



Critical Decisions Approach to C2

12th ICCRTS

“Adapting C2 to the 21st Century”

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

Basic assumptions of the NCW

- ❖ Modern Information and Computer Technology (ICT) gives unprecedented possibilities to collect, manage and distribute data, information and knowledge.
- ❖ Today's and tomorrow's military operations can be characterized by uncertainty and complexity.
- ❖ Swift decisions (of high quality) are very important.

Problems/Weaknesses with the NCW

- ❖ The enemy and the terrain are very absent in the NCW standard descriptions.
- ❖ It seems to be a prerequisite of NCW that you are able to get high quality battlefield awareness. This not always (or very seldom) the case.
- ❖ 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
- ❖ Even if you manage to transfer a battlefield awareness to all concerned there remain problems.

Scenario 1: Nuclear war between states

→ *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

❖ *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*

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/ counter-terrorism is needed

❖ *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.

Scenario 3. - continued

❖ *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

❖ 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)

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

❖ *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

❖ *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 an 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.
- ❖ 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.

Scenarios

❖ Scenario 1 (*Nuclear war between states*)

This is a case for a very centralized decision-making

❖ Scenario 2 (*A conventional intrastate war*)

This scenario is probably where the basic NCW-ideas will fit best

Scenarios - continued

- ❖ **Scenario 3** (*A stabilizing operation by a western coalition. The operation takes time, and counterinsurgency/counter-terrorism is needed*)

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.

- ❖ **Scenario 4** (*A plan-European intifada*)

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

Scenarios - continued

- **Scenario 5** (A nuclear threat is directed against the EU in general (or a specific EU-member), **Scenario 6** (A coordinated bio-attack by terrorists against major airports within the EU), **Scenario 7** (A massive attack against major nodes (by bombing but also through cyberspace) of the banking systems)

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

- ❖ 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.

Concluding remarks - continued

- ❖ There has all the time been a tension between centralization and decentralization. Modern ICT can support both alternatives.
- ❖ Security operations today and in the future could be very different
- ❖ You must be able to work in several modes

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).

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).