The basic idea underlying this paper is that behind NCW and Effects Based Operations (EBO) are some basically sound principles. In its development stage of today it is already an improvement in certain types of operation, but not all. This paper tries to have a constructive – critical attitude to NCW. There are at least two problems with this:

- Criticism towards NCW can be dismissed referring to a misunderstanding of NCW or that NCW has moved forward to another version, (Reid, Goodman, Johnson and Giffin 2005)
- In spite of good intentions the criticism is considered to be more destructive than constructive. To clarify how we look upon NCW and its weaknesses there will be a section concerning basic assumptions of the NCW and a section of problems/weaknesses.

### **Basic assumptions of the NCW**

The basic assumptions are taken from DoD Command and Control Research Program (CCRP) publications and commentaries on these (Foghelin 2005; Mitchell 2006 ch 2)

- Modern Information and Computer Technology (ICT) gives unprecedented possibilities to collect manage and distribute data, information and knowledge. There are many examples on the civilian side that the proper use of ICT could give a competitive advantage. There are reasons to believe that modern ICT could give an advantage also in military operations (technology push). Many technologies could be used to improve sensors, data transmission, data fusion, information handling, information distribution... There should be possibilities to make better decisions faster.
- Today's and tomorrows military operations can be characterized by uncertainty and complexity. Using standardized tactics (derived from historical lessons-learned) will not be the best way to handle these operations. Rapid decision-making outgoing from adequate battlefield awareness is a clear advantage.
- Swift decisions (of high quality) are very important as already have been mentioned in the previous paragraph. Technology will be of good use but changes are also needed in organization and degree of decentralization. Sending information up and down in a hierarchical organization in the spirit of Max Weber will be too time-consuming. Decisions should be taken near to the edge. Flexibility is created by using temporarily joint units. A common battlefield awareness makes it possible to "self-synchronize".

### **Problems/Weaknesses with the NCW**

There are a number of weaknesses or at least problems/question marks inherent in the NCW-concept:

- The enemy and the terrain are very absent in the NCW standard descriptions. A general abstract description of an enemy with some military attributes is not enough to make a proper assessment of the usefulness of the NCW. Just take a couple of examples:
  - You are fighting against a (very) limited number of platforms in an "open terrain" (sea, air, and desert).
  - You are performing a counterinsurgency in an urban terrain against an enemy without uniforms or platforms.

For me the first example is much more promising for a constructive use of the NCW-concept.

There is a risk that you recommend a concept for every operation when it is really advantageous for a limited number.

- It seems to be prerequisite of NCW that you are able to get high quality battlefield awareness. This not always (or very seldom) the case. Reasons:

- Scarcity of technical resources like, e.g., sensors, transmission capacity, data handling capacity...etc.
  - In a complex terrain it can be very difficult to detect the enemy.
  - By hostile interference the battlefield awareness can be distorted.
- To be able to spread decisions to the edge and self-synchronize you must be able to share the battlefield awareness. There could be problems with this sharing:
- Lack of transmission capacity.
  - Hostile interference in the transmission phase.
  - There could be delays in the transmission to certain receivers.
  - Information overload. How to find the relevant information?
  - It is considered too risky to spread classified information (the enemy, it is too dangerous for your intelligence agents, etc.)
- Even if manage to transfer a battlefield awareness to all concerned there remain problems.
- Even if you share the geographical localization of every enemy unit you can have very different opinions about the enemy's intentions and what to do about them. Good decisions in the edge and self-synchronizations require more than a shared awareness.
  - Especially in peace support operations actions taken (even within some general Rules of Engagement (ROE) could be considered not appropriate afterwards. Who is responsible in a self-synchronized operation?
- In the NCW-concept differences in quality between decision-makers are seldom discussed. Normally it is taken for granted that all are equal and the decisions should be near to the action or by self-synchronization.

It's not reasonable to assume that all are equally good at decision-making.

If you have a perfect net (all have all the time all information) the best decision-maker available should make the decisions

Sometimes there could be necessary to make a choice between a good decision-maker with not so good information and a not so good decision-maker with good information.

Even in a net with decentralized decision-making it is probably necessary to have some rules for decision-making.

## **Scenarios (Foghelin 2006)**

A weakness, as we see it, with the NCW-concept is that it normally is discussed in very general terms concerning the operations. If examples are given they tend to be of the following type;

- Carefully selected historical examples to illustrate a point.
- A very simplified example of a decision-situation also to illustrate a point.

To be able to comment on something more realistic I will start by giving some scenarios which later on will under go some analysis.

### **Scenarios**

The scenarios are generic. There are two reasons for this. The first is the political sensitivity in naming specific actors. The second reason is the purpose of the scenarios: They should point to possible classes of conflicts rather than analyzing more specific ones.

The high impact/low probability end of the conflict spectrum is selected instead of the low impact/high probability end. The argument for this decision is the political tendency to be reactive. Low impact/high probability conflicts are supposedly being analyzed already. It is more important to draw attention to new high impact/low probability cases.

A common background for the scenarios:

The point of time for the scenarios is about 20 years in the future. The world order is roughly the same as today, i.e., the world is anarchical with the states being the most important players, even if non-state actors are increasingly important.

From now on to the point of time for the scenarios, there has not been any major war or major use of Weapons of Mass Destruction (WMD).

The world is more multi-polar than today.

New (military) technologies have been introduced (e.g., unmanned vehicles (air, land and sea), new Command, Control, Communications and Computers, Information, Surveillance, and Reconnaissance (C4IRS) systems...etc., but no real revolution.

Territories are increasingly important for most states: They contribute to the quality of life of the citizens and can provide domestic access to natural resources.

## **Scenario 1: Nuclear war between states**

### **Background**

In spite of great efforts with different means to stop the proliferation of technologies for WMD, the situation does not look good. You can be pessimistic (Allison 2004, 2006; Gray 2005: 255-290; Foghelin 1999) or somewhat more optimistic (Frost 2006) concerning the proliferation of nuclear weapons, but you cannot exclude the possibility. We have to be prepared for a world with several more actors (state or non-state) which possess nuclear weapons. You can always hope (and work for) all nuclear actors being very responsible and

careful. Sadly, however, the number of conflicts which can go nuclear will increase with the number of actors possessing nuclear weapons.

### **Scenario**

Two newly nuclearized states, each with a limited number of nuclear warheads, start a war in which nuclear warheads are used early by both parties. The reasons for early use of nuclear weapons are mainly lack of intelligence concerning intentions and the risk of pre-emption from the other side.

### **Problems and questions**

Which actions could have been taken by the states or by the world community to prevent the outbreak of the nuclear war?

How could the war be limited, i.e., ending before all nuclear warheads have been used?

## **Scenario 2: A conventional intrastate war**

### **Background**

Conventional wars between modern states (esp. democracies) are not customary. They are considered too costly, uncivilized, and not the best way of problem solving. While these arguments are valid, and have been throughout history, wars have broken out anyway.

The first Iraq war (1991) and the Kosovo operation have, for many, been examples of the superiority of high tech units. You must be careful, however, not to draw far-reaching conclusions from these special cases. The USA is the superpower which can afford both quality and quantity in its armed forces. There was also quite a gap between the war-fighting capabilities (equipment and strategy/tactics) between the USA and Iraq/Serbia.

Since the end of the cold war, most modern states have reduced the number of units in their armed forces considerably.

### **Scenario**

This scenario is about two (post)-modern states with modern armed forces in a conventional war against each other. The war starts with a surprise (pre-emptive) attack from one of the parties.

### **Problems and questions**

Will the decreasing number of units in the armed forces of modern states increase the temptation of pre-emptive attacks?

With few high-tech units on each side, what will the war look like? Which targets will assume the higher priority, military or civilian? Which will be the most valuable type of units? What will be the relative influence of quality vs. quantity of forces? What is the relative likelihood of long wars vs. short wars?

The basic question is whether our perceptions of an "Industrial war" are still valid for a modern state-state war. Many things have changed, both soft (societal organization...) and hard (technologies used...), since WW II.

### **Scenario 3. A stabilizing operation by a western coalition. The operation takes time, and counterinsurgency/counterterrorism is needed**

#### **Background**

Since WW II, several long-term counterinsurgency wars/operations have taken place where a western state or coalition of states has taken part. The successes are few. (Mack 1975; Smith 2005: 223-263). Examples:

- Vietnam (France)
- Vietnam (USA, main coalition partner), (Krepinevich 1986)
- Malaysia (UK), (Barber 1971; Corum 2006)
- Algeria (France)
- Afghanistan (Soviet Union), (Roy 1991)
- Northern Ireland (UK)
- Chechnya (Russia), (Kramer 2004/05)
- Iraq (USA, main coalition partner), (Gordon, Trainor 2006; Hendrickson, Tucker 2005)

Even though the examples are spread over wars/operations of great differences, (culture by the western state(s), goals for the parties, technologies used...), there seems to be a pattern.

The wars/operations have not been successful from the West's point of view. The exceptions are, perhaps, the British operations in Malaysia and Northern Ireland.

The adversaries have used asymmetries with success. They have successfully turned a short operation to a very long one, avoided decisive battles, and won the battle for hearts and minds...

The problems for the Western countries have often been:

- In democracies it is difficult to fight very long wars.
- It is difficult for the West, considered the superior party, to use all available means, as it tends or could tend to violate aspects of a "just war" from the perspective of international law.
- In a long, frustrating war, incidents occur which should not; these will be used by the media.
- It often has been difficult to create a clear connection between tactics and strategy.

Counterinsurgency (which also could be related to counterterrorism) is a type of operation which could be considered necessary in the future (in spite of its often not having been successful in the past).

Creveld (Creveld 2006) does mention two successful cases of counterinsurgency. One is the British in Northern Ireland, where major characteristics were patience and discipline. Patience (i.e. for multi-year- long engagements) is never easy in democracies. Discipline is normal for armed forces; the problem is keeping discipline at all times. A few incidents can spoil the reputation of the armed forces for a long time. Creveld's second example is from Syria (1982) where massive genocide was used to deter further acts of counterinsurgency. Even if efficient in a way, this method cannot be used by democracies (and, hopefully, by few others).

While it is possible to learn lessons from history, (Hammes 2005; Hoffman 2005; Metz 2005), it is often difficult to apply the lessons learned in a proper way.

The difficult question is: can you find a strategy/tactics (including technical systems) which can be used successfully in counterinsurgency/counter-terrorism while within the restrictions of democracies? (Gray 2005: 212-254, 259).

Historical experiences show that nation-building is a demanding and protracted task (Dobbins 2003/2004).

### **Scenario**

An intrastate conflict develops in a state of concern for many other states in the world. Mandated by the UN, a coalition of several willing states initiates a stabilizing operation. In spite of some initial successes the operation runs into difficulties in the form of insurgencies and terrorism.

### **Problems and questions**

Criteria for continuation of the operation.

Taking into account earlier experiences, what can be done to improve the situation (policy, technology, tactics, and type of personnel...)?

What could have been done before the operation to improve the probability of success?

Taking into account earlier difficulties of these types of operations, should the conclusion be to abstain and delimit the operation to a sort of containment?

## **Scenario 4. A pan-European intifada.**

### **Background**

The harmonious coexistence of immigrants in Europe, let alone full integration, has not been successful in all states and for all immigrants. Certain ethnic/religious groups have more difficulties than others. One of these groups is the Muslims.

Frustration can be expressed in many ways. Violence, e.g., in the form of suicidal bombing, is one extreme way. Inspired by what is going on in the rest of the world, violence with roots in religious fundamentalism has come to Europe.

The long-term solution to the problem is better integration; for the short-term this is not sufficient.

### **Scenario**

A coordinated, in time, action takes place all over Europe. Islamist fundamentalist groups bomb many places simultaneously.

### **Problems and questions**

How can you prevent this scenario from taking place at all?

Which counteractions should be taken and by whom (police, gendarmerie, military)?

Possible coordination of the crisis management through EU/Brussels?

## **Scenario 5. A nuclear threat is directed against the EU in general (or a specific EU-member).**

### **Background**

For the general background concerning proliferation of technologies/fissile material/know-how in the nuclear arena, see scenario 1 above.

### **Scenario**

A threat is announced by a terrorist group or a “rogue state.” A nuclear device will explode somewhere within the EU if certain conditions are not fulfilled. Nothing is said in the message about the type of nuclear device and how it is going to be delivered.

### **Problems and questions**

How to handle this crisis situation in general?

Information to the public through mass media?

Searching for bombs?

Air defence?

Border control?

Possible operations in the threatening rogue state?

Deterrence (by nuclear means)?

## **Scenario 6. A coordinated bio-attack by terrorists against major airports within the EU.**

### **Background**

A bio-attack against our societies has been considered a serious threat for a long time. For different reasons bio-agents have not been used in any major attack so far (Lederberg 1999: 211-232). A number of factors (technical development, escalation of terrorist attacks, psychological effects) make it necessary, however, to consider a bio-attack as a possible and dangerous threat (UI, CSIS, IMEMO, FOI, 2006).

### **Scenario**

Anthrax is spread by aerosols simultaneously at a number of airports. No pre-warning has been given.

### **Problems and questions**

How to identify the biological agents?

Restrictions on movement in and out of the airports concerned? How to be sure which are not concerned? Handling of mass-media? Crisis communication strategy?

Coordination from EU/Brussels?

Vaccines (production, distribution, priorities...)?

## **Scenario 7. A massive attack against major nodes (by bombing but also through cyberspace) of the banking systems.**

### **Background**

Cyberspace attacks were quite typical scenarios some years ago. The expected problem with Y2K gave further nourishment to the hype. If there have been any major attacks since then, they have not been announced. (Even if they have been attacked, business does not want to announce it because it could decrease confidence in their activities). The mere technical possibilities for an attack are not enough. There must be a desirable goal which can be reached. While terrorist groups normally seek attention, this is probably more easily accomplished by bombing, etc., instead of a cyber attack. For an organized crime group, on the other hand, a cyber attack could be a possibility. The goal is then to earn money.

### **Scenario**

A cyber-attack against the banking system is carried through by a combination of physical bombing and cyberspace. The chaos created will be used to transfer money to the organized crime group.

### **Problems and questions**

How much damage can you accomplish through a combination of a physical and a cyberspace attack?

Can you use the chaos for making money?

Crisis management in different dimensions?

## **Scenarios: C2 and critical decisions**

Two general observations:

- The scenarios are very different. It does not seem plausible that the requirement on command and control derived from the range of scenarios will be the same. (Maybe with the exception on a high philosophical level).
- In some scenarios there are a few decisive moments, in others there are many decisions on lower levels (type situations) which will lead to the final outcome. In the second case it is important to make a meta-decision (policy or doctrine) in order to have a high probability of success in the type situations. It is also important to select the correct type of organisation, and potentially the correct technology as well.

### **Scenario 1**

This is a case for very centralized decision-making. The key aspect is how the central command and control system could survive. The crucial decisions are to start and to stop the nuclear exchange.

### **Scenario 2**

This scenario is probably where the basic NCW-ideas will fit best. There will be a limited number of very important battles (e.g., MIDWAY in WW II).

Important questions for C2:

- What can be done to get a robust C2-system (against hostile disturbances etc.)?
- In a high tempo of operations how to make the right decisions (by whom, with what type of decision-support).

### **Scenario 3**

After an initial phase counterinsurgency operations tend to consist of a repetition of many similar situations. To be successful in this type of operations you must have a viable concept on the tactical level (with a C2 to match) and strategically have staying power. History shows that neither is easy. History also shows that it is difficult to change your tactical concept more radically. "More of the same" seems to be the preferred policy (see references under scenario 3-Background).

### **Scenario 4**

This is in a way a civilian counterpart of scenario 3. The requirements and problems are the same.

### **Scenario 5, 6 and 7**

You can distinguish three phases:

- Prevention:** A high-level cooperation between representatives from states and intelligence to find countermeasures.
- Crisis management:** To manage the acute crisis. Many actors and complicated information/massmedia problems.
- Reconstitution:** Less demanding requirements on C2.

## **Concluding remarks**

Let's imagine that the year is 2050 and we look on the last century of changes in warfare, especially in the area of command and control. A few guesses of findings:

- Information technology has had a major impact on warfare.
- The impact has not been restricted to improving the technical capabilities of certain functions. There has also been an impact on organization, responsibilities, etc.
- The development has been driven by a combination of visions and solutions to pressing near-term problems. Sometimes there has been an insurmountable gap between visions and practical problems. Sometimes there has been a constructive cooperation.
- There has all the time been a tension between centralization and decentralization. Modern ICT can support both alternatives. The choice

between the alternatives is a question of culture. If you want to change the culture you must realize that it is difficult and time-consuming (Citino 2005).

Security operations today and in the future could be very different. The best C2 will not be the same.

You must be able to work in several modes (examples of this can be seen in: (Gompert, Lachow and Perkins 2006; Atkinson, Moffat 2005)).

The basic question is how many /wide range) modes of operation in the C2-area, are you capable to manage (human resources, technical systems)?

We would recommend two “Zero Based Budgeting” (ZBB) type of studies. The first would deal with a modern (both parties are modern) intrastate war. The main challenges for the command and control will be:

- Robustness of systems (both technology and human factors)
- The borderlines between man – in – the loop and automation.
- The borderlines between political and military decisions.

The second ZBB study should deal with international operations (the broad area from counterterrorism to support to failing states). In general the West will probably be more selective in taking part. More thorough assessments of the probability of success will be needed. A closer military-civilian cooperation is a must. For command and control important points will be:

- Command and control systems which are interoperable and robust (much more than a question of technical standardisation)
- A for the operation adapted balance of leadership (political – civilian – military).

## References

Allison G: *Nuclear Terrorism. The Ultimate Preventable Catastrophe.* Times Books. New York 2004.

Allison G.: "A Nuclear Terrorism Report Card." *The National Interest* – Spring 2006. pp 63-75.

Atkinson S.R. and Moffat J.: *The Agile Organization. From Informal Networks to Complex Effects and agility.* CCRP. Washington, D.C. USA 2005.

Barber N.: *The War of the Running Dogs. How Malaya Defeated the Communist Guerrillas 1948-60.* CASSELL 2004 (1971).

Citino R.M.: *The German Way of War. From the Thirty Years' war to the Third Reich.* University Press of Kansas. USA 2005.

Corum J. S: *TRAINING INDIGENOUS FORCES IN COUNTERINSURGENCY: A TALE OF TWO INSURGENCIES.* STRATEGIC STUDIES INSTITUTE. March 2006.

Creveld M. van: Grausamkeit oder Zurückhaltung. Wie reguläre Armeen asymmetrische Kriege gewinnen können. s 86-94. *IP* April, 2006.

Dobbins J. F.: "America's Role in Nation-building: From Germany to Iraq." *SURVIVAL*, vol. 45. No 4. Winter 2003-2004. pp. 87-110.

Foghelin J.: Impacts of the New Societal Conflicts. pp 41-66 in Axberg S. and Foghelin J. (Eds): *Perspectives on Military Technology.* The Royal Swedish Academy of War Sciences 2006.

Foghelin J.: RMA, NCW, EBO, Transformation..."one damned thing after another. What is next?" *KKrVA HoT* 6 2005, pp 93-103. (*The Royal Swedish Academy of War Sciences. PROCEEDINGS AND JOURNAL*).

Foghelin J.: "Forms of Conflict, Actors, Means and Methods of Control." From a seminar arranged by The Royal Swedish Academy of War Sciences on October 21, 1999.

Frost R.M.: "Nuclear Terrorism after 9/11." *Adelphi Paper* 378. IISS. Routledge, 2005.

Gompert D.C., Lachow I, and Perkins J.: *Battle-Wise. Seeking Time-Information Superiority in Networked Warfare*. NDU Press. Washington, D.C. USA 2006.

Gordon M.R. and Trainor B.E.: *COBRA II The Inside Story of the Invasion and Occupation of Iraq*. Pantheon Books. New York, 2006.

Gray C.S.: *Another Bloody Century. Future Warfare*. Weidenfeld & Nicolson. London, 2005.

Hammes T.X.: *Rethinking the Principles of War: The Future of Warfare*. Pp 263-288 in McIvor.

Hendrickson D.C. and Tucker R.W.: "Revisions in Need of Revising: What Went Wrong in the Iraq War.?" *Survival*. Vol 47. No 2. Summer 2005, pp 7-32.

Hoffman F.G.: *Principles for the Savage Wars of Peace*. Pp 299-322 in McIvor.

Kramer M.: The Perils of Counterinsurgency. Russia's War in Chechnya. *International Security*, Vol 29, No 3 (Winter 2004/05), pp 5-63.

Krepinevich Jr, A.F.: *The Army and Vietnam*. The Johns Hopkins University Press, Baltimore and London 1986.

Lederberg J. (Ed): *Biological Weapons. Limiting the Threat*. The MIT Press Cambridge, Massachusetts 1999.

Mack A.: WHY BIG NATIONS LOSE SMALL WARS: THE POLITICS OR ASYMMETRIC CONFLICT. *World Politics*. 27 (1975):2. January pp 175-200.

Metz S.: *Small Wars: From Low Intensity Conflict to Irregular Challenges*. Pp 279-298 in McIvor.

Mitchell P.T.: NETWORK CENTRIC WARFARE. Coalition operations in the age of US military primacy. *Adelphi Paper* 385. IISS. London 2006.

Reid D.J., Goodman G., Johnson W., Giffin R.G.: All that Glisters: Is Network-Centric Warfare Really Scientific? *Defense & Security Analysis*, Vol. 21, No 4, pp 335-367, December 2005.

Roy O.: *The Lessons of the Soviet/Afghan War*. Adelphi Papers. 259. Summer 1991.

Smith R.: The Utility of Force: The Art of War in the Modern World. London. Allen Lane. 2005.

Tunberger J., Blomqvist J., Andersson B., Granholm N., Lohmander S.: Strategi för det oväntade 3 – Den nya osäkerheten. (Strategy for the Unexpected 3 – the New Insecurity) FOI-R—1981—SE. Användarrapport (User report, language: Swedish), May 2006.

### **About the author**

Jan Foghelin. M.SC. in Engineering Physics. Engineering Director at Swedish Defence Research Agency. Former head of Division of Defence Analysis. Fellow Royal Swedish Academy of War Sciences. Email: [Jan.foghelin@foi.se](mailto:Jan.foghelin@foi.se).