SAS-085 Final Report on C2 Agility

ANNEX B CASE STUDY NOTES

SAS-085 conducted a series of case studies to see if C2 Agility related concepts could be observed in actual operations of various kinds and to test a series of C2 Agility-related hypotheses. This document contains the notes for each case generated by the case study team. These are not mean to be products, in of themselves, but rather serve as documentation for the analysis of the cases contained in the body of the final report.

Annex B – Case Studies

B.1 Rwanda Genocide Case Study

B.2 Estonia Cyber Attack in Spring 200 7 Case Study

B.1 Rwanda Genocide Case Study

Identify the Focus of and the Boundaries for the Case Study

a. What is the level of analysis? (e.g. Individual, Team, Organization, or Collective)

The analysis was conducted mostly at the organization level and a bit from the collective level. The analysis done is limited to the difference sources of information listed the bibliography.

b. Who or What Organizations are included in the case study? (e.g. the Collective responding to the Haiti Earthquake Crisis, Air-Ground Control Strike Teams in Iraq and Afghanistan)

This case study includes the following entities of the collective:

- UN Member states
- UNAMIR
- Media
- Operation Turquoise sent by France

c. What temporal boundaries are included?

a. When does the case begin and end?

The case study begins on the 5th of October 1993 with the establishment, by the Security Council, of the UN Assistance Mission for Rwanda (UNAMIR) , with Brigadier General Dallaire as the Force Commander of the military component. It ends on the 19 July 1994, by the RPF victory which ended genocide by the Hutu extremists.

b. Are there phases involved? If so, what are their boundaries?

The UNAMIR can be broken into four major phases:

- UN Security Assistance Mission,
- Violence Escalation,
- Rwanda Monitoring Mission, and
- Security and Protection of Refugees and Civilians.

Phase 1: UN Security Assistance Mission – 5 October, 1993 – 6 April 1994

The 5th October 1993, the Security Council established the UN Assistance Mission for Rwanda (UNAMIR) with Brigadier General Dallaire as the Force Commander of the military component. This mission intended to help implement the Arusha Peace Agreement signed by the Rwandese parties on **4 August 1993.**

UNAMIR's mandate (Security Council Resoluton 872) was: *to assist in ensuring the security of the capital city of Kigali; monitor the ceasefire agreement, including establishment of an expanded demilitarized zone and demobilization procedures; monitor the security situation during the final period of the transitional Government's mandate leading up to elections; assist with mine-clearance; and assist in the coordination of humanitarian assistance activities in conjunction with relief operations*. (http://www.un.org/en/peacekeeping/missions/past/unamirM.htm)

The United Nations sent a lightly armed peace-keeping force to Rwanda to assist in implementing peace accords between the Rwandan government (controlled by Hutus, the country's largest ethnic group) and the RPF. Commanded by Canadian General Roméo Dallaire, UNAMIR comprised 2500 troops who were forbidden to use force except in self-defence. Brigadier General Dallaire arrived in Kigali on 22 October, 1993 with an advance party of 21 personnel.

The Secretary General's Special Representative (SRSG), who was to have overall responsibility for UNAMIR, arrived on 23 November, 1993.

Phase 2: Violence Escalation – 6 April 1994 – 21 April 1994

On April 6, 1994, the president of Rwanda was killed when his plane was shot down. This event set off a **100-day "tidal wave of violence".**

On the first night of the war, Rwandan government forces were murdering Tutsi and Hutu moderate politicians. Dallaire dispatched one unit of 10 Belgian peacekeepers to secure the home of Rwanda's prime minister. The Belgians were by far the most experienced of his soldiers. But they were ambushed, taken prisoner and later tortured, mutilated and murdered

April 9-10, 1994, France and Belgium sent troops to rescue their citizens. American civilians are also airlifted out.

April 14 1994, one week after the murder of the ten Belgian soldiers, Belgium, a key contributor to UNAMIR, withdraws its forces from UNAMIR.

Phase 3: Rwanda Monitoring Mission – 21 April 1994 – 17 May 1994

April 21, 1994, **the UN Security Council vote unanimously to withdraw most of the UNAMIR troops, cutting UNAMIR back to 270 troops.** The mandate of UNAMIR was adjusted by Security Council **resolution 912 (1994)** of **21 April 1994**, so that it could *act as an intermediary between the warring Rwandese parties in an attempt to secure their agreement to a ceasefire; assist in the resumption of humanitarian relief operations to the extent feasible; and monitor developments in Rwanda, including the safety and security of civilians who sought refuge with UNAMIR*. (http://www.un.org/en/peacekeeping/missions/past/unamirM.htm)

So, while the slaughter goes on, UN peacekeeping forces stand by since they are forbidden to intervene, as this would breach their "monitoring' mandate".

Phase 4: Security and Protection of Refugees and Civilians – 17 May 1994 – 18 July 1994

After the situation in Rwanda deteriorated further, UNAMIR's mandate was expanded by Security Council **resolution 918 (1994)** of **17 May 1994***, to enable it to contribute to the security and protection of refugees and civilians at risk, through means including the establishment and maintenance of secure humanitarian areas, and the provision of security for relief operations to the degree possible*. (http://www.un.org/en/peacekeeping/missions/past/unamirM.htm)

May 17, 1994, the UN finally **agrees to send 55000 troops** (UNAMIR II) to Rwanda.

Disputes over **costs delayed** the troops' deployment. UNAMIR II was authorized in May, 1994 but only a tenth of the authorized troop strength was made available by UN member states as late as July 1994.

On June 22, 1994, the U.N. Security Council authorized France to deploy 2500 troops (Operation Turquoise) to Rwanda as an **interim peacekeeping force**, with a **two-month U.N. mandate**

The war ended on July 18, 1994, "The RPF took control of a country ravaged by war and genocide. On 19 July, the RPF succeeded in occupying the whole of Rwanda except for the zone controlled by the French. The RPF victory ended genocide by the Hutu extremists

d. Other boundaries (e.g. separate analyses of the collective and of specific organizations within the collective).

Due to differences in locations and/or cultures, UNAMIR can be decomposed into different entities:

- UN Security Council
- Triumvirate of UN DPKO (Department of Peacekeeping Operations) in New York city : General Maurice Baril (Head of military component of UN DPKO), Kofi Annan (under-secretary-general), Iqbal Riza (chief of staff of DPKO)
- UNAMIR HQ in Rwanda, including:
  - (General Roméo Dallaire (Commander of UN forces in Rwanda) and
  - Booh Booh (Secretary General's Special Representative (SRSG))
- Contingents from Belgium
- Contingent from Ghana
- Contingent from Bangladesh

These entities will then be considered as entities of the collective.

Describe the Challenge or Opportunity that gave rise to the need for C2 Agility.

The need for C2 Agility arose from different factors:

- The complexity of the political situation in Rwanda was such that no one was really understanding the situation in Rwanda –
  - The humanitarian situation of Rwanda in 1993 was a vital clue to the impending political explosion in the country.
  - Rwanda Government side was divided and riven with internal conflict.

    - Extremist militias were not controlled
    - The intents of the different Rwanda opponents were not clear. Even now, we do not know who shot down the plane of the prime minister
- The urgency of the situation –
    - At time of the crisis, people were dying every day.
- The lack of resources available to UNAMIR –
    - At the time of the formation of UNAMIR, there were about 80000 peacekeeping soldiers deployed across the world. Many countries did not offer troops for UNAMIR because they were already stretched too thin and it was stated that most countries lack the capacity to be involved in more than two peacekeeping operations at any given time.
    - Many of the troops that were contributed are considered to have lacked training
    - These troops lacked equipment and such equipment that was supplied was often deficient

What would have been the consequences of a failure to act in a way that demonstrates C2 Agility?

Demonstration of C2 agility allowed saving people life (around 30000 Rwandans from both sides that were under UNAMIR's protection).

Overall, UNAMIR is considered as a failure of UN. This is based on the fact that it ended up by Massive Rwanda Genocide executed by Hutu extremists against Tutsi in 1994: on a population estimated to 7.9 million before the war: up to 800000 people had been murdered, another 2 million or so had fled, another million or so were displaced internally, 47000 children had been orphaned and over 250000 women had been raped.

Was C2 Agility Manifested? If so, how? (Be as clear and precise as possible, but keep this simple so that it does not require repetition in the next steps.)

C2 agility was manifested in different ways:

- UNAMIR was able to use, in parallel, different C2 approaches with different organisations
    - Different levels of C2 were required depending on the maturity level of the contingent , as well as the level of trust between the leaders (see VII)
        - Conflicted C2 with Banglaseshi Contingent
        - Deconflicted C2 with France
        - Coordinated C2 with Ghana Contingent
        - Collaborative C2 with Belgium Contingent
- After the departure of the Belgium Contingent, UNAMIR changes his interaction pattern with the media community, going from very limited, sharply focused using traditional public affair staff (Conflicted C2) to significant broad in order to coordinate efforts (Coordinated C2)
- A collaborative C2 approach has been observed between UNAMIR HQ and Department of Peacekeeping Operations (DPKO), while options and recommendations were developed mainly by UNAMIR HQ in consultation with DPKO. After the announce of the death of the President of the Rwanda, UNAMIR HQ decided to protect the current as well as the future prime ministers of Rwanda. This was outside the mandate of the mission. Due to time constraints, this decision has been made without consultation with DPKO. This is an evidence of going from Collaborative C2 (initial approach) to Edge C2.

Which Enablers and Inhibitors of C2 Agility were observable? (Remember that the basic six may not be independent. Include discussions of the relevant Agile Behaviors, but try to tie them to one or more Enablers. Specify inhibitors that impacted C2 Agility)

a. **Versatility –**
    a. None.
b. **Responsiveness –**
    a. **Conflicts between mission's intent and mission mandate (see VIII.d)**
        i. Decisions outside the mandate of the mission were made to try to save current prime minister and future prime ministers.
    b. **Proposition of new option as response to a hierarchical decision – (see VIII.a)**
        i. General Dallaire received the order to withdraw all forces. Ability to deal with extremely uncertain and fluid circumstances allowed General Dallaire team to send to UN an acceptable proposal in response to the order of withdrawing all forces. Gen Dallaire made the proposal to UN to keep a reduced complement of approximately 450 troops and withdraw the rest. The new proposal was done timely, so Security Council could review its decisions . The UN headquarters accepted General Dallaire's proposal. This resulted in the saving of 30000 Rwandans from both sides that were under UNAMIR's protection.
c. **Resilience**
    a. None

d. **Innovation –**
    a. **The use of the media to strike the conscience of the world and to try to prod the international community into action - (see VIII.b)**
        i. Instead of only using public affair staff, General Dallaire decided to talk himself to all reporters requiring information about what was going on in Rwanda.

e. **Flexibility –**
    a. **The use of the media to strike the conscience of the world and to try to prod the international community into action - (see VIII.b)**
        i. General Dallaire offers to a BBC reporter who was with the departing Belgian contingent, protection, food and sustainment as well as the mean to get a story to the world every day if the reporter accepted to stay with them
        ii. Anything in the realm of possible was done to permit a maximum of different media outfits and journalists in theatre in order to report what was going on in Rwanda
    b. **Tactical distributed decision-making to support the evacuation of foreign nationals - (see VIII.c)**
        i. To support the evacuation effort of the foreigners, new ROE were signed by Gen Dallaire.
        ii. The new rules also permitted local commanders to decide on the level of force they needed to use.

f. **Adaptation –**
    a. **Proposition of new option as response to a hierarchical decision - (see VIII.a)**
        i. General Dallaire received the order to withdraw all forces. Ability to deal with extremely uncertain and fluid circumstances allowed Gen Dallaire team to send to

UN an acceptable proposal in response to the order of withdrawing all forces. Gen Dallaire made the proposal to UN to keep a reduced complement of approximately 450 troops and withdraw the rest. The UN headquarters accepted Gen Dallaire's proposal. This resulted in the saving of 30000 Rwandans from both sides that were under UNAMIR's protection.

What C2 Approaches were being used? (How can C2 Approach Agility be inferred from what was reported or observed?) Did C2 Approach change, either for a collective, organization, team or one or more individuals?

Conflicted C2:

- **DPKO with Member States**
  - France decided to send a military intervention force into the Area of Operations (AOR) of UNAMIR, even before receiving formal permission of the Security Council. This was done without consulting UNAMIR.
- **UNAMIR HQ and Member States**
  - The Belgian contingent, allegedly UNAMIR's most effective military force, was withdrawn unilaterally by Belgium
  - Member states with intelligence information of value to UNAMIR did not always share important data
- **UNAMIR HQ and Bangladeshi Contingent**
  - At the most critical point in UNAMIR's history, when the genocide started, BGen Dallaire appeared to have no control over the Bangladesh contingent.
    - Bangladeshi commanding office demanded that every order be delivered to him on paper and was resisting the use of his troops for operations
    - Bangladesh Contingent possessed the capability to provide UNAMIR with a supply of water - water that was urgently needed. However, this contingent was officially forbidden, by his country, to assist, no matter how many people were dying, because of the grave concern about suffering casualties. As a result, hundreds of the displaced persons under UNAMIR protection were dying of thirst every day.
    - After the Presidential Guard and militia had been killed, along with their families, UNAMIR were trying to rescue Rwandans and expatriates who were in danger, bringing them to UNAMIR compounds. However, at that time, Bangladeshi did not respond to request for helps. He did not opened the doors of the Amahoro Stadium complex even if he was asked for it. Bangladeshi commander had received direct orders from his chief of staff in Dhaka to stop taking risks, stay buttoned down, close the gates and stop carrying Rwandans in the APCs. He did exactly what he was ordered, ignoring UNAMIR chain of command.

Deconflicted C2

- **UNAMIR and foreign powers**
  - Several foreign powers sent military intervention forces to extract their own nationals from Rwanda (the UNAMIR AOR).
- **UNAMIR and Operation Turquoise (France)**
  - Minimal sharing of information was made between UNAMIR and this intervention force (Turquoise). There were only doing liaison with BGen Dallaire

Coordinated C2

- **UNAMIR HQ and Ghana Contingent**
  - Ghana contingent was coordinating all effort with UNAMIR HQ

- **UNAMIR with the media**
    - At the beginning, there were a conflicted C2 approach between UNAMIR and the media. While the departure of Belgium contingent, the C2 approach has been changed to a coordinated C2 approach. Gen Dallaire thought that media can spark the conscience of the world about the fact that the massive murder activity continued (see VIII.b).

Collaborative C2

- **UNAMIR HQ and UN DPKO**
    - UNAMIR and UN DPKO used a coordinated C2 approach. Options and recommendations were developed mainly by UNAMIR HQ in consultation with DPKO
- **UNAMIR and Belgium Contingent**
    - Gen Dallaire and Col Luc Marchal (from Belgium contingent) worked together to determine and execute the best course of actions according to the evolution of the situation

Edge C2

- **UNAMIR HQ and UN DPKO**
    - UNAMIR and UN DPKO used a coordinated C2 approach. At some point, due to time constraints and the urgency of the situation, UNAMIR made the decisions to protect the current prime minister and the future prime minister, which were outside its mandate . On their side UN DPKO was trying to involve the different member states to provide support to UNAMIR. At some extend, this can be considered as an edge C2.

What interesting and important vignettes are included or can be derived from the case study to help create illustrative stories?

a. Proposition of new option as response to a hierarchical decision

- 18th of April late night, UNAMIR received DPKO (Department of Peacekeeping Operations) Triumvirat code cable 1173 with the following directives: If the opponents wouldn't agree to a ceasefire by nine in the next morning New York time, UNAMIR was to start its withdrawal. They were asking UNAMIR to assess the consequences of the withdrawal on those who had "taken refuge" at UNAMIR sites. P.396
- 19th of April. Gen Dallaire sent a military assessment of the situation describing the terrible situation along with all the tactical and moral reasons for keeping at least a small force inside the country.
- 20 April, early hours . NewYork sent a code cable ordering to stop withdrawal until further orders. 3 proposals would be presented to the security council: p.450, which included:
    - Reinforce UNAMIR and expand its mandate to attempt to coerce the opposing force into a ceasefire, and to attempt to restore law and order and put an end to the killings
- 21 April, UN Security Council vote unanimously to withdraw most of the UNAMIR troops, cutting UNAMIR back to 270 troops. The Council had finally voted for the skeleton force option.
- 22 April, UNAMIR received the Security Council Resolution 912.
- This decision allowed to save 30000 Rwandans from both sides that were under UNAMIR's protection

b. The use of the media to strike the conscience of the world and to try to prod the international community into action.

The response of NewYork to Dallaire's reports on the status of the situation was the modification of the mandate 872 into a monitoring mandate (resolution 912). Considering that the monitoring mandate will not allow to stop the slaughters, General Dallaire decided to step up the media campaign. His intent was to spark the conscience of the world about the fact that the massive murder activity continued. Accordingly, he offers to a BBC reporter who was with the departing Belgian contingent, protection, food and sustainment as well as the mean to get a story to the world every day if the reporter accepted to stay with them. This initiated incoming of reporters coming from other news agencies. Anything in the realm of possible was done to permit a maximum of different media outfits and journalists in theatre in order to report what was going on in Rwanda. Furthermore, each night, any journalists calling for interviews were giving access to General Dallaire. The result was that the media made the public (world) aware about what was happening in Rwanda. It led to a growing international outcry. In May 17, 1994, amid a growing international outcry, the UN finally agreed to send 55000 troops (UNAMIR II) to Rwanda. But disputes over costs delayed the troops' deployment. Accordingly, better public awareness influenced international political will which led UN to maintain UNAMIR.

c. Tactical distributed decision-making to support the evacuation of foreign nationals

The mandate of the UNAMIR mission was defined by the Security Council. ROE had also to be approved by the Security Council.

After the prime minister was killed and the massacres happen, several foreign powers sent military intervention forces to extract their own nationals from Rwanda (the UNAMIR AOR). To participate in the evacuation, Gen Dallaire approved new ROE . These were in force for the duration of the evacuation. The mission was under ROE not to use force except in self defence, while the new one authorizes his troops to disarm the belligerents and to intervene with force after warning shots. The new rules also permitted local commanders to decide on the level of force they needed to use.

Meanwhile, Gen Dallaire priority was to have a truce agreement with RPF and and RGF, allowing safe evacuation of the foreign nationals.

Result: the evacuation of the foreign nationals was a success on April 12.

- 650 expatriates from 22 nations on 10 French flights
- Two hundred and eleven UN personnel left on three Canadian Forces Hercules flights.
- A company of French Marines arrived and more paratroops were standing by in Bangui. Eight flights brought in half of the Belgian para brigade, along with motorbikes and three armoured vehicules.

d. Conflicts between mission's intent and mission mandate

UNAMIR HQ was using a collaborative C2 approach with UN DPKO (proposals were mostly proposed by UNAMIR HQ in consultation with DPKO, but they were approved by Security Council)

The C2 approach has been changed for a limited period time, just after the shot down of president plane. At that time, we can see an edge C2 approach. Effectively, due to time constraints and the urgency of the situation, UNAMIR made some decisions that were outside its mandate. These decisions were:

- To protect the prime minister by sending in the Belgian contingent that led to the death of Belgian soldiers.
- To extract the future prime minister Faustin Twagiramungu from his encircled home, bring him to his headquarter and protect him (He had been designated by an August 1993 peace accord to fill this position).

It demonstrates that effective command under such complex and time constraints conditions requires a leader to maintain the intent of the mission and keep a view of the full breadth of the peace agreement, all while dealing with extremely uncertain and fluid circumstances.

Figure B.1.1 Case Study Evidence Table – UNAMIR HQ - UN DPKO

Component/Concept	Phase 1	Phase 2	Phase 3	Phase 4
C2 Approach Space				
Situation Complexity (high, med, low?)	medium	high	high	high
Appropriate (Required) approach				
Allocation of Decision Rights (none to broad)	limited	Limited / broad	limited	limited
Distribution of Information (none to broad)	broad	broad	broad	broad
Patterns of Interaction (tightly constrained to unconstrained)	As required	As required – significant broad	As required	As required
Actual approach	Collaborative	Collaborative / Edge	Collaborative	Collaborative
Agility Components (low, med, high?) (State evidence for Agility as well as lack of agility)				
Flexibility (inflexibility)		Evidence Found		
Adaptiveness (lack of adaptiveness)		Evidence Found		
Responsiveness (unresponsive)		Evidence Found		
Versatility (Robustness) (lack of versatility)				
Innovativeness (lack of innovativeness)				
Resilience (lack of resilience)				
Self-Monitoring (we're not sure if self-monitoring is part of the original model or not).	Was done continuously	Recognized the need to change C2 approach	Was done continuously	Was done continuously

Figure B.1.2: Case Study Evidence Table – UNAMIR HQ - Media

Component/Concept	Phase 1	Phase 2	Phase 3	Phase 4
C2 Approach Space				
Situation Complexity (high, med, low?)	medium	high	high	high
Appropriate (Required) approach				
Allocation of Decision Rights (none to broad)	none	Emergent	Emergent	Emergent
Distribution of Information (none to broad)	Limited	All Relevant Information	All Relevant Information	All Relevant Information
Patterns of Interaction (tightly constrained to unconstrained)	Limited, Sharply Focused	As Required	As Required	As Required
Actual approach	Conflicted	Conflicted / Coordinated	Coordinated	Coordinated
Agility Components (low, med, high?) *(State evidence for Agility as well as lack of agility)*				
Flexibility (inflexibility)		Evidence Found	Evidence Found	Evidence Found
Adaptiveness (lack of adaptiveness)				
Responsiveness (unresponsive)				
Versatility (Robustness) (lack of versatility)				
Innovativeness (lack of innovativeness)		Evidence Found	Evidence Found	Evidence Found
Resilience (lack of resilience)				
Self-Monitoring (we're not sure if self-monitoring is part of the original model or not).	Continuous	Continuous/Recognized the need to change approaches	Continuous	Continuous

Figure B.1.3: Key Findings

Key Finding	Example
Role of Leadership in achieving and maintaining C2 Agility or C2 Approach Agility	1
Evidence for C2 Agility (i.e. Different Approaches over Time)	See V.
Recognition that Collective comprises of different entities, that often have different C2 approaches	Depending on the maturity level of the contingent , as well as the level of trust between the leaders, UNAMIR was using conflicted, deconflicted, coordinated or collaborative C2
Collective size changes over time. Case study leads to confirm.	Yes, UNAMIR went from about 2500 troops to 270 troops to 55000 troops
'Comfortable' C2 Approach creates a tension for transitioning to the appropriate (required) C2 approach	
Risk Assessment, part of self-monitoring	The assessment of the situation made by General Dallaire was that there would be a possibility of genocide in Rwanda. It was obvious to him that the withdrawal of UNAMIR would only facilitate the execution of the genocide. This state of awareness was required to propose new options to DPKO when he received the order to redraw. The possibility of the genocide justified the need to work with the media to inform the world of the necessity to maintain UN forces in Rwanda
Role of Competence	Ability to deal with extremely uncertain and fluid circumstances and crisis environment were required
Requisite Variety in Skills and Resources, necessary to cope with the complexity and dynamics of the situation	
Trust and interpersonal relationships, key enablers	We have observed evidence of Collaborative C2 when trust existed between leaders. (ex. Between Gen Dallaire and Col Marchal)
Role of Compromise, key enabler for or manifestation of flexibility, Advantage Agility Components?	• Physical capability and means are essential to agility • Agile C2 will require full engagement of the different actors at all levels • Cooperation (and collaboration) requires trust and good relationship amongst actors • Cooperation required clear roles amongst actors • Middlemen may have a negative impact on the quality of the information provided • Clarity of communication process amongst actors is required for agile C2 • Agile C2 requires real-time situation awareness at all levels
More Research Required to Understand Conflicted C2	
Politically Driven C2 Approach. That is other external influences that may determine where an entity ends up in the C2 approach space	The fundamental failure was the lack of resources and political commitment devoted to developments in Rwanda and to the United Nations presence there. There was a persistent lack of political will by Member States to act, or to act with enough assertiveness. This lack of political will affected the response by the Secretariat and decision-making by the Security Council, but was also evident in the recurrent difficulties to get the necessary troops for the United Nations Assistance Mission for Rwanda (UNAMIR) (from Independent Inquiry requested by the Secretary-General)
Off diagonal approaches (C2 Cube, as opposed to the previously defined approaches of conflicted, deconflicted, etc…) are the rule, rather than the	

exception	

B.2 Estonia Cyber Attack in Spring 200 7 Case Study

Author(s): Prof. Michael Henshaw, Mr. Abideen Tetlay, and Prof. Carys Siemieniuch
Institution: Loughborough University (UK)
Contact Address: Engineering Systems of Systems Group (ESoS)
School of Electronic, Electrical and Systems Engineering
Garendon Wing, Holywell Park
Loughborough University
Loughborough, Leicestershire
LE11 3TU, UK

Glossary

Agile C2 Approach	To provide the enterprise with additional C2 approach options that involve entities working more closely together and with the ability to identify and implement the most appropriate approach to coalition C2 given the situation (e.g. mission, conditions, and set of coalition partners – contributing entities). (Moffatt & Alberts, Dec. 2006)
Botnets	A collection of compromised computers connected to the Internet. Termed bots, they are used for malicious purposes. When a computer becomes compromised, it becomes a part of a botnet. Botnets are usually controlled through standards based network protocols such as IRC and http. (Wikipedia, 2013)
C2	Command and Control
CERT-EE	Computer Emergency Response Team for Estonia
Cyber	A prefix that means computer or computer network, as in cyberspace, the electronic medium in which online communication takes place. (Thefreedictionary, 2013)
De-conflicted C2 Approach	The avoidance of adverse cross-impacts between and among the participants by partitioning the problem space and the solution(Moffatt & Alberts, Dec. 2006).
DDoS	In a Distributed Denial-of-Service (DDoS), large numbers of compromised systems (sometimes called a botnet) attack a single target.
DNS	Domain Name Server (DNS) - translates Internet domain and host names (human recognised name) to IP addresses (numerical, computer-recognised name).
DoS	Denial of Service (DoS) usually affects internet services for public use (e.g. Government or service provider sites) by effectively disabling the site for a period of time.
Firewalling	A firewall is a protective device to prevent unauthorised access to an individual computer or a network. Generally, the device is software-based and applies a set of rules that determine whether a network transmission is a legitimate communication.
HTTP	(HyperText Transfer Protocol) The communications protocol used to connect to Web servers on the Internet or on a local network (intranet). Its primary function is to establish a connection with the server and send HTML pages back to the user's browser. It is also used to download files from the server

	either to the browser or to any other requesting application that uses HTTP. (PCMag.com, 2013)
IRC	Internet Relay Chat (IRC) is a protocol for live interactive Internet text messaging (chat) or synchronous conferencing(Wikipedia, 2013). Used mainly for group discussion forums.
Manual Ping flood	A Ping is a tool for checking the connectivity between two IP hosts. A Ping Flood is a method of achieving a Denial-of-Service (DoS) attack by overwhelming the target computer or system with ping requests. Clearly the attacker must have a greater bandwidth than the target, so requests from huge numbers of computers will generally be used to overwhelm the target computer. Because the target will usually generate automatic (echo) responses, both incoming and outgoing bandwidth is affected. The target uses so much CPU time managing the requests that other services it provides are slowed down or disabled.
NATO	North Atlantic Treaty Organisation
Network Centric Warfare	Is a theory of warfare, based on better use of information(D S Alberts, Garstka, & Stein, 2000).
Spam	The use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. (Wikipedia, 2013)
IP Address	Internet Protocol Address: a numerical label assigned to each device in a computer network. This includes all devices, printers, scanners, etc. as well as computers. It is used to locate and address devices on the network.
ISP	Internet Server Provider: this is a company that provides access to the Internet.
Security Patches	A Patch is a piece of software designed to fix problems with, or update a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs, and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems(SoftwareUpdates, 2013).

Executive Summary

a. Focus and Boundaries

The level of analysis is at the Collective due to the involvement of a number of organisational units operating in a collaborative Command and Control (C2) manner. The specific organisational units involved were CERT-EE, Estonian MoD and NATO as well as local and international IT Security Experts.

There are two main temporal boundaries, namely Political and Cyber. The attackers determined the phases and with respect to C2 Agility, they created an environment to their advantage restricting their opponents which is classical Network Centric Warfare.

The events associated with the attack included both the cyber attack itself and a wider civil unrest. The analysis of C2 approach must acknowledge these different boundaries. It is concluded that to correctly understand the nature of agile C2 in this context, the analysis must encompass the wider set of interactions and view the cyber attack(s) only as a part of the wider actions.

Analysis is enhanced by considering the C2 approach of both attackers and defenders, although it is acknowledged that there is a lack of specific information on both sides and the approaches have been deduced only from published material. However, cyber attacks appear to be the very epitome of asymmetric warfare and as such the relative C2 of the opposing forces is significant in its own right.

b. Challenge or Opportunity for C2 Agility

The challenge facing the Estonians was the specific nature of the attack. This type and form of attack was something which the Estonians have never experienced before and they had no procedure for dealing with it; at the time of the attack the Estonians had no national Cyber Security Strategy, but did create one the following year in 2008. The Estonians needed to be agile, but lacked Shared Situational Awareness (SSA) and a Cyber COP (Common Operating Picture) to help them to analyse and respond to the challenge with optimum agility. The SSA and an equivalent Cyber COP was created on the fly in a dynamic exploratory manner involving national and international organisations, such as CERT-EE, MoD, NATO and national and international IT Experts. The Estonians simultaneously experienced different types of attack from psychological, physical and Cyber.

It is speculated that the opportunity from the Russian perspective was one of ideology and a broader message to countries in and around Estonia who have recently joined NATO perhaps warning them of the consequences of what could happen if you get too close to NATO. One could also argue that the Russians wanted to project their power over Estonia and the Cyber attack was one medium in which they could do this.

c. Was Agility Manifested? If so, How?

It is clear that agility was manifested by the Estonians and that as far as the cyber attacks were concerned, the choice of a collaborative C2 from the outset was a factor in being able to recover from the cyber attacks. The choice of collaborative C2 was necessitated by the need to draw on expertise from a wide set of sources (both from internal and overseas sources). The Estonians showed agility in the way the counter measures were organised and managed collaboratively with a number of key national and international organisations, such as CERT-EE, MoD, NATO and IT Experts. The Estonians were able to switch some web sites to “lightweight mode” for example as one of their counter measures.

However, the C2 approach for the wider conflict, that included civil unrest, seems to have been de-conflicted; it is not clear that this was the best choice for overall agility. It is not clear, then, that the Estonians exhibited significant C2 agility in the context of the wider conflict.

Nevertheless, tt seems that the Estonians demonstrated sufficient C2 Agility with regard to the cyber aspects of the attacks to reduce their impact and the overall timeline, thus minimising the economic impact. The extent to which the economic consequences were mitigated cannot be established unambiguously; because it is not clear to what extent the reduction in attacks were simply the result of the attackers desisting, rather than being weakened.

From the attacker perspective, C2 Agility was manifested by the sheer volume of the co-ordinated attacks leading to the high impact and it would appear that different C2 approaches were adopted by different groups of attackers; however, the cyber-attacks (and some aspects of the physical attacks) seem to have relied principally on Edge C2.

d. Enablers and Inhibitors of C2 Agility

The Estonians were able to react to a change in the environment in a timely manner (responsiveness) and identified multiple ways to succeed and move seamlessly between them (flexibility). However, in terms of resilience they overcame losses, damage, and setbacks (the ability to recover from or adjust to misfortune/damage, and the ability to degrade gracefully under attack or as a result of partial failure). (SmallWarsJournal, 2013)

The attackers were able to react to a change in the environment in a timely manner as evidenced by two pronged Cyber-attack (responsiveness) and identified multiple ways to succeed in their Cyber attack (flexibility). They were able to do new things and the ability to do old things in new ways (innovativeness) for example DDoS attacks and were able to change work processes and the ability to change the organization in order to take advantage of characteristics of a situation (adaptiveness).

e. Summary of Observations/Conclusions about C2 Approach Agility

The Estonians showed De-conflicted C2 Approach as shown in Figure 4 by the avoidance of adverse cross-impacts between and among the participants by partitioning the problem space and the solution space. They introduced counter measures collaboratively with national and international parties which included CERT-EE, MoD, NATO and IT Experts to bring the situation under control and to normal levels.

The attackers showed Agile C2 Approach, because they were able to provide the enterprise with additional C2 approach options that involved working more closely together in terms of the synchronisation of the attacks which occurred in two phases. For example, working alongside the Russian media and implementing the most appropriate approach to coalition C2, given the situation (e.g. mission, conditions, and set of coalition partners – contributing entities). For example, it was reported that computers in 178 countries were involved in the Cyber attack against Estonia in Spring 2007. However, the level of C2 Agility declined with the introduction of the Estonian counter measures.

f. Important stories or vignettes in the case study

Two vignettes have been produced in the form of a flow chart depicting decision points and command and control (C2) activity for the cyber attack from the attacker perspective, i.e. the cause and from the Estonian perspective, i.e. the effect, but without formally presenting this as a cause-effect tree or analysis and summarised in the Decision Tree table.

An introductory note on sources used for this Case Study and its relevance

Although there has been a considerable amount of analysis and a substantial number of reports published concerning the cyber attack on Estonia in 2007, there is no publically available document that definitively states the nature of the Command and Control. The information provided in this case study is, therefore, the authors' assessment based on analysis of the behaviours as reported in the various sources referenced for this study. The C2 approach for both the defenders (Estonian Government) and the attackers (Russian organisations) has been derived. There is no independent corroboration of the C2 approach that has been derived herein for either organisation.

Cyber warfare in many respects represents the ultimate example of asymmetric warfare; attack is comparatively easy and inexpensive, defence is highly complex and, generally, very expensive. This case study suggests that Co-ordinated or Collaborative C2 approaches are most appropriate for defence, whereas the Edge C2 approach is ideally suited to effective cyber attack of the types exemplified in this case study.

Identify the Focus of and the Boundaries for the Case Study

a. **What is the level of analysis? (e.g. Individual, Team, Organization, or Collective)**
   The level of analysis is at the Collective due to the involvement of a number of organisational units operating in a collaborative Command and Control (C2) manner. The specific organisational units involved were CERT-EE, Estonian MoD and NATO as well as local and international IT Security Experts as depicted in Figure B.2.1

   Although the case study is ostensibly concerned with a cyber attack, the analysis has indicated that the nature of the conflict can only be properly understood by considering the cyber aspects in context of the wider activity. Furthermore, it is observed that it is important to understand attackers C2 and defenders C2 within equivalent boundaries.

b. **Who or What Organizations are included in the case study?**
   The Estonians showed a remarkable degree of agility bearing in mind the cyber attack was the first of its kind to hit the country. Entities such as CERT-EE, MoD and NATO with support of local and international IT Security Experts were able to work closely together with the ability to identify and implement the most appropriate approach to coalition C2 given the situation.

   On the Estonian side the following organisations were involved: CERT-EE, Estonian MoD and NATO as well as local and international IT Security Experts as illustrated in Figure 1.

   On the attacker side, it has been speculated that the following organisations were involved: Russian Parliament, Russian Media, and the Nashi Russian political youth movement. It should be noted that the Russian Parliament has always denied involvement and that NATO has not found proof of official Russian Government involvement in the attack. However, the Head of Russian Military Forecasting Center, Colonel Anatoly Tsyganok appeared to support the speculation of Government involvement by confirming publically that Russia was capable of such an attack(Thomas, 2010). For the purposes of this

case study, the Russian Government is included as an organisation in the conflict (figure 1). If not the Russian Government, then some co-ordinating body should be assumed to be involved.

In terms of C2 Agility from the attacker perspective they appeared to display a combination of approaches, including Edge C2, Co-ordinated C2 and De-conflicted C2 as defined by the six C2 maturity levels(Moffatt & Alberts, Dec. 2006). The attackers were very successful in avoiding adverse cross-impacts between and among the participants by partitioning the problem space and the solution space (De-conflicted C2). This allowed them to increase the overall effectiveness in a number of ways by seeking mutual support for their intent and the increased sharing in the information domain to increase the quality of information being presented to the public.

c. What temporal boundaries are included?

There are two main temporal boundaries, namely Political and Cyber as depicted in Figure 1 and Figure 2, respectively.

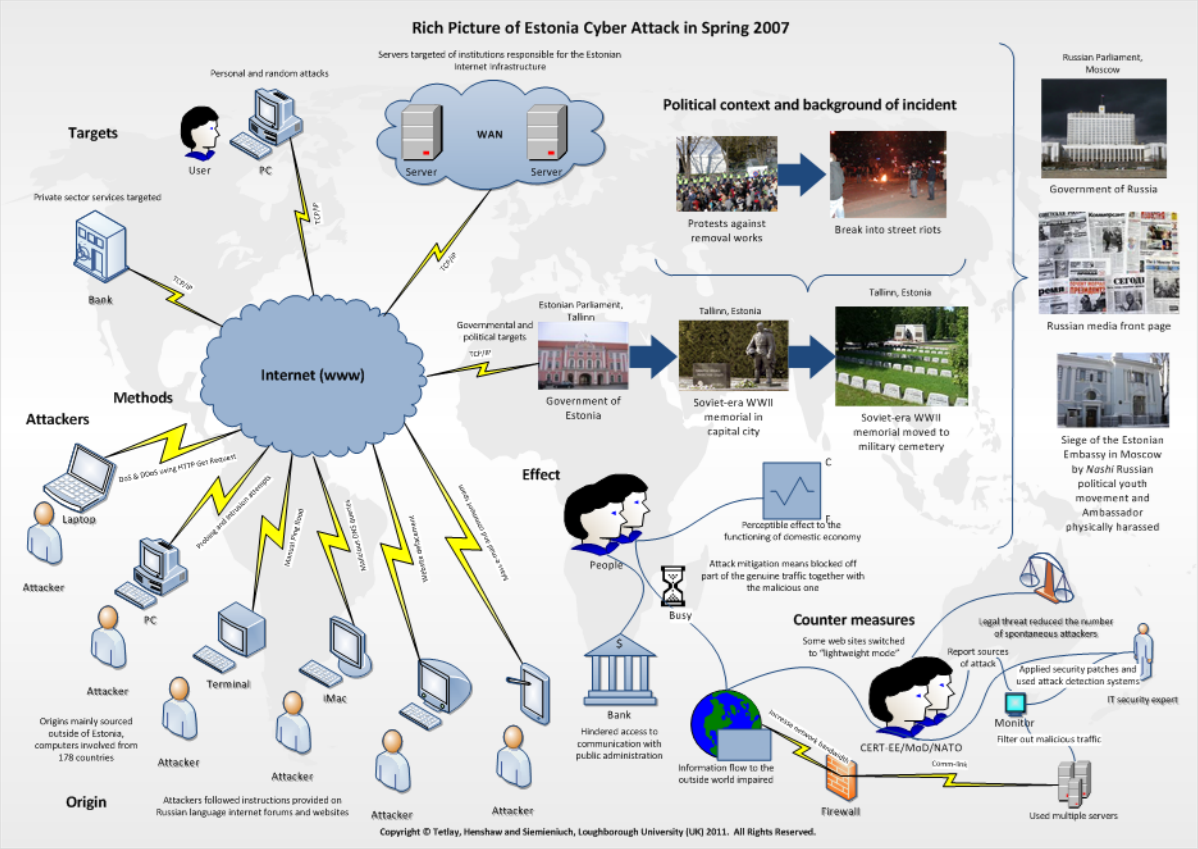


Figure B.2.1: Rich Picture of Estonia Cyber Attack in Spring 2007

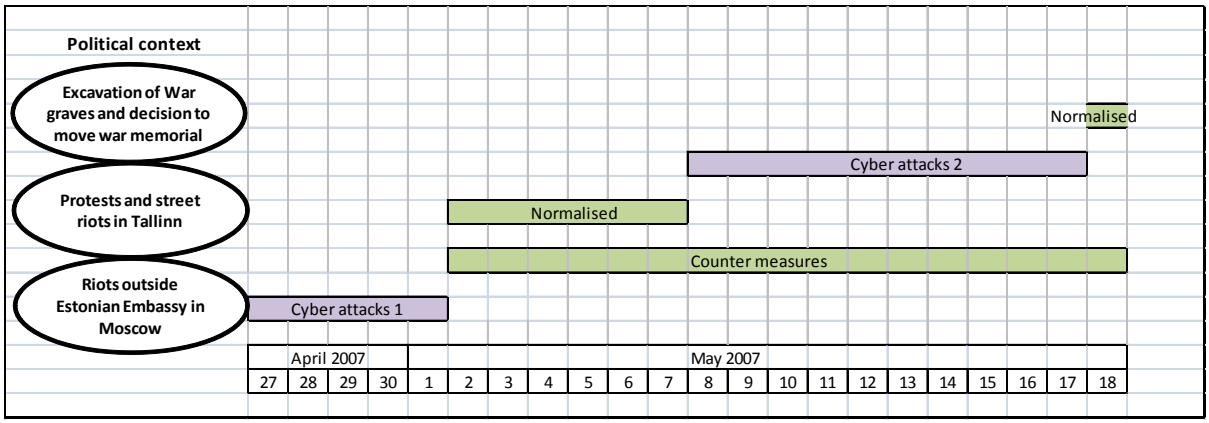


Figure B.2.2: Timeline of the Estonia Cyber Attack in Spring 2007

The Rich Picture (Figure B.2.1) based on (2011) provides a précis of the cyber attack on Estonia in Spring 2007, showing the:

Political context and background of incident

The Estonian Government announced a decision to relocate a WWII memorial, from the Soviet era, from a location in the centre of the capital city (Tallinn) to a military cemetery outside the centre. This was opposed by the Russian Government and media. As a result, protests against the removal works began and these developed into riots in Tallinn. There was also a siege of the Estonian embassy in Moscow by the Russian political youth movement (Nashi) and the Estonian Ambassador was harassed physically.

Methods of Attack

The attackers used the following methods:

- DoS & DDoS using HTTP Get Request
- Malicious DNS queries
- Probing and Intrusion attempts
- Manual Ping flood
- Mass e-mail and comment spam
- Website defacement

Targets

The attacks progressively developed against a range of Estonian targets. These were Servers of institutions responsible for the Estonian Internet infrastructure, then Governmental and political targets. The attacks then progressed to services provided by the private sector (e-banking, news organisations). Personal and random targets were also attacked.

Origin of the attacks

The attacks came mainly from outside Estonia and computers from 178 different countries were involved. Following the posting of instructions on Russian language internet forums and websites, the early (first phase) attacks were largely carried out by nationalistically or politically motivated individuals. The second phase of attacks had features of a centralised Command and Control (C2). The Russian authorities denied any involvement.

Effect

The attacks impacted communication both within and outside of Estonia. Information flow to the outside world was impaired and access to public administration sites was hindered. This means that information and services from Government were unavailable to citizens. A side-effect of the attacks was that the mitigation actions also blocked part of the genuine traffic as well as the malicious traffic. Cumulatively, this had a perceptible effect on the domestic economy by disrupting sectors of commerce, industry and government because of their reliance on ICT infrastructure and electronic communications. The day-to-day operation of banks, media corporations, government institutions, small and medium size enterprises were all adversely impacted.

Counter measures

The response was co-ordinated by the Computer Emergency Response Team for Estonia (CERT-EE) with assistance from experts and system administrators within and outside the country. IT experts from public and private sectors engaged round-the-clock. An important aspect in responding to the attacks was international co-operation that was organised by the Ministry of Defence. They informed partners in the EU and NATO. NATO network incident handling entities provided advice and national CERTs (US, Germany, Finland) helped to locate sources of attack.

The technical measures enacted were to increase the bandwidth of the communications systems, and the use of multiple servers and/or connections. Firewalls were introduced to filter out malicious traffic and security patches were applied to reduce vulnerabilities. Some sites were temporarily switched to “lightweight mode” to reduce the effect of ping floods etc. and additional attack detection systems were introduced.

There was also a campaign to raise public awareness by broadcasting news about Estonia co-operating with foreign authorities to locate cyber criminals and bring them to justice. This reduced the number of spontaneous attacks.

a. When does the case begin and end?

Figure 3 depicts the start and end dates of the Cyber attack against Estonia in the Spring of 2007; this draws largely on information from(2011). It also illustrates the phases and the events which took place during the attack.

b. Are there phases involved? If so, what are their boundaries?

The attackers determined the phases; and with respect to C2 Agility, they created an environment to their advantage restricting their opponents which is classical Network Centric Warfare (see Figure B.2.3).

Phase	Date	Activities
		PHASE 1
Phase 1: Emotional Response	27-Apr-07	• Simultaneous attacks against multiple websites of the Estonian government and government agencies. • Access to websites temporarily limited for users located outside of Estonia. The cyber attacks start simultaneously with rioting on the streets of Tallinn late on Friday. The attacks on e-services continue from this date until the end of May when the tensions over the bronze soldier statue begin to subside. The first phase of attacks (27-29 April) is described as emotionally motivated; the attacks are relatively simple and the co-ordination is rather ad hoc. The attacks are labelled “cyber riots”. Calls appear on various Russian-language internet forums with instructions to launch ping commands (simple commands to check the availability of the targeted computers).
	28-Apr-07	• Multiple-sourced Distributed Denial of Service (DDoS) attacks • Media outlets carrying news of the street riots and political situation are also attacked. Executable .bat files were made available for users to copy onto their own computers. They could then launch automated ping requests, which achieved denial of services (DoS). Because they are co-ordinated, they are effective at disturbing their targets. Attacks were also co-ordinated via IRC (Internet Relay Chat). Pinging was followed by malformed web queries to government and media websites. This latter represented the use of a more specific means of attack.
	29-Apr-07	• Malicious attacks originating from outside of Estonia. • Access for users situated outside of Estonia limited due to technical

Phase	Date	Activities
		countermeasures taken to handle the attacks. In general, the attacks from 27-29 April were simple and ineptly co-ordinated and were easily mitigated.
		PHASE 2
Phase 2: Main Attack	30-Apr-07	• Cyber attacks continue. • Attempts to halt the functioning of the entire public sector data communications network. The second phase was characterised by a better co-ordination of more sophisticated attacks; in particular, the second phase included the use of larger botnets. The co-ordination of the attacks led to four major waves, as discussed below, with some attacks having clear historical significance. The co-ordination was managed in the same way as the first phase, i.e. the use of Russian language internet forums to distribute instructions and details of targets to attack. The style of the postings to the internet forums was very simple instructions that did not require advanced technical knowledge, thus it was possible to participate with only a computer and an internet connection. The attacks had a greater impact because of the co-ordinated scheduling of the attacks, which generated greater volumes of simultaneous queries sent to the targets. The domain name servers (DNS) and routers that were run by Elion (Estonia's largest telecommunications and internet provider) were repeatedly attacked between 30 April and 3 May causing service disruptions. Throughout phase 2 the network traffic was above the normally expected levels, even outside of the peak attacks, but generally these attacks were manageable. Nevertheless, some sites remained inaccessible for periods of time.
	01-May-07	• The number of attacks increased during the early hours of the morning; these mainly targeted web and name servers of government entities. Implementation of new technical counter measures causes some short-term unavailability of websites in Estonia itself, but the situation is under control.

Phase	Date	Activities
		• There are three serious attacks at 8 pm, midnight, and 11 am that affect web traffic.
	02-May-07	• Normality returns and communication networks function normally. Government websites are viewable, though some running on minimised versions.
	03-May-07	• Although the volume of internet traffic is higher than usual, implementation of security measures and additional server capacity maintains data communication networks. • Attacks begin against online media outlets and private enterprises. • There is a large DDoS attack on government internet traffic and web services. Co-operation between ISPs mitigates this attack.
	04-May-07	**FIRST WAVE OF ATTACKS (4 May)** There was an intensification and precision in the concentration of DDoS assaults on websites and DNSs that indicated co-ordination and the use of botnets. The attackers used various means to conceal their identities including the use of global botnets, routing the attacks through proxy servers in other countries (including NATO countries), and spoofing their IP addresses. • There are reports of increased volumes of spam-email. • In the early morning, the Estonian websites availability is unstable/unreliable for users located abroad.
	05-May-07	• The situation is relatively calm.
	06-May-07	• The situation is relatively calm.
	07-May-07	• International co-operation in fending off the attacks is clearly starting to pay off. • In order to minimise possible risks, all government and private sector IT specialists, as well as home users, were requested to pay special attention to security settings of their computers and networks in order to avoid being taken under hacker control.
	08-May-07	• At 11 pm, a large cyber attack commenced that carried on for a long

Phase	Date	Activities
		time. • Government websites and data communications networks remain the main targets.
	09-May-07	**SECOND WAVE OF ATTACKS (9 – 11 May)** The 9th May is a national holiday in Russia in celebration of victory day, on which the defeat of Nazi Germany is remembered. This date was, therefore, significant with reference to the bronze memorial solider, about which there was controversy between Estonia and Russia. A new wave of attacks was, therefore, anticipated and they materialised at 23:00 (Estonian time) on 8th May, which was the start of 9th May in Moscow. The DDoS attacks increased by about 150% and lasted throughout 9th and 10th May. Once again the attacks targeted Government information websites, but were not as intense as previous attacks. This time, though, the banks experienced sustained DDoS attacks that lasted from 9th May until 11th May. • Cyber attacks appear to be attempting a "cyber blockade" of Estonia. • Dissemination of information hindered from Estonia to the outside world. • Estonia's largest commercial bank (Hasapank) unavailable to customers for 1.5 hours.
	10-May-07	• Attempts to cyber blockade Estonia continue, with both the public and the private sector targeted. • There are many large-volume attacks that lasted a long time taking place in parallel. • The work of Hansabank (the country's largest bank) Internet channels are disrupted; it is unavailable to customers for 2 hours.
	11-May-07	• No information
	12-May-07	• No major attacks reported.
	13-May-07	• No information

Phase	Date	Activities
	14-May-07	• Minister of Defence raises the issue of cyber attacks against Estonia at a meeting with EU defence ministers.
	15-May-07	**THIRD WAVE OF ATTACKS (15 May)** Approximately twelve hours of strong DDoS attacks. This involved a large botnet of approximately 85,000 hijacked computers. The attacks were largely directed against Government websites and banks. Because, by now, network capacities had been increased in response to the earlier attacks, the increase in network traffic did not post too much of a threat. • Attacks against the second largest commercial bank, SEB Eesti Ühispank. Off line for about 1.5 hours.
	16-May-07	• By midnight, single large attacks had sub-sided to weekend level.
	17-May-07	• No information
	18-May-07	**FOURTH WAVE OF ATTACKS (18 May)** Another large DDoS attack against government websites occurred. Banks continued to experience some disruption even after this date, although this was much diminished. • Continued filtering of network traffic in co-operation among IT security staff of public and private sector entities in co-ordination with CERT-EE.

Source: Estonian Informatics Centre

Figure B.2.1: Phases and Timeline of the Estonia Cyber Attack in Spring 2007

d. Other boundaries (e.g. separate analyses of the collective and of specific organizations within the collective).
N/a

Describe the Challenge or Opportunity that gave rise to the need for C2 Agility

The challenge facing the Estonians was the specific nature of the attack. This type and form of attack was something which the Estonians have never experienced before and had no procedure for dealing with it; at the time of the attack the Estonians had no national Cyber Security Strategy, but did create one the following year in 2008. The Estonians needed to be agile, but lacked Shared Situational Awareness (SSA) and a Cyber COP

(Common Operating Picture) to help them to analyse and respond to the challenge with optimum agility. The SSA and an equivalent Cyber COP was almost created on the fly in a dynamic exploratory manner involving national and international organisations, such as CERT-EE, MoD, NATO and national and international IT Experts. The Estonians experienced different types of attack from psychological, physical and Cyber.

It is speculated that the opportunity from the Russian perspective was one of ideology and of a broader message to countries in and around Estonia who have recently joined NATO perhaps warning them of the consequences of what could happen if you get too close to NATO. You could also argue that the Russians wanted to project their power over Estonia and the Cyber attack was one medium in which they could do this.

In the spring of 2007 Estonia fell under a cyber attack campaign lasting a total of 22 days. The attacks were part of a wider political conflict between Estonia and Russia over the relocation of a Soviet-era monument in Tallinn. Due to the lack of definitive quantitative data, the author will use qualitative analysis to explain the cyber attacks.

In the spring of 2007 Estonian government agencies, on-line news organizations, banks and many others fell under a wide scale cyber attack. In order to analyze the cyber attacks that took place in Estonia from April 27th to May 18th 2007.

27th of April marked the beginning of cyber attacks that targeted Estonian internet-facing information systems. Attacks of various types continued for a total of 22 days. Even though the attack types were well known, they were unparalleled in size and variety compared to a country the size of Estonia. Furthermore, Estonia is highly networked, so a wide scale attack on the availability of public digital services has a significant effect on the way of life of ordinary citizens and businesses alike. Therefore, these cyber attacks cannot be disregarded as mere annoyances but should be considered a threat to national security.

The attacks that had the main impact on the general public were Distributed Denial of Service (DDoS) attacks that ranged in sophistication from single individuals using low-tech methods, such as ping floods, to expensive rentals of botnets (that are usually used for spam distribution). Attacks also included spamming of the larger news portals and commentaries and defacements of websites, including that of the Estonian Reform Party website(Enisa, 2011).

The Estonian authorities, including the Foreign Minister Urmas Paet, accused the Kremlin of direct involvement in the attacks, but the Estonian defence minister later admitted there was no evidence to link the Russian authorities to the attacks.

The most high confidence conclusion that can be drawn from the information presented here is that the attacks were performed by patriotic Russians who were sympathetic to the Russian government's agenda and coordinating their activities on-line. The log analysis is not sufficient to attribute the attack to any specific person, organization or state, because it only covers log events at the target side.

Although the case study ostensibly concerns C2 agility in a cyber warfare context, it is important to note that the cyber attacks took place within a wider context of political activity and street protests/riots. C2 agility is manifested (or not) across a range of activities of which information disruption is a component.

What would have been the consequences of a failure to act in a way that demonstrates C2 Agility?

If the Estonians failed to act in a way that demonstrated C2 Agility then the economic consequences would have been far greater than was experienced. The Estonians demonstrated C2 Agility and thereby reduced the impact of the Russian attack and the overall timeline minimising the economic impact.

Was C2 Agility Manifested? If so, How?

From the Russian perspective, C2 Agility was manifested by the sheer volume of the co-ordinated attacks leading to the high impact and there is evidence that different C2 approaches were used in different parts of the conflict, or by different groups within the conflict. The Estonians also showed Agility in the way the counter measures were organised and managed collaboratively with a number of key national and international organisations, such as CERT-EE, MoD, NATO and IT Experts. The Estonians were able to switch some web sites to "lightweight mode" for example as one of their counter measures. However, it is not clear that the Estonians showed C2 agility, in the sense that the C2 appears to have been a deconflicted approach throughout.

Most of the Attacks were DDoS

Most of the malicious requests were clearly identifiable from the rest of the traffic, because they contained phrases or words that normally do not appear in the traffic. The set of phrases was fairly limited, which made searching much easier. Example queries directed at the police web server are displayed below:

GET /est/0427_05.html?id=493&AnSSip=_A_M_E_R_I_C_A_N__W_H_O_R_E_ HTTP/1.1

Typically such requests were repeated thousands of times in a limited period (e.g. 15,000 queries in 30 minutes). Since such activity is commonplace, it is not clear what percentage of these attacks were related to the conflict. At least 40 different IP addresses were observed at probing or intrusion attempt.

In technical terms, the co-ordinated cyber assault and isolation of Estonia was mitigated by a number of outbound high-capacity fibre optic data links to several countries (Sweden, Finland, Latvia, and Russia), which were owned by a number of e-communication network operators. Furthermore, an agreement was in place between the main e-communication infrastructure-owning operators that enabled them to divert the excessive traffic to a particular ISP(army, 2011). A further technical response was to gradually increase the bandwidth of the state information system servers, so that it had greater capacity for data traffic. By the time of the second wave (9-10 May 2007), the bandwidth of the government networks had increased by several times. Further technical responses included application of security patches, firewalling, more use of attack detection systems, and using multiple servers and/or connections. Access was also blocked to some servers, and the filtering grew more effective as time went on, as patterns in the attack were distinguished. In co-operation with the ISPs, the data transmission capacity of incoming data to Estonia was reduced. Although these measures blocked part of the attack, they also had the negative aspect of blocking legitimate traffic. Some sites were restored to a "lightweight mode" – e.g. the Police Board that temporarily switched to a simple one-page html-view – to better cope with the amount of incoming queries(2011). Use of "lightweight" mode for restored websites reduced traffic (e.g. a Police Board switched temporarily to a simple one-page html view, in order to cope better with incoming queries.

Another aspect of agility demonstration was the expert knowledge at the disposal of the Estonian authorities. The response was co-ordinated by CERT-EE and top IT specialists from the private and public sectors were engaged on a round-the-clock basis(2011).

Which Enablers and Inhibitors of C2 Agility were observable?

The six Enablers and Inhibitors of C2 Agility are:

1. Responsiveness
2. Versatility
3. Flexibility
4. Resilience
5. Innovativeness
6. Adaptiveness

These were used in Figure B.2.4 to determine which Enablers and Inhibitors of C2 Agility were observable.

Enablers/Inhibitors	Estonian Perspective	Russian Perspective
Responsiveness	Yes	
Versatility	Yes	
Flexibility	Yes	Yes
Resilience	Yes	
Innovativeness		Yes
Adaptiveness		Yes

Figure B.2.4: Enablers and Inhibitors of C2 Agility

The Estonians were able to react to a change in the environment in a timely manner (responsiveness) and identified multiple ways to succeed and move seamlessly between them (flexibility). However, in terms of resilience they overcame losses, damage, and setbacks (the ability to recover from or adjust to misfortune/damage, and the ability to degrade gracefully under attack or as a result of partial failure).

The Russians were able to react to a change in the environment in a timely manner as evidenced by the two pronged Cyber attack (responsiveness) and identified multiple ways to succeed in their Cyber attack (flexibility). They were able to do new things and the ability to do old things in new ways (innovativeness) for example DDoS attacks and were able to change work processes and the ability to change the organization in order to take advantage of characteristics of a situation (adaptiveness).

What C2 Approaches were relevant?

At the outset, the Estonians appear to have used a de-conflicted approach to the conflict as a whole, but within this, there was a co-ordinated approach to combating the cyber elements of the conflict (figure 4). The de-conflicted C2 approach avoided adverse cross-impacts between and among participants. As time moved on, the response to the cyber-attacks became collaborative, so that counter measures were introduced collaboratively with national and international parties which included CERT-EE, MoD, NATO and IT Experts to bring the situation under control and to normal levels.

The attackers also showed an Agile C2 Approach as depicted in Figure 4, there appears to have been co-ordination at the overall conflict level, with the carefully synchronised street riots and cyber-attacks. Indeed the riots were labelled ‘cyber riots’. The distribution of information, concerning targets and methods of attack, enabled edge C2 behaviour. For example, it was reported that computers from 178 countries were involved in the Cyber attack against Estonia in Spring 2007. However, in phase 2, the use of massive botnets indicated a more co-ordinated approach to the cyber-attacks. Edge behaviour still continued, but its effect was diminished

because of the counter-measures that the Estonians had put in place. It is clear that the attackers demonstrated C2 approach agility by shifting the emphasis from edge to co-ordinated.

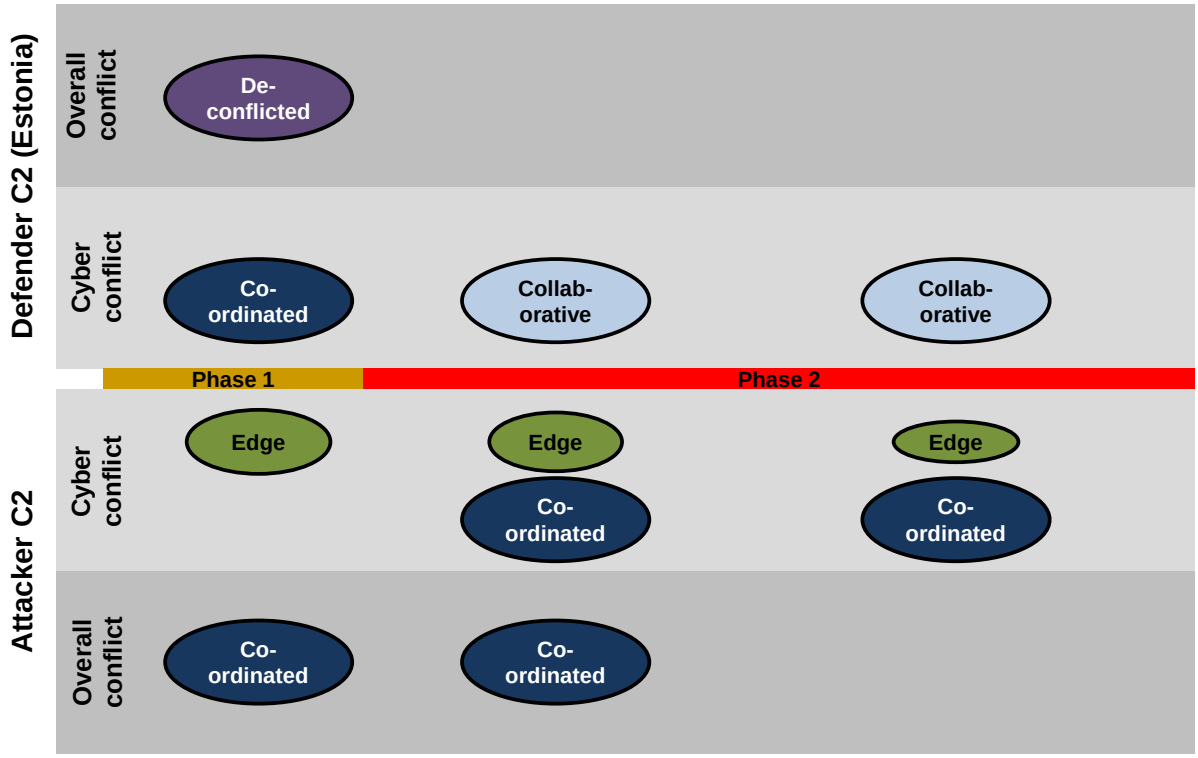


Figure B.2.5: C2 Approaches

What interesting and important vignettes are included or can be derived from the case study to help create illustrative stories?

Two vignettes have been produced overleaf in the form of a flow chart depicting decision points and command and control (C2) activity for the cyber attack from the Russian perspective (Figure B.2.7), i.e. the cause and from the Estonian perspective (Figure B.2.8), i.e. the effect, but without formally presenting this as a cause-effect tree or analysis and summarised in the Decision Tree table below.

Trigger	Event	Question?	Decision	Question?	Decision	Outcome
Preparatory works for the excavation of war graves; Moved WWII memorial from Tallinn to military cemetery in Tallinn	Cyber attack	What do we do now?	Co-ordinate and collaborate a counter measure	With whom?	CERT-EE/MoD /NATO and ISP/IT security experts/ Home users	Introduced counter measures and Situation normalised

Table B.2.6: Decision Tree Table

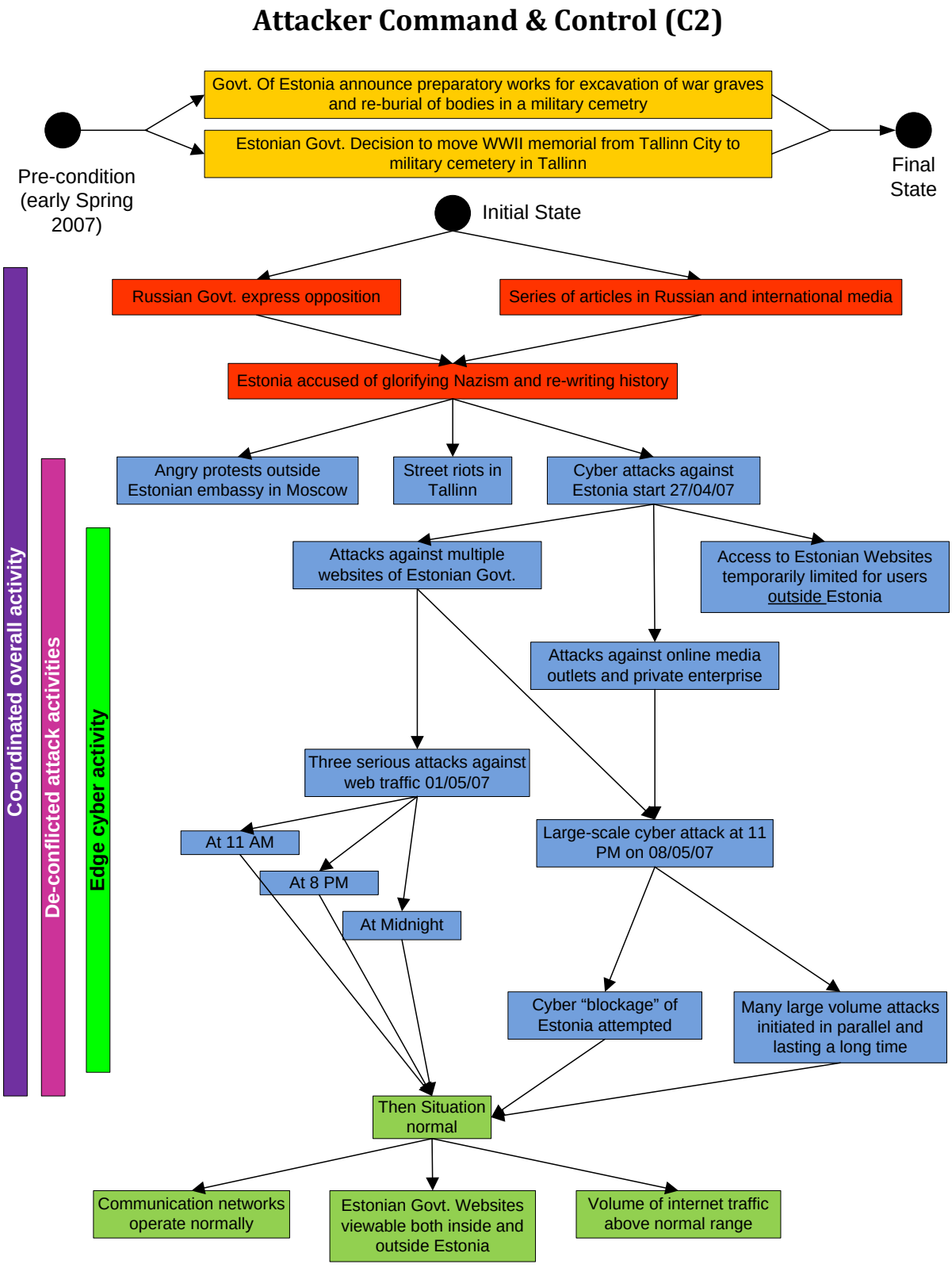


Figure B.2.7: Attacker Command and Control (C2)

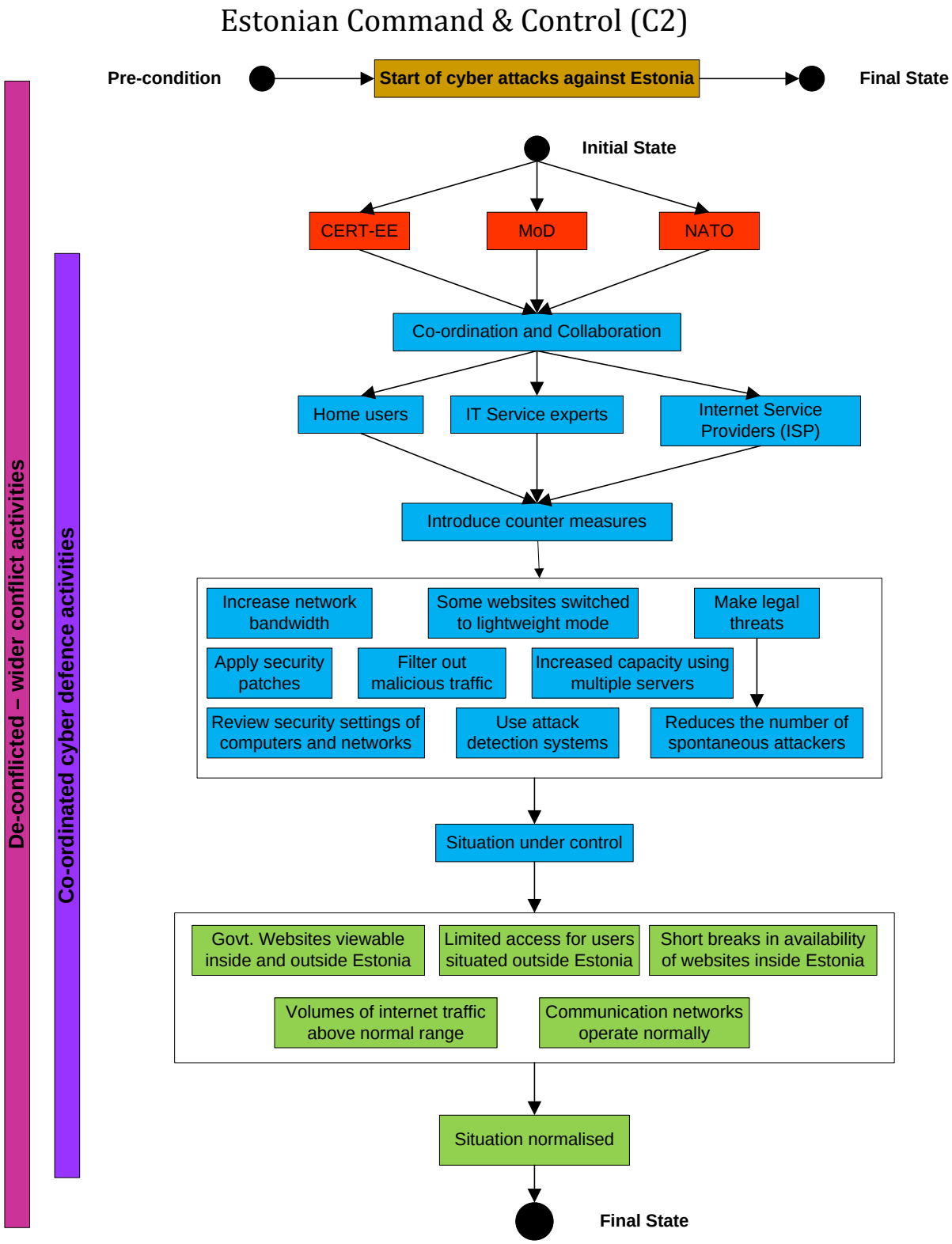


Figure B.2.8: Estonian Command and Control (C2)

Case Study Assumptions and Limitations

a. **What constraints did you encounter that might limit the case study or the evidence supporting it?**
The main constraints which limited the case study were not having enough factual data from the Russian side and only descriptive narrative text was used from the Estonian perspective.

b. **What assumptions did you make when carrying out or documenting the case study?**
It has been assumed that the cyber attack was part of a wider political initiative instigated by Russia. The extent of government sponsored activity, though, is unknown. It has been assumed that the Estonian Cyber attack was instigated by the Russian government with the aid of Russian nationals inside and outside of Estonia.

Conclusions

This case study focuses on the C2 applicable for the cyber attack on Estonia in Spring 2007. The precise nature of the C2 is difficult to determine from publically available documents, but the evidence suggests that the Estonians (as defenders) used a de-conflicted C2 approach, whereas the attackers (assumed to be Russia) used an edge C2 approach, at least in part. It is assumed that the attack originated from Russia, but it is known that attacks were launched from 178 different states by individuals assumed to be sympathetic to the Russian cause.

At the collective level of analysis, an important aspect of a case study, such as this, is that the cyber warfare must be considered in the context of the wider political (and physical) activities. Although the case study focused on the cyber aspects of C2 agility, consideration has been given to the C2 agility for the conflict as a whole. It is noted that a proper understanding of the C2 agility is only possible through consideration of the wider conflict and not just the cyber part of the conflict.

Whilst the Estonians demonstrated agility in their response, it is not clear that this was C2 agility, but rather that it was agility within their chosen C2 approach. On the other hand, it would appear that the attackers used a variety of C2 approaches at different levels (individual, team, organisation, collective), which may be evidence of C2 agility. It is clear that several C2 approaches can be used simultaneously (at different levels) and it seems that cyber warfare may be particularly well suited to edge C2 for attacks. It is possible that defence (of computer networks and computer systems) may also be well suited to an edge approach, but it is not clear that this was demonstrated in this case study.

Acknowledgements

The authors would like to thank participants in the NATO RTO C2 Agility and Requisite Maturity Programme which is part of the US DoD funded Command and Control (C2) Research Programme (CCRP http://www.dodccrp.org/ and SAS-085, Grant Ref. EP/I006672/1 that is developing new models for NATO NEC C2) for their advice, encouragement and for reviewing the draft version of this document.

The authors would also like to thank fellow CCRP colleagues and team members Dr Julius Barath, Dr Richard Hayes and Dr Paul Phister for their initial analysis of the SAS-085 Estonia Case Study for which we are extremely obliged.

Bibliography

[2] Excerpts from Log File Analysis of the Cyber Attacks Against Estonia in the Spring of 2007, June 2009, v 1.0 (Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, ccdcoe@ccdcoe.org)

[3] Georgia Cyber Campaign Overview, 7-16 Aug08

[4] Cyber Attacks Against Georgia: Legal Lessons Identified (Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm, Liis Vihul, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, ccdcoe@ccdcoe.org)

[5] Estonia Country Report (European Network and Information Security Agency—ENISA, Jan10, http://www.enisa.europa.eu)

[6] International cyber Incidents: Legal Considerations (Eneken Tikk, Kadri Kaska, Liis Vihul, Cooperative Cyber Defence Centre of Excellence—CCD COE, www.ccdcoe.org, 2010)

[7] Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective (Ran Ottis, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia)

[8] Maturity Levels for NATO NEC Command, TR21958 v.2.0, Dec. 2006, James Moffat and David S Alberts

Works Cited

Alberts, D. S., Garstka, J. J., & Stein, F. P. (2000). *Netwrk Centric Warfare - Developing and Leveraging Information Superiority* (2nd ed.). CCRP.

army, c. (2011). Retrieved 2011, from www.carlilse.army.mil

Cyber Conflict Studies Association. (2011). Retrieved FEb 12, 2013, from http://www.cyberconflict.org/

Enisa. (2011). *enisa europa*. Retrieved Feb 2013, from www.enisa.europa.com

Farlex. (2013). *The free dictionary*. Retrieved February 14, 2013, from http://www.thefreedictionary.com/
Long Mile Computers. (2013). *Software Updates*. Retrieved Feb 18, 2013, from http://longmilecomputers.ie/IE/software_update.html
Moffatt, J., & Alberts, D. S. (Dec. 2006). *Maturity Levels for NATO NEC Command.*
PC Mag. (2013). *PCMag.com*. Retrieved FEb 18, 2013, from http://www.pcmag.com/encyclopedia_term/0,2542,t%3DHTTP&i%3D44501,00.asp
Small Wars Council. (2013). *Small Wars Journal*. Retrieved Feb 12, 2013, from http://council.smallwarsjournal.com/
Thomas, T. L. (2010). RUSSIAN INFORMATION WARFARE THEORY:THE CONSEQUENCES OF AUGUST 2008. In S. J. Blank, & R. Weitz, *THE RUSSIAN MILITARY TODAY AND TOMORROW:ESSAYS IN MEMORY OF MARY FITZGERALD* (p. 282).
Wikipedia. (2013). *Wikipedia, the free encyclopedia*. Retrieved FEb 2013, from http://en.wikipedia.org/wiki/Botnet

B.3 Georgia Cyber Attack in August 2008

Author: Prof. Michael Henshaw

Introduction

The Russian-Georgian war of August 2008 was relatively small and of short duration, but it is highly significant historically as the first example of cyberspace actions that were synchronized with military action in the physical domain (Hollis, 2011). Although the Russian Government have denied involvement in the cyber-attacks, the regional targeting of cyber-attacks were so closely linked to the areas of subsequent military offensive action that an absence of high-level co-ordination appears implausible (Markoff, 2008).

South Ossetia is a territory about 60 miles to the North-West of the Tblisi (capital of Georgia); after the collapse of the Soviet Union, S. Ossetia claimed independence from Georgia, but this was not accepted by the international community. Following the Georgian War (1991-92) S. Ossetia broke away and became, de facto, an independent republic. The majority of the S. Ossetian population is ethnically distinct from Georgians, with their own language and an affinity with Russians. Tensions remained high in the region and a peace-keeping force of Ossetians, Russians and Georgians was established. A similar situation existed in Abkhazia following a war in 1993. S. Ossetia received considerable financial support from Russia after the Georgian war (CCDCOE, Nov 2008). Tensions in the region continued to rise and spilled over into conflict in August 2008.

The conflict included conventional military operations conducted by Russian armed forces and S. Ossetian militia against the Georgian armed forces; however, cyber attacks against Georgian public and private business websites significantly disrupted the Georgian Government's ability to inform its own population and interested parties outside the country of the conflict; this impacted its conduct of military operations. In many ways, the conflict could be considered to be conventional; attacks on communications are a part of conventional warfare, it just so happens that in this case the communications systems were attacked using cyber mechanisms.

Data Sources

This case study has been developed from a number of openly published sources; it has not been possible to authenticate the conclusions about C2 approach, but they are inferred from the news reports and analyses presented in the open literature, especially the analyses contained in (CCDCOE, Nov 2008) and (Unit, 2009).

Comparison with Estonia cyber-attack in 2007

Although there are many similarities between the cyber-attack on Georgia and that which took place a year earlier in Estonia, it is important to identify some particular distinctions. Firstly, the level of co-ordination between cyber-attacks and events in the physical domain are different. Initially, there was no co-ordination in attacks on Estonia, although this did develop later in the second phase. Secondly, the impacts were somewhat different; in 2008, Georgia was not comparable to Estonia as an information society, with only a very small proportion of the population having access to the internet (CCDCOE, Nov 2008). Whereas, the cyber-attacks in Estonia significantly impacted economic targets (banks etc.) this was less pronounced in Georgia, with the main focus being on preventing the Georgian Government from promoting its point of view and distributing necessary information concerning the progress of the war. The impact was felt as a direct disruption to military effectiveness.

The attacks in Estonia and Georgia were similar, though, in the nature and mechanisms used; focusing primarily on denial of service.

Focus of, and the Boundaries for, the Case Study

Level of analysis

The C2 approach has been considered from both the Georgian and the Russian sides. On the Georgian side, the analysis has been at the collective level. For the Russian side, the analysis has also been conducted at the collective level; however, it is important to note that the Russian Government denied involvement in the cyber-attacks, though the military involvement in the physical conflict is clear. The coincidence of cyber and physical attacks tends to suggest that senior level co-ordination was present, but Russia has claimed that the cyber-attacks were simply the work of individuals sympathetic to Russia's position. In 2009, Georgian National Security Council chief Eka Tkeshelashvili claimed she knew exactly who was behind the network assault: "There's plenty of evidence that the attacks were directly organized by the government in Russia." (Shachtman, 2009), however, proof was lacking.

Organizations included in the case study

The Russian C2 appears to have been co-ordinated, but relied on Edge C2 for the cyber aspects of the conflict. In fact, the cyber attacks appear to have originated from a diverse groups comprising Russian hacker forums, the RBN (Russian Business Network) which has been linked to criminal activity, SoftLayer Technologies, Inc, which is controlled by Atrivo that is linked to spread of malware and various cyber crimes, and cyber activists

sympathetic to the Russian cause (CCDCOE, Nov 2008). The Russian military are clearly included in the conflict in the physical domain.

The Georgian C2 was deconflicted, at the overall conflict level, with the military and cyber activities being managed separately. In terms of the cyber activities, though, the C2 seems to have been collaborative, with considerable collaboration occurring between CERT-EE (Computer Emergency Response Team for Estonia), CERT Georgia, CERT Poland and CERT France. Various private individuals provided alternative servers to host Georgian websites, and the Georgians displayed a level of agility in the speed with which information was transferred to these sites. The advisers from other countries (especially Estonia) were called in very quickly and the knowledge gained the year before in Estonia concerning countermeasures was applied quite rapidly. Georgian hacker forums are also considered, although they were, in fact, effectively neutralized prior to the attacks (i.e. they were attacked first). This prevented Georgian hackers conducting countermeasures against Russian-sympathetic hackers. Co-ordination between the cyber experts and the military seems to have been lacking. (Hollis, 2011) has noted that more sophisticated fusing of data concerning cyber activity could have been used to improve military situational awareness by, for instance, identifying the geographic location of the next military attacks. The Georgian Government, as targets of the cyber attacks is included in the case study analysis.

Temporal boundaries

Although there is a wider political context, the temporal boundaries for the relevant C2 analysis concern only the period immediately before and during the attacks. There are no distinct phases for this conflict, unless one considers the first stage, in which dress rehearsal attacks were experienced about three weeks prior to the conflict, to be preparatory and the second stage to be the main conflict.

Political context of war

The political context has been briefly described in the introduction. Tensions had existed between Georgia and S. Ossetia from 1992 and there were occasional flare-ups of violence. Exchanges of fire occurred in June 2008. The trigger for the Georgian-Russian war of 2008 was, however, a Georgian attempt to reconquer S. Ossetia on 7th August 2008 through a large-scale military offensive. In 2009, a special report commissioned by the European Union (EU, 2009) concluded that this attack was not justified by international law.

Origin of cyber attacks

In a speech in November 2009, the Georgian National Security Council chief, Eka Tkeshelashvili suggested a three-part hierarchy to the attacks; she stated (Shachtman, 2009):

> *At the top of the hierarchy are the "Soldiers": the professional planners, computer scientists, engineers, and other implementers, including the military itself. Next are what some call the "Mercenaries." These are criminal organizations paid to carry out certain elements of the attacks. In this case, there are strong signs implicating an outfit known as the Russian Business Network (RBN). And, finally, there are the "Volunteers." These are individuals with PC's who are recruited to carry out attacks. They are provided with access to all the necessary software tools, as well as to detailed instructions for carrying out the attacks. In other words, they don't have to be skilled and "educated" hackers. This is literally a mobilization of the masses."*

Her suggestion is that the attack was a well-co-ordinated and effective use of cyber effects to disrupt communications to such an extent that the Georgian Government was temporarily prevented from operating their cyberspace and informational capabilities during operations (Hollis, 2011).

If one considers Tkeshelashvili's analysis to be correct – and note that it is not substantiated except by circumstantial evidence – then the three hierarchies can be considered to represent three levels of C2 approach: Co-ordinated at the professional level, collaborative at the mercenary level, and edge at the criminal organization and volunteer level. For the purposes of the analysis here, we consider only two levels, as there does not appear to evidence available publically to support the mercenary assertion.

Methods of cyber attack

The main methods of attack were defacement of Georgian public websites and DDoS (Distributed Denial of Service) attacks. Defacement attacks were designed to discredit the President of the Republic of Georgia, Mikheil Saakashvili; photographs of him were posted on his Presidential website alongside photographs of Hitler striking similar poses. Similarly, photographs of the president were included in a collage of photographs of 20th century dictators on the website of the National Bank of Georgia.

DDoS attacks targeted both public and private websites. These included various departments of Government, news and media sites hosted within Georgia, and financial institutions.

Batch scripts were distributed via Russian blogs, forums and other websites in order to attack Georgia. Also instructions on how to ping flood the government sites were distributed on Russian language sites. An email list

for Georgian politicians, that was originally created by a lobbying organization, was circulated to help direct the distribution of malware.

In fact, these various attacks created a cyber blockade of Georgia. Although short-lived, attacks were targeted into geographical areas where the conflict was taking place, making it difficult for Georgia to communicate its own point of view and general information messages.

Effect of cyber attacks

In 2007, Georgia had comparatively few internet users; about 7% of the population were internet users, compared to 57% and 32% in Estonia and Lithuania, both of which also suffered significant cyber-attacks around the same period (CCDCOE, Nov 2008). However, the cyber-attack was effective in preventing the Georgian Government from communicating current news of events concerned with the conflict to Georgians but, more particularly, to the outside world. It also prevented the Georgian Government from broadcasting its own perspective on the conflict.

It is generally the case that disruption of enemy communication is an important part of a conflict strategy, in this sense, a cyber-attack is no different from any other attack designed to disrupt enemy communications.

Countermeasures

A number of the affected websites temporarily changed their IP addresses and some changed hosts. The overall cyber defence strategy was managed by CERT Georgia; although their role is usually to support educational institutions, during the attacks they assumed the role of national co-ordinator (CCDCOE, Nov 2008). CERT Poland and CERT France carried out analysis to support the introduction of countermeasures and two specialists from CERT Estonia arrived in Georgia to support local CERT.

Boundaries and phases of the case study

There is a single phase to the attacks, although certainly there was a period of preparation before the conflict began on 7th August 2008. The following timeline is drawn from several sources, but mainly from a comprehensive timeline provided on Wikipedia (Wikipedia, 2013); it treats only the main events without significant detail. Because of the supposed co-ordination between military and cyber conflict, the timeline is

annotated with (POL), (PHY), or (CYB) to indicate events that happened in the Political, Physical (i.e. military), and cyber domains respectively.

Date **2008**	**Event**
16Apr	(POL) Russia establishes direct official relations with secessionist authorities in Abkhazia and South Ossetia.
14-15Jun	(PHY) Violent clashes in S. Ossetia: S Ossetian authorities report that Georgian forces shell Tskhinvali and fired on S. Ossetian militia on outskirts of Tskhinvali. (POL) Georgia claims this is a response to Ossetian shelling on Georgian villages: Ergneti, Nikozi, and Prisi.
Early July	(CYB) "Dress rehearsal": evidence of synchronized cyber-attacks on Georgian Government sites (Hollis, 2011) (Markoff, 2008)
5Jul	(PHY) Russia conducts military training exercises (called Caucasus Frontier 2008) in several regions including N. Ossetia to practice assisting Russian peace keepers in Abkhazia and South Ossetia. (POL) Georgian Foreign Ministry protests.
15-31Jul	(PHY) USA and Georgia conduct military training exercises (called "Immediate Response 2008") at Vaziani Military base to improve combined capabilities and strengthen regional cooperation.
19-20 Jul	(CYB) Website of Georgian President becomes unavailable for more than 24 hours due to a multi-pronged DDoS attack. Website is temporarily moved to a US server
1Aug	(PHY) Clashes and shelling erupts between Georgian and Ossetian forces; worst violence for years.
3Aug	(POL) Russian Foreign Ministry warns that extensive military conflict is about to erupt.
5Aug	(POL) Russia vows to defend S. Ossetia. (CYB) OSInform (S. Ossetian news agency) website hacked and its content replaced by feed from a Georgian sympathetic news station.
07-08 Aug	(PHY) Georgia attempts to reconquer S. Ossetia through a large-scale military offensive. (PHY) following shelling of the Georgian peacekeeping checkpoint in Avnevi (14:00), Georgian forces are mobilized and personnel are withdrawn from JPKF HQ in Tskhinvali. Georgian peacekeeping troops begin to evacuate their posts in S. Ossetia. At about 19:00 Georgian President, advised earlier by his general in charge of peacekeepers, orders a unilateral ceasefire. Observed by both sides, it held until about 22:00.

	8th Aug (CYB) Main phase of cyber attacks against Georgian sites begins. Multiple C&C servers associated with Georgian Government are hit by co-ordinated attack against internet infrastructure. Georgian news portals (e.g. apsny.ge and News.ge) and non-Georgian news sites sympathetic to Georgia are hit together with online discussion forums. (PHY) Georgia launches offensive (called Operation Clear Field) in early morning with about 10,000 troops. Enter Tskhinvali by 08:00 and engage Ossetia militia in fierce battle. Russian artillery takes up positions in north of city and fire on Georgian forces. Russian Air force fly sorties against Georgian targets. (CYB) The Georgian government switches to hosting locations to the USA; the Ministry of Foreign Affairs opens a Blogspot account to disseminate information. Some commercial websites are also taken over. Prolonged attacks against websites of the Georgian President, and other government sites: the central government, the Ministry of Foreign Affairs and Ministry of Defence remain unavailable at least until 11 August. In all 54 sites associated with communications, finance, and government are attacked preventing citizens accessing information and instructions. (Hollis, 2011)
09Aug	(CYB) Early morning, largest commercial bank of Georgia comes under cyber attack (PHY) Russians move between 5,500 and 10,000 troops to S. Ossetia through the Roki Tunnel. (CYB) Official websites and news sites in Gori disabled by DDoS attacks. (PHY) Russia bomb and occupy Gori causing more than 56,000 to flee the city by 11 Aug (CYB) Tulip Systems Inc. (USA) offers help to the Georgian government and transfers the web sites of the President and of a prominent Georgian TV station to company servers in the USA.
10Aug	Turkish section of the Baku-Tbilisi-Ceyan oil pipeline attacked by local militants apparently on their own initiative (Unit, 2009)
09-10 Aug	(CYB) Ministry of Foreign Affairs was transferred to a Blogger account. And to a server located in Estonia (CYB) Office of the President of the Republic of Poland provided a section on their website for official press releases of the Georgian government. (POL/CYB) Two CERT-EE (Estonia) information security specialists to assist in mitigation efforts. (CYB) International IT security researchers find evidence of target lists, instructions, and downloadable DoS tools distributed over Russian web forums (CCDCOE, Nov 2008)

10Aug	(POL) International calls for peaceful solution and European Union and United States offer to send joint delegation to help negotiate a ceasefire. Russia rules out peace talks until Georgia withdraws from S. Ossetia and signs a legally binding pact renouncing use of force against S. Ossetia and Abkhazia (Wikipedia, 2013) (CYB) Attacks intensified and more information distributed on targets, including: Georgian government sites vulnerable to SQL injections (e.g. from forum: stopgeorgia.ru), instructions on how to ping flood, and distribution of public lists of email addresses of Georgian politicians for spamming and targeted attacks. Shadowserver reported new attacks against .ge sites. In this case, the IP address of C&C server involved was located in Turkey (Nazario & DiMino, 2008). (PHY) Group of Russian Warships arrive on Georgian maritime border.
11Aug	(CYB) Dancho Danchev (Danchev, 2008) reports that one of Georgia's most popular hacking forums has been down for 24 hours under permanent DDoS attack, in order to prevent Georgian hackers from exchanging information about cyber events.
11Aug	(CYB) Georgian news portal (civil.ge) comes under DDoS attack and is switched to a Blogger account. (PHY) Russian paratroopers carry out raids on Georgia military bases to prevent reinforcements being sent to S. Ossetia. Russian forces meeting virtually no resistance.
12 Aug	(POL) Russian President Medvedev orders end to military operation in Georgia, stating: "the operation has achieved its goal, security for peacekeepers and civilians has been restored. The aggressor was punished, suffering huge losses." (Kramer & Barry, 2008). EU President –in-Office (Sarkozy) facilitates six point plan that prevents further military action by Georgia in S. Ossetia and Abkhazia. (CYB) botnet attacks subside and attack model changed to a Microsoft Windows batch file that attacks Georgian websites distributed.
13Aug	(CYB) large-scale ICMP attacks on Georgian government websites from Russian computers. Also coordinated TCP SYN flood attacks, which are globally sourced, suggesting botnets. (PHY) Russian forces enter and clear Gori
15 Aug	(POL) Georgia signs six point peace plan
16 Aug	(POL) Russia signs peace plan, followed by Presidents of S. Ossetia and Abkhazia sign peace plan.
17Aug	(PHY) Some Russian troops withdrawn; about 3,700 remain.

26Aug	(POL) Russia is first UN member to de jure recognize independence of South Ossetia
27Aug	(CYB) Last large-scale cyber attack (HTTP requests) on Georgian government websites, mainly the Ministry of Foreign Affairs.
28Aug	(CYB) Cyber attacks diminish and are successfully blocked.
3Sept	(POL) Nicaragua recognizes independence of S. Ossetia
30Sept 2009	(POL) EU-sponsored report (EU, 2009) concludes that the war was started by a Georgian attack that was not justified by international law.

Manifestations of C2 Agility

C2 Approach Agility

The Russians demonstrated C2 approach agility by choosing a C2 that enabled co-ordination at the strategic level, but relied on Edge C2 for the specific cyber activities. As noted in the Estonia case study, Edge appears to be an effective strategy for cyber attacks that are mainly DDoS in type. There does not appear to have been a change in the C2 approach during the conflict.

The Georgians also adopted an appropriate C2 at the level of the cyber conflict; i.e. they used a collaborative approach, which seems necessary to act within a useful timeframe. However, the lack of co-ordination of the cyber countermeasures and analysis with the military conflict probably represents a missed opportunity. The C2 approach, at the strategic level does not appear to be sufficiently agile. Indeed, the outcome of the conflict, which was a resounding defeat for Georgia, suggests that amongst other factors, a failure to effect C2 approach agility may have contributed to the result of the conflict.

Agile behavior

The technical competence of the cyber experts demonstrated agile 'types of behavior' with respect to countermeasures, but ultimately the Georgian responders did not actually demonstrate agility. The main example of agile behavior was the speed with which external organizations acted to provide hosts for important Georgian websites. These organizations also provided appropriate technical capabilities to enable rapid transfer of information to their sites.

Observable Enablers and inhibitors of C2 agility

The six enablers and inhibitors of C2 agility are: responsiveness, versatility, flexibility, resilience, innovativeness, and adaptiveness. These are listed in table 1 to determine which enablers and inhibitors of C2 agility were observable.

Enablers/Inhibitors	Georgian perspective	Russian perspective
Responsiveness	Yes	Yes
Versatility		
Flexibility		Yes
Resilience		
Innovativeness		Yes
Adaptiveness	Yes	Yes

The Georgians were able to react to the attacks through recruitment of international experts to mitigate the cyber attacks and the concomitant C2 within the cyber situation indicated adaptiveness (e.g. the shift of CERT Georgia from work with educational institutions to be the national co-ordinator).

The Russians responded to the Georgian attack with rapid deployment of cyber attackers; the preparatory attacks to gain intelligence demonstrated innovativeness, as did the forms of the attack and their applicability to the purposes of propaganda and information blockading. The co-ordination between the cyber attacks and the military operations indicate both adaptiveness and flexibility.

Relevant C2 Approaches

The relevant C2 for the attackers seems to have been adopted; i.e. co-ordination at the strategic level and Edge at the cyber-attack level.

For the defenders, the appropriate C2 is suggested to be co-ordination at the strategic level and collaboration at the cyber level. In fact, the Georgians only achieved one of these appropriate types.

Case study assumptions and limitations

The case study information has been drawn from publically available publications and there has been no explicit checking of the validity of the deductions about C2 from this information. It should also be noted that the types of attack were essentially DDoS and website defacement, neither of which cause long-term damage (although the intrusion may have been used subsequently by criminal participants). The conclusions about C2 approach must, therefore, be viewed as applicable to these types of attack only, and not to cyber-attacks in general.

Conclusions

(Hollis, 2011) has drawn a number of conclusions about the role of cyber in small conflicts; in particular, he has indicated that for a nation to engage in the time-sensitive cyberspace warfare environment it must prepare well to achieve the capabilities of "trained human capital supported by doctrine, organization, command and control (C2), and technology." Essentially, this is summarized by the straightforward statement that agility in conflict where cyber is involved requires strenuous and continuous preparation. Cyber is clearly a manifestation of a facet of warfare concerned with information superiority. Cyber attacks are, in essence, no different from any other operations to impact intelligence, but the methods used to achieve these impacts are different. In particular, the use of a variety of attackers ranging from bona fide experts to criminal gangs is an effective strategy for DDoS type attacks, requiring the distribution of information about how and where to attack, but using an Edge C2 approach for delivery of the effect.

The ideal C2 for attacking appears to be co-ordination at the collective level, but edge at the cyber-attack level (for DDoS types of attack). For defence, it is clear that co-ordinated C2 is most appropriate at the collective level, but collaborative C2 is required at the technical cyber level.

Works Cited

CCDCOE, Nov 2008. *Cyber Attacks against Georgia: Legal Lessons Identified,* Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence.

Danchev, D., 2008. *ZDNet.* [Online]
Available at: http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670
[Accessed 29 Aug 2013].
EU, 2009. *Independent International Fact-Finding Mission on Conflict in Georgia, Report Vol 1.,* s.l.: European Union.
Hollis, D., 2011. Cyberwar Case Study: Georgia 2008. *Small Wars Journal*, 6 Jan.
Kramer, A. & Barry, E., 2008. *Russia, in Accord With Georgians, Sets Withdrawal.* s.l.:New York Times.
Markoff, J., 2008. Before the Gunfire, Cyberattacks. *New York Times*, 12 Aug.
Nazario, J. & DiMino, A. M., 2008. *An In-Depth Look at the Georgia-Russia Cyber Conflict 2008,* s.l.: Shadowserver.
Shachtman, N., 2009. *Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It,* s.l.: Wired.
Unit, U. S. C. C., 2009. *Overview by the US-CCU of the Cyber Campaign against Georgia in August 2008,* s.l.: s.n.
Wikipedia, 2013. *Timeline of the Russia–Georgia war.* [Online]
Available at: http://en.wikipedia.org/wiki/Timeline_of_the_Russia%E2%80%93Georgia_war
[Accessed 29 Aug 2013].

B.4 Garda Earthquake Case Study

Executive Summary

This case study illustrates the Italian Civil Protection's response to the Garda Earthquake in 2004 and highlights some organizational and cultural changes that had taken place previous to the emergency, and that seem to have been crucial for the manner in which the emergency was handled. After responding to the emergency in an almost self-synchronized way, with components activating autonomously, the organization takes more and more the shape of an organism, with a mixed operations center encompassing representatives of all components. The more the situation stabilizes, the more the collective's shape changes (components traditionally involved with first response leave their place to those more concerned with reconstruction, such as engineers, architects, technicians, and so forth) and shifts from Collaborative to Coordinated, and responsibility is laid more within the Local components (province).

The Organization

The Italian Civil Protection is a collective that aggregates a broad number of organizations. It is not a Corps like the Civil Defence; this is the result of a choice made in 1992 to change the face of the organization and highlight its active function and role. The focus on the word "Protection" is thought for a more proactive attitude than "Defence" (seen as passive response to events). The organization, as it is today, is the result of the changes brought about by the law 225/92 that defines all functions and roles within the organization. One of the results of this law is that the core of the Civil Protection lays in the coordination of a multitude of competences, as opposed to having professionals available around the clock.

It is also very important to highlight that the tasks of Civil Protection are not only relative to providing Emergency Response, but they are also (and perhaps even more) focused on Prevention, Forecasting, and Reconstruction (as explained in Art. 3 225/92).

The Components of the organization are described in Art. 6 of the above mentioned law:

- Firefighters, as the main component
- Armed Forces
- Police
- Rangers

- National Technical services
- National Research groups, including the National Institute of Geophysics
- Red Cross
- Health structures on the territory
- Volunteers and National Corps of Alpine Rescue Institutions
- Groups of Scientific Research and Private Organizations
- Citizens and Voluntary Groups
- Professional Categories (Architects, Engineers, Experts of Geology, etc.)

- Technical national services (authority of rivers, regulation of lakes, etc)

What components are activated and according to what structure depends on the nature of the event (A, B or C) and is determined in the law 225/92.

A Modular Force

An organization based on a "modular" force was chosen; a Corps was considered as too large an organization in case of micro emergencies whereas it would be too little in the face of considerable crisis. A modular approach, on the other hand, allows the organization to be scalable based on the specific situation it faces. As will be illustrated in the next paragraph, the organization works on different layers: National and Local. The National Civil Protection can be mobilized if needed to support major events and catastrophes with full force and all material resources (as it was the case after the Tsunami in 2004 when the fleet and other resources from the national pool have been employed), while for smaller events or need for specific competencies, response can be tailored at a more local level.

Chain of Command

National Level: the Situation Room is the institutional level where political decisions are made and the Crisis Unit (Unità di Crisi) is the operational C2 center, where decisions are executed. Both are located at the Department of Civil Protection in Rome, which is an independent Department within the Government and lies directly under the Prime Minister. This allows considerable speed in decision-making.

Local Level (in each region and province): Rescue Coordination Center (Centro Coordinamento Soccorsi) is the institutional level where political decisions are made (where to place tents, what sort of urbanistic responsibility is to be given to the mayors, etc) and the Operational Room (Sala Operativa) is where decisions are executed.

Before 1992 the Civil Protection was a Corps and was called Civil Defence. The Armed Forces played a very central role in the organization. In the face of several emergencies during the 70s and 80s it became clear that stove-piped efforts and individual attempts to deal with emergencies would not help: what was needed was a joint effort. Particularly after the Friuli earthquake the engagement of the civilian population emerged as the very crucial factor for the success of the operation. This is why it is now clear to everybody that the Volunteers are the most crucial among Civil Protection components.

Since 1992 the law 225 defines the structure and components of the Civil Protection, and mandates to all Governors to define regional laws.
According to the national law, each Civil Protection, at the National and Local Levels (all the way down to single municipality) shall define:

- Plan of Forecast and Prevention of Risks through a scientific study of the territory
- Emergency plan, which is a theoretic model of intervention that is then adapted to the specific contingency. So, for instance, an emergency plan would locate suitable locations where to place tents, aid, and such broad, yet crucial, guidelines, but it would not include how the organization would act in case of emergency. How to act is something that cannot be decided in advance, as it is very highly contingency dependent.

Since 2002, the National Civil Protection lies directly under the authority of the Prime Minister; this has been decided to allow the Chief of the Civil Protection to have a cross cutting authority over all components.

a. Focus and Boundaries of the Case Study

This case study looks at the intervention of the Italian Civil Protection after the Garda earthquake, province of Brescia, in 2004. The leadership of the Brescia chapter of the Civil Protection had, at that time, just led a major reorganization (which began in 2000) driven by the intention of generating more flexibility and cohesiveness. The main tenets of this reorganization are also described. The case study does focus on the Collective, not having the time or resources to conduct a deeper investigation at the component level.

b. Challenge or Opportunity for C2 Agility

As is often the case with natural disasters, response can be planned and prepared only to some extent, due to the unpredictability of events. A number of challenges were met:

- Geography and demographics of the area,
- Worsened by the impossibility to communicate through the usual radio channels used by the Civil Protection,
- Tsunami in Thailand one month later, which caused a diversion of major Civil Protection resources.

c. Was Agility Manifested? If so, How?

Yes, agility was manifested

1. By having a self-synchronized action at the peak of the emergency. Without any coordination several units self-activated and self-managed in the field.
2. By shifting, while the situation changed and the acute emergency phase faded, towards a more Collaborative structure, then turning into Coordinated when the circumstances allowed.

d. Enablers and Inhibitors of C2 Agility

Enablers:

- Strong organizational culture (strengthened by the 'being a system' philosophy, which involved also local population),
- Extended network thanks to the 'double identity' campaign for recruitment of volunteers,
- Broad and rich pool of competences among volunteers, thanks to the 'double identity' campaign,
- Cohesiveness,
- Capability (due to competence level) and Possibility (due to organizational practice) to make decisions and take initiative at the tactical level (Mission Command)

Inhibitors:

- Situational determinants
- Strong organizational sub-cultures
- External factors (Tsunami in Thailand)

e. Summary of Observations/Conclusions about C2 Approach Agility

Garda Lake Earthquake took place 24 November, 2004, with epicenter in the town of Saló in the province of Brescia, Italy. The collective studied in this case study is the Italian Civil Protection: built

according to a 'modular force' model, this organization is an aggregate of virtually every organization that would respond to a civil emergency including individual citizens and voluntary groups. The local Brescia Province's leadership of the Civil Protection between 2000 and 2009[1] developed the model illustrated in this case study, known among members of the organization as 'Brescia Model'.

Core Concepts

The structural reorganization took place in parallel with major cultural changes, some of them illustrated below:

Double Identity

The notion of "Double Identity", developed for the recruitment of volunteers, was one of the strongest concepts driving the model: everyone can, and is encouraged to, be a member of Civil Protection. Each member, whether a banker, a student or a housewife, identifies with the collective in a way similar to: 'once a Marine, always a Marine'. This strong sense of belonging creates the basis for collaboration and cohesion also among people who meet on duty for the first time while providing the collective with a broad and rich pool of competences and skills. Members literally span from students to bankers and bring a very multidimensional network to the organization.

All members of the Civil Protection take part in local exercises arranged every two-three weeks, as well as in regional exercises every quarter and a large national exercise yearly.

Being a System

One of the principles that drove the reorganization of the Civil Protection in the Brescia Province has been the idea that every citizen must be made aware and responsible of her surroundings and sphere of action. The idea is that each person shall take charge and feel responsible of own security instead of solely relying on external entities. Following this principle, campaigns for the prevention of risks have not been formulated with a language that communicates intrinsic security. The message is never "if you do this you will be safe" because being safe does not depend on following rules, rather it depends on developing the sensitivity to feel and read the environment around you. The so-called Perception of Risk. This is a campaign that stems from the observation that, particularly influenced by video games, people tend to think that they can change the environment, while the point is that the environment has

[1] This case study is referred to the organization as it was organized in the years 2000-2009 in the Province of Brescia. What is illustrated here shall not be inferred as valid to describe the collective after 2009, as major leadership change took place.

its own life and what we need to do to be safe is to learn how to read it. This led to a series of initiatives aimed at stimulating an active role in the people, some of which are illustrated below:

- Distribution of DVDs with courses of self-protection and risk perception to all primary and secondary schools' students. However, it was chosen *not* to send DVDs directly to the schools, but to provide each pupil with a voucher that they had to send in order to receive the DVD at home. In this way the pupil is not a passive recipient of information, but an active decision maker that requires the DVD and watches it at home with his family, with consequent spill over of the educational effects to the whole family
- All schools must carry out compulsory exercises
- Campaign for risk perception on the mountains during summer and winter (the province is categorized as having high avalanche risk)

Support to the volunteer groups. The province counts 200 volunteer groups with around 10.000 active members.

Plans as learning tools

The province of Brescia, the third largest province in Italy comprehends 1.247.192 inhabitants with a density of 260, 61 inhabitants/ km^2 on an area of 4.785,62 km^2 with 206 municipalities. Each municipality must develop a Forecast, Prevention, and Emergency Plan. This means that each municipality must conduct a study of its territory, risks and situation, develop plans and exercise upon them.

Plans include, among others:

- Dams

- Industry with relevant risks (tanneries, oil refineries, and so forth). In case of industrial or military secret the plan is developed by the province but handled by the Prefecture under the Department of Homeland Security (Ministry of Internal Affairs)

- Sensitive plans, not only relative to sensitive industries but also specific religious sites, train stations, potential terrorist targets

Each area is assessed and evaluated, and contingency plans are developed. The Province runs risk assessments of all possible threats. Each municipality must develop risk analysis and assessment for all its territory and emergency plan(s). The Emergency plan(s) for the Province of BS comprehends more than 300 tables and 50 scenarios. However, how much is it used in case of real emergency? In fact, ***the plan must be developed to make people aware of the situation, potential risks, and to make them keep***

always an eye open. It helps to identify areas where to gather people, what roads to use and so forth, but in reality, ***it is not used as an operational tool to define how to behave***, but rather a tool to increase the level of awareness, self-responsibility, and vigilance. The ***plan is more a learning tool than an operational tool***. It gets updated during and after each exercise, and also after real life episodes. After this particular earthquake, there has been a commission that has updated the plan based on the Lessons Learned during the emergency. There are some analysis and reports, but most Lessons Learned can be seen in the changes made to the plan.

f. Important stories or vignettes in the case study.

Vignette I: November 24th2004, Peak of the Emergency

- 23:59 Earth tremor, 5.3 Richter scale, no fore-warnings.

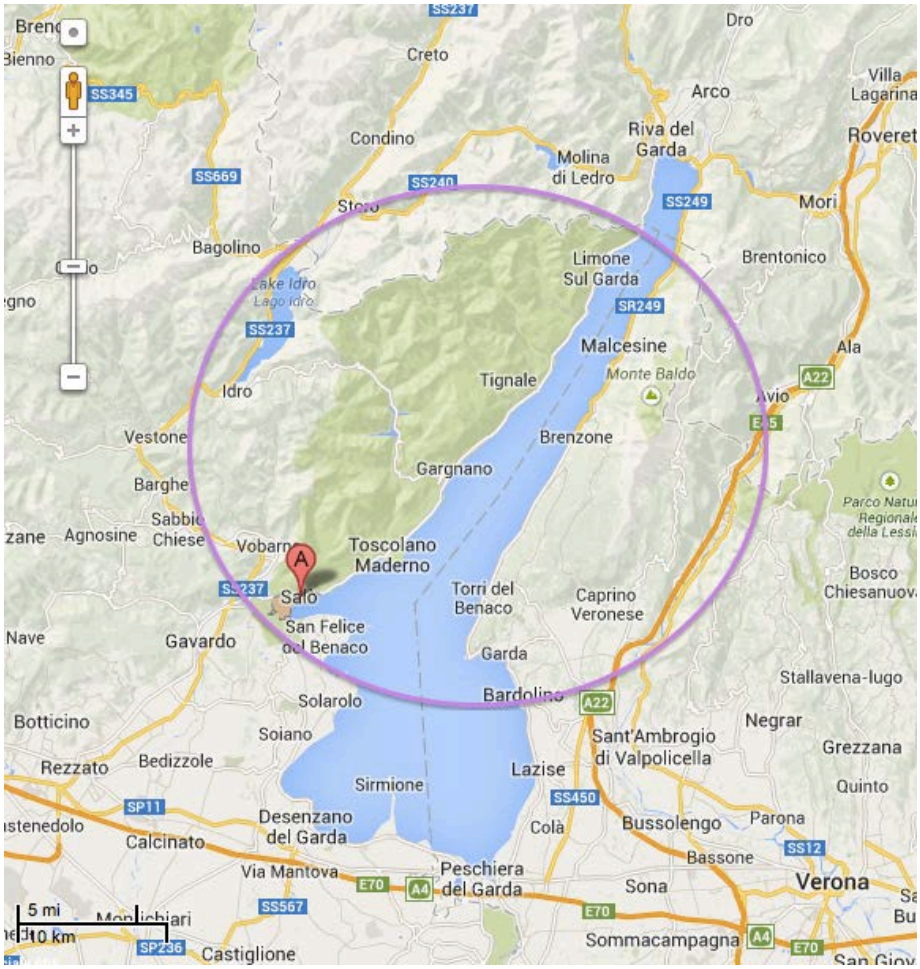


Figure B.4.1: area of Influence of the Earthquake with epicentre in the town of Salo'. Vobarno, Malcesine,Tignale, Limone sul Garda were also heavily damaged. Note the territorial characteristics.

- The tremor is felt in Turin, Genoa and, East, in the region of Veneto

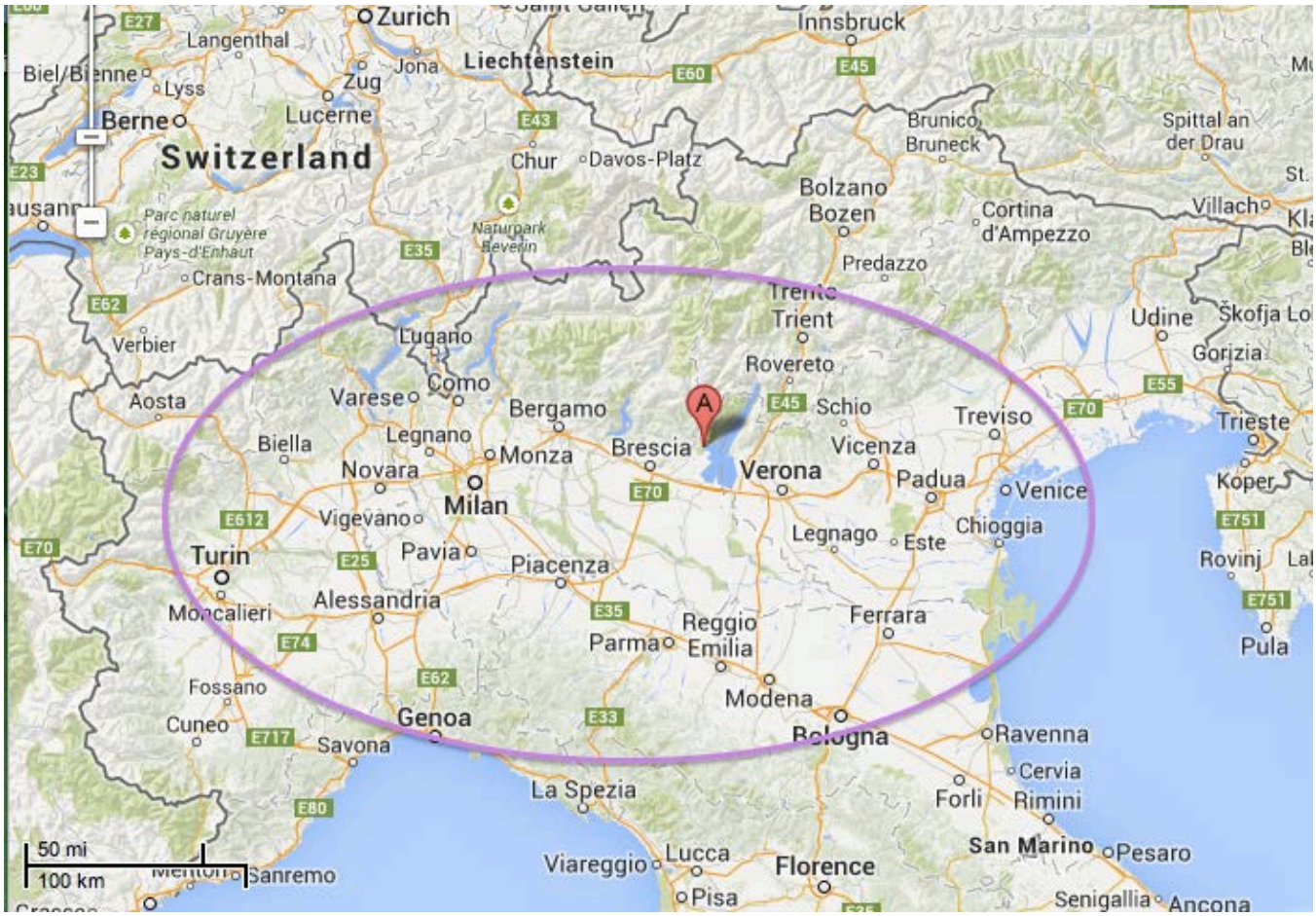


Figure B.4.2: Area where the earthquake was perceived.

- The Garda Volunteers activate immediately
- Some minutes later, the National Institute of Geo-Physics divulgates a message about a tremor registered in the Garda area.
- The Chief of the Province Civil Protection receives a call while entering his home after a meeting. His family has felt the tremor and he leaves to go back to the Civil Protection local HQs in Brescia (about one hour by car).

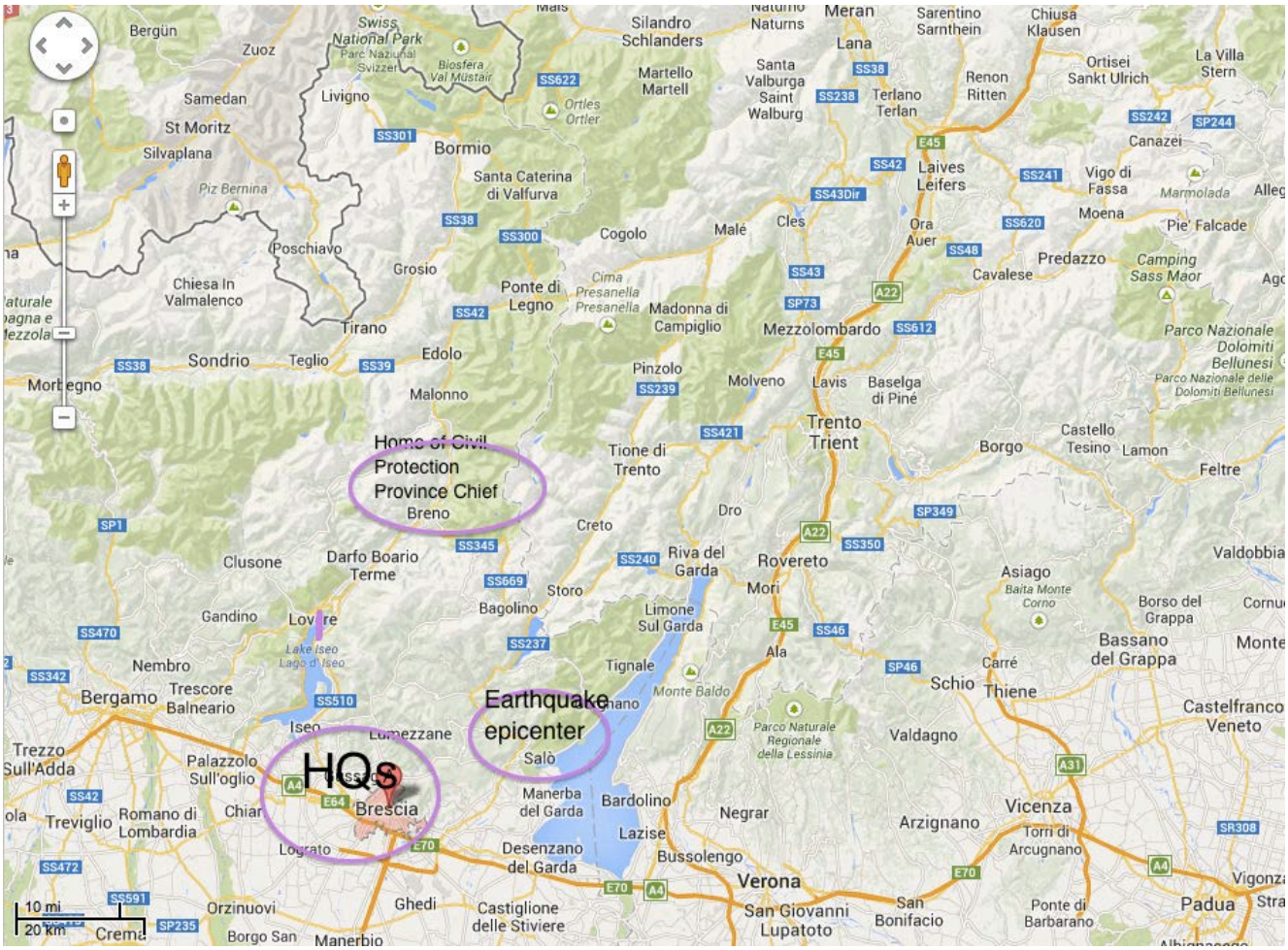


Figure B.4.3: Distances between Epicenter, Civil Protection HQs, and Local Chief's home.

- The Operation Room is already activated: it got activated upon the fire-fighters feeling the tremor; they then contacted the police, carabineers, 118, etc. In this way the operation room activates spontaneously, nobody waits for a formal order.
- After some minutes everybody is in the Prefecture of Brescia where the Centre for Rescue Coordination has been opened (the Decision Making organism). The operation rooms of all components are all active.
- At this point each component follows its own competence and they all work in parallel focused on their specific typical tasks (fire-fighters, 118, police, and so forth). At this point they are not coordinated from the top, they automatically do what they usually do (118 takes care of wounded, fire-fighters and carabineers look for people) and they spontaneously coordinate with each other on the ground. Everybody moves and faces the emergency within their core competences.

- The ones that are physically closer to the event are the ones that activate first and then they proceed as an onion: local fire-fighters get in touch with the ones in neighboring municipalities and so on, almost based upon word of mouth, until they reach the command center in Brescia.
- Brescia starts then to communicate with others. Each component does this in parallel (fire-fighters, police, 118, etc).
- The mechanism that gets activated here seems rather irregular in the first minutes, because at that point nobody has a Common Operational Picture. Meantime, media start covering the news and divulgating the first numbers.
- In the Centre of Rescue Coordination a Desk is activated for each component; it's an information node, as each desk gathers information from its people on the ground and a Common picture is built piece after piece, completely Bottom Up.
- All this information is placed on a map and the geographical area is delineated: Salò, other villages, some place in a neighboring valley
- Then the people in the Centre of Rescue Coordination start actively to cross check the information at 360 degree contacting mayors and parish priests.
- The volunteers' net is paramount because it acts as multiplier of all the potential information sources, thanks to the private network each volunteer can rely upon.
- In a few hours it is possible to come to a common picture of the event.
- In parallel, the National Civil Protection has received the information that the event is not manageable with local resources solely and is making available its fleet and columns (the fleet is an asset of the National Civil Protection and so is the column + some extra vehicle that belong to diverse components).

Vignette II

November 25th

- At 6 am, Nov 25th, the chief of the National Civil Protection arrives at the site and receives a brief (10 min) and then leaves for a helicopter visit of the area, with stop in 4 or 5 places (tot. two hours).

9 am: Decision is made to open the Unified Operational Room (Like our JOC?) at Salo inside a high school. The intervention of the National PC here becomes paramount:

- They provide the technicians and engineers that examine the building
- All the national technical services are called to support the national PC, hence in about two hours electricity is assured in the area, so are the telephone lines, water, etc.

- This is all handled top down through the national PC: making it possible for the local task forces to do their job in the best conditions possible.
- **The Mixed Operational Center is opened:** it is a collaboration center that gathers representatives of all components.
- During November 25th the gym of the local high school is fixed with 20 desks, each desk has an operator.
- Command over these desks goes to a man designated by the National Chief and the vice prefect is responsible of administration (all necessary paper work, orders to evacuate or to go back to certain buildings, etc). This is the so-called COM (Centro Operativo Misto): Mixed Operational Center.
- The COM follows the functions and procedures described in its Founding Ordinance (Decreto di istituzione), which is made ***ad hoc*** by the prefect. In this document it is defined who does what.
- In this specific case, the Founding Ordinance of the COM states that the Province is in charge of all relations with media and all communication, connections with volunteers and all logistics to support the work of the COM.

In parallel, relief to the population must be provided through:

- Institution of centers to gather information from the population
- Search for places where the population can be accommodated.

Together with the representatives of the Regional Civil Protection a decision is made NOT to build temporary accommodations. Looking back, it turned out to be a good decision; however, at the time it was made, it involved taking a risk.

- The choice falls upon engaging the numerous hotels of the area (Garda). This decision is motivated by:
    - More immediate comfort for the population
    - A will to involve all the locals in a more rapid reconstruction: having local people in the hotels, in an area that heavily depends on tourism, would affect the economy of the region. Hence, a good incentive for everybody (including politicians and other stakeholders) to make sure that homes are rebuilt as soon as possible.
- The National Chief promulgates an ordinance (he is the only one in the organization with the mandate of signing an ordinance that has economic bearing) and makes sure that the hotels get compensation. This decision was taken with the purpose of making everybody 'own the problem'.

- Night between November 25th and November 26th: most of the time is spent trying to intercept the several rescue crews that had left from all parts of the nation. These need to be selected and some must be sent back.
- Some of the disaster relief work turns out to be dedicated to arranging the myriads of people who want to be helpful.

During the first response phase all components activate immediately within their competences, in a sort of self-synchronization. After that each component is assigned a role. i.e. fire-fighters where in charge of cleaning all roofs and secure buildings, and so forth.

In the COM (Mixed Operations Center) there is a representation of ALL components (small teams) and also the relevant organisms for the area; in this case there were also Caritas, parishes (the parishes' net has proven fundamental in this particular emergency), groups of psychological support, and so forth. It will be better described in Vignette IV

Vignette III

Following Days

The so-called "Community Areas" are created: big tents with heat where people can gather to talk, as they would do in a square or bar. Also some churches (or tents that worked as churches) are reactivated (this was responsibility of the Scouts).

- Efforts are made to establish and maintain contact with the population. i.e. in Pompeino, a small village rather isolated, people were very angry and claimed that they were forgotten. In fact, they were not, as many firefighters and engineers were already working there. However, talking to people it emerged that they felt forgotten because media and TV had not visited them. So, a detached branch of the COM was open there and directed by a representative from Rome: everybody felt happy and nurtured.

- The days following the quake are mostly spent making an estimate of the damages, an evaluation done by Engineers, Architects, and Technicians that came after an appeal at the respective Professional Organizations.

- This engagement led to the fact that in a few days many people could return to their homes that had been declared secure.

- Ordnances are emitted for those buildings that are not “runnable” and an estimate of the damages is completed (about 80 million Euros).

Vignette IV

The Mixed Operations Center as a Collaboration Hub

Information sharing is another critical point: a team representing each component is present in the COM (Chief, administrator, secretary, operator, technician, etc) and they talk to each other, it’s the so-called active communication: everybody collaborates and talks directly to the representative of each component in the COM. Each component has its own communication net with its people downwards and upwards (i.e. police uses its own radio channels, Armed Forces, 118, volunteers, Red Cross etc), but the representatives in the COM talk with each other so it becomes a sort of information and coordination node. Further, components in the field also communicate directly with each other. In the COM there are also representations of all service providers (electricity, Telecom, etc). It is a complex structure that has all the power and mandate to handle the emergency. There is a daily operational brief, no more.

In parallel the Centre for Rescue Coordination is always active in the prefecture: if there are communication problems within the COM, the issue is moved to the CRC.

The functionaries from the National Department of PC staid around one month, in an operational function. The National Chief got back once a week as operational controller; he got a brief as follows:

- Sit update from each component in the COM
- Meetings with all mayors
- Visits out in the territory

The Mixed Operations Center was closed about one month after the emergency.

Identify the Focus of and the Boundaries for the Case Study

e. What is the level of analysis? (e.g. Individual, Team, Organization, or Collective)
Collective.

f. Who or What Organizations are included in the case study?

All components of the collective:

Firefighters (main component), Armed Forces, Police, Rangers, National Technical services, National Research groups, including the National Institute of Geophysics, Red Cross, Health structures on the territory, Volunteers and National Corps of Alpine Rescue Institutions, Groups of Scientific Research and Private Organisations, Citizens and Voluntary Groups, Professional Categories (Architects, Engineers, Experts of Geology, etc.), Technical national services (authority of rivers, regulation of lakes, etc)

What temporal boundaries are included?

a. When does the case begin and end?

It begins on November 24th 2004 and ends in November 2005, but it is mostly focused on the first three months.

b. Are there phases involved? If so, what are their boundaries?

This case study can be divided into three phases:

Phase 1: Peak of the Emergency

Phase 2: Following Days into Stabilization

Phase 3: Stabilization and Reconstruction

Phase 1: Peak of the Emergency

The Peak of the Emergency phase took place immediately after the quake and within the first twenty-four hours was over. Within these twenty-four hours, self-synchronization has been the main feature, particularly in the very first hours, and shifted gradually more and more towards collaboration as information was gathered and a Common Operational Picture started to take shape. The Mixed Operations Center also was set up nine hours after the earthquake.

Phase 2: Following Days and into Stabilization

A common Operational Picture is gathered from a few hours after the emergency, the Mixed Operational Center becomes the collaboration hub. Search and Rescue leaves place to stabilization: all buildings are checked within a few weeks. A decision is taken not to build temporary homes, but to move the people in need into local hotels in order to: 1. Support the local economy, which depends heavily on tourism and has been damaged with the earthquake, and 2. Encourage and inspire local population to engage in the reconstruction of their homes as soon as possible.

Phase one and two are illustrated in the Vignettes above, as they are the episodes where most clearly we can see the shifts in C2 approach along with shifts in the situation.

All institutional components are involved, from municipality level to National (Government). The emergency phase lasts until all buildings are declared secure, about 2 to 3 months, but starts earlier to shift into Stabilization.

Phase 3: from Stabilization and Reconstruction

The Emergency phase gradually shifts into Stabilization and Reconstruction. There are no clearly established boundaries that define such phases, and they take place almost in parallel.

The priority is given to houses: there are around 2500 families without a home. It is chosen to adopt a mechanism of diversified aid based on paying the first homes first, and then take care of others (second homes, vacation homes, and so forth). Next is cultural patrimony, which is a more delicate and expensive job.

Public Administration has been kept outside the reconstruction, on purpose: private families must participate in the design and can suggest an enterprise; the Public Administration finances upon approval. The management of funds is left to the Region, with a specific commissary for all decisions taken in a coordination office. While getting deeper into stabilization and reconstruction, the control shifts towards the local municipalities.

In the beginning of Nov 2005 (less than one year later) the situation was declared closed and all people had returned to their homes.

g. Other boundaries (e.g. separate analyses of the collective and of specific organizations within the collective).

Describe the Challenge or Opportunity that gave rise to the need for C2 Agility.

The need for C2 Agility arose from different factors:

- The nature of the emergency: an earthquake cannot be predicted and requires, hence, immediate and proper response as soon at it happens
- Different phases pose different requirements, approaching all of them through the same C2 approach would be ineffective or lead to a waste of resources
- The fragmented nature of the territory
- The Tsunami one month later diverted major resources

What would have been the consequences of a failure to act in a way that demonstrates C2 Agility?

- More casualties

- Longer time needed to establish a common operational picture
- Slower and less effective search and rescue activity (for example, the impossibility to communicate through official unified radio channels was countered by switching to local volunteers radio frequencies)
- Vacuum effect when the national resources have been diverted to the Tsunami emergency
- Economic losses due to the relevant weight of tourism on local economy (avoided by using touristic structures to host the people who had lost their homes)
- Longer time to rebuild the buildings that had been destroyed (by empowering the population in the reconstruction the process got speeded up)

Was C2 Agility Manifested? If so, how? (Be as clear and precise as possible, but keep this simple so that it does not require repetition in the next steps.)

Yes because the C2 approach varied along with the shift in the environment. At the highest level of emergency Edge C2 was witnessed, with each component self-activating, yet acting in a synchronized manner without formal coordination. This shifted towards Collaborative as soon as the peak of the emergency was over and a common operational picture was gathered. The Mixed Operations Center functioned as a hub to coordinate efforts, yet allocation of decision rights was very distributed and a high level of Mission Command enacted. This further shifted towards Coordinated into Phase 3, when the main focus was reconstruction.

Which Enablers and Inhibitors of C2 Agility were observable? (Remember that the basic six may not be independent. Include discussions of the relevant Agile Behaviors, but try to tie them to one or more Enablers. Specify inhibitors that impacted C2 Agility)

g. <u>This will be illustrated below with reference to the different phases (the emergency phase is here sub-divided into first hours, peak of emergency, and following two days), as well as the different C2 approaches that have been employed</u>

Phase 1: Peak of the Emergency

- Challenges:
  - No Situational Awareness,
  - No Common Operational picture
  - Chaos
- Action: each component of CP spontaneously activates after the first tremor, before the official emergency is declared
- Agility Properties Observed:
  - **Responsiveness**: volunteers and other components activate before the emergency is officially declared

- **Versatility**: Lines of communication are down, they switch to local volunteer groups' radio, they self coordinate in the field, as there is no official radio channel that is reserved for the Civil Protection
- **Resilience**: search for alternative ways to gather information for the establishment of a common operational picture (COP) as soon as possible by using alternative radio frequencies, talking with people, recurring to personal network, and involving parishes.

- **C2 observed: Edge**
  - ADR: Distributed Allocation of Decision Rights:
    - Very broad: Each component activates autonomously and they establish connections to each other
  - PI: Patterns of Interaction:
    - Informal,
    - Cross cutting,
    - And basically unconstrained. High level of interaction and information exchange, mostly of informal nature
  - DI: Distribution of Information:
    - Ongoing and gets broader while each small tactical team gathers information and shares it with the Operational Room where all these small pieces of the puzzle are gathered into a larger Common Operational Picture

Phase 2: Following days up to end of Emergency Phase

Challenges:

- Provide an efficient emergency response service. People are very upset and need to feel that they are taken care of.
- Provide shelter to 2500 families

- Action taken:
  - Establishment of a Coordination Room (Mixed Operations Center) with representatives from each sub-component,
  - Coordination Room acts according to ***ad hoc*** procedures, established by the prefect

- Component's representatives communicate vertically with own people in the field, who also interact with other components' personnel tactically
- Set up tents and Info points
- National Chief of Civil Protection visits the area and spend time with components' personnel and local population
- National Civil Protection acts as enabler to the local Civil Protection by providing technicians from the National Service and some aircraft from the fleet (National Pool).
- Choice not to build temporary homes, but to use local touristic resources instead in order to:
    - Support the local economy, as the touristic season got damaged by the earthquake
    - Provide an incentive for people to engage in reconstruction of their homes as soon as possible

This phase can be characterized as a phase of organizational transition where the CP goes from the self synchronized first response towards setting up its structure for operations: Collaborative according to SAS085 model.

- Agility Properties Observed:
    - **Responsiveness**: immediate response to perceived dissatisfaction in population of areas who felt forgotten
    - **Innovativeness and Adaptiveness**: Choice not to build temporary homes, but to use local hotels instead, this is an innovation in relation to the common practice up to that time (of using pre-fabricated shelters) and shows adaptiveness in the sense that it exploits a local resource (hotels, tourism) to provide immediate accommodation to the victims while, at the same time, a motivation to reconstruct the area as soon as possible to avoid damaging the touristic season.
    - **Innovativeness**: finding ad hoc solutions (send TV)
    - **Flexibility**: Ad Hoc procedures for the Situation Room

- C2 observed: **Collaborative**

    - ADR:
        - Rather Broad Allocation of Decision Rights in the field, but less than in the previous phase, since the Mixed Operational Centre is activated. Representatives of the National Civil Protection are always present as enablers.
    - PI:
        - Patterns of Interaction are high, formal and informal, although formally coordinated through the Mixed Coordination Center Situation Room that acts as node among representatives from each component. Representatives coordinate in the Room, and then communicate with own people in the field, who also interact with other components tactically.
    - DI:
        - Distribution of information among components is on-going and takes place vertically within each component's own channels from the Mixed Operational Center Situation Room to the field (and vice versa), and horizontally in the field among members form different components, and in the Situation Room among members from different components.

Phase 3: Stabilization into Reconstruction

During this phase the organization shifts from fully collaborative C2 and slowly into coordinated.

- Challenges:
    - To return to normal activities as soon as possible,
    - Design quick and efficient reconstruction processes
    - To provide homes for all the 2500 families that are without one
    - Tsunami in Thailand hits after one month: shift of attention to that region and resources from National CP
- Action taken:
    - Engage locals in the reconstruction as much as possible
    - Pull out the Public Administration from reconstruction work and instead put each family in charge of designing project and choose entrepreneur
    - Gradually shift control of the situation to the local municipalities

- Agility Properties Observed:
    - **Versatility**: Pull out the Public Administration from reconstruction and put families in charge of own homes
    - **Resilience and Adaptiveness**: After the Tsunami in Thailand, the attention of public opinion and of resources sent as support from the National Civil Protection shift to support the new larger operation. In spite of this, stabilization and reconstruction proceed (resilience) and a decision is made to speed up the process to put in charge local authorities: the Region is still in charge of funding, and the operational role of the Province gradually shifts over to local municipalities (adaptiveness).

    - C2 observed: shifting from **Collaborative towards Coordinated**

    - ADR:
        - More centralized Allocation of Decision Rights, no need to have it as distributed in the field as before, although through the Mixed Operational Center (which is closed two months after the earthquake). Furthermore, although there is still sharing of decision-making and responsibility among Region, Province, and Municipality, the latter is increasingly put in charge.
    - PI:
        - Patterns of Interaction are more regular and less intense
    - DI:
        - Distribution of Information more structured

What C2 Approaches were being used? (How can C2 Approach Agility be inferred from what was reported or observed?) Did C2 Approach change, either for a collective, organization, team or one or more individuals?

See above

Case Study Evidence Table – Civil Protection Garda Earthquake – Collective Level

Component/Concept	**Phase 1**	**Phase 2**	**Phase 3**
C2 Approach Space			
Situation Complexity (high, med, low?)	High	Medium	Low
Appropriate (Required) approach			
Allocation of Decision Rights (none to broad)	Broad	Broad	Limited
Distribution of Information (none to broad)	Broad	Broad	Broad
Patterns of Interaction (tightly constrained to unconstrained)	Unconstrained	From Unconstrained to Structured	Structured
Actual approach	Edge	Collaborative	Collaborative/Coordinated
Agility Components (low, med, high?) (State evidence for Agility as well as lack of agility)	?	?	?
Flexibility (inflexibility)		Evidence found	
Adaptiveness (lack of adaptiveness)			Evidence found
Responsiveness (unresponsive)	Evidence found	Evidence found	
Versatility (Robustness) (lack of versatility)	Evidence found		
Innovativeness (lack of innovativeness)	Evidence found	Evidence found	Evidence found
Resilience (lack of resilience)	Evidence found		Evidence found
Self-Monitoring (we're not sure if self-monitoring is part of the original model or not).	Not consciously	Not consciously	Not consciously

Key Findings

- Variety among members of the Civil Protection proved to be a Critical Success Factor. The reorganization brought about in 1992 and aimed at rendering the Civil Protection an 'umbrella' organization which includes various components generated variety. ***Variety*** was then maximized with the double identity recruitment campaign.

- More Relevant than personal relationships is the ***strong Organisational Culture***: it glues together also people who do not know each other and build a sense of ***belonging, identity***, and ***pride***.

- The creed "Being a ***System***" seems to have worked as very powerful narrative and provided a solid foundation.

- Campaign "Do you want a ***Double Identity*** *?" turned out to be crucial because people used their own network to access resources and information when needed. It acted as* ***Force Multiplier***

- *Distributed Collaborations*

- The plan is a ***Learning Tool,*** *not used during the Operation.*

- ***Cohesiveness*** based on personal relationships and collaboration is the major strength of the organization and enables Mission Command. Trust cannot be commented upon so far, as it would require further and deeper inquiry.
- Strong role of a charismatic & respected **leader** as a point of reference and source of cohesion. NOTE that the interviewees refer to the National Chief as the charismatic and respected leader that gave them inspiration and vision, but the data available are insufficient to determine whether it is 'this specific person' or whether it is the 'figure' of a charismatic leader that acts as motivator and cohesive force.
- ***Self-monitoring:*** it is not explicitly considered or institutionalized by the organization. However, in practice, the high level of interactions among components (different sub-organizations) and among 'echelons' (particularly among representative in the Mixed Operations Centre, then down to the tactical level, and then again among operators in the field) results in what is described as *being attuned* with the environment (i.e. moving into a calmer phase, happenings at the political level such as Tsunami and reallocation of resources).

Case Study Assumptions and Limitations:

a. What constraints did you encounter that might limit the case study or the evidence supporting it?

The findings presented here have been constrained by time and resource issues. Due to these issues, the interviews have been conducted following a snowball approach, which bears scientific shortcomings. The inquiry conducted so far has provided interesting and rich insights. However, the amount of people interviewed is too little to provide conclusive results. it would be beneficial to continue the investigation, eventually expanding the perspective and gather data from other angles. For instance, further work should be conducted focusing on the activity of specific components and/or, particularly, on what did not work.

b. What assumptions did you make when carrying out or documenting the case study?

The case study was conducted under the assumption that this was a successful operation, because this is how the public and the official channels described it. Attempts have been made at finding data about problems or unsuccessful episodes, but the time constraints mentioned above hindered the search.

X: Conclusions

This case study, although rather small, presents some interesting elements regarding the concept of agility. The vision of the provincial chief of providing the organization with a broader and richer pool of competences and personalities through the 'double identity' campaign for the recruitment of volunteers proved to be crucial as it rooted the organization to its territory, and volunteers switched to their personal networks when needed information and help. Further, the other pillar of the reorganization, the 'being a system' campaign, also seems to have contributed to build a solid foundation of collaboration and interaction among local population and the Civil Protection. The local population is not considered as a passive recipient of help and rescue, but as an active part in being prepared and in responding to the emergency.

A peculiar element of this case study is the co-presence of a strong National Level (and Leader) with a (as) strong Mission Command attitude. The two seem to co-exist in equilibrium, as the National representatives act as facilitators, and enablers, particularly by providing resources, to the local level, which is in fact the one 'in charge'. The figure of the leader emerged as very relevant from the interviews, although it is unclear whether the salient element is 'this specific person' as a leader or the more abstract idea that there is a 'strong leader' who keeps it altogether. Interviewees suggested that this specific leader made a difference, as they indicate him as very charismatic, although not controlling, and very respected. This issue would need to be explored further.

It seems that, particularly thanks to the reorganization that preceded the events, this organization has developed the foundations in terms of mindset, culture, and procedures, for manifesting C2 agility. In fact, the C2 approach adopted during various phases of the emergency shift according to changed conditions in the environment: at the peak of the emergency, when chaos reigns, the components self activate and self synchronize. While the situation gets less hectic and more structured, although still within an emergency, the set up of the Mixed Operations Center facilitates coordination, still leaving a high degree of freedom to each

component. The national representatives are there, but not taking over the operation. While the situation gets more into a stabilization phase, responsibility shifts further towards the level of municipalities.

It must be added that the way the chain of command is designed allows and facilitates flexibility, as local chiefs have a rather high decision making power. However, the decision to locate people in hotels has been possible because the national chief reached the area within a few hours (He is the only one who can make decisions involving a large amounts of money). This leads us back to the interplay between national level and mission command, which should be further explored. Further investigation would also be needed to explore the events described here from the view-point of single components.

The model described here is referred to 2000-2009, it is unclear whether the Civil Protection in Brescia still follows these principles.

Acknowledgements

The authors of this case study would like to thank Mr. Corrado Scolari, Head of Civil Protection in the province of Brescia 2000-2009, for his support during the data gathering process, and all the members of the Civil Protection who have kindly agreed to being interviewed.

A special thanks goes to Dave Alberts, Dick Hayes, and all the members of SAS-085 for a very inspiring collaboration during the work of the group.

Bibliography

Bonfante, S. (2010) *Missione Abruzzo, testimonianze di Protezione Civile* http://www.arimagenta.it/documenti/arire/Lombardia%20-%20Missione%20Abruzzo.pdf

Emergency plan of the Province of Brescia www.provincia.brescia.it/protezione-civile/piano

Fare Sistema. Book published by the Civil Protection Brescia

Homepage of the parish of Brescia with documents related to the earthquake http://www.diocesi.brescia.it/diocesi/sisma/sisma.php

Italian Experimental Seismic Network (IESN) http://www.iesn.org/speciali/garda/garda.htm

Educational DVD divulgated by Civil Protection province of Brescia

Law 225/1992 http://www.protezionecivile.gov.it/cms/attach/editor/225_1992.pdf

Law 401/2001 http://www.protezionecivile.fvg.it/ProtCiv/GetDoc.aspx/9.pdf

National Civil Protection Homepage http://www.protezionecivile.gov.it

Newspapers' articles http://www.protezionecivile.gov.it/cms/attach/copy_461_09.pdf

Salo's earthquake, homepage of the Garda Volunteers
http://www.volontaridelgarda.org/terremoto/interventi_di_soccorso.html

Silverman, D. (2009) *Doing Qualitative Research*. SAGE Publications Ltd. Third Edition.

La Protezione Civile siamo noi (The Civil Protection is Us), presentation.

Video Documentary 'La Protezione Civile siamo noi' http://www.lastoriasiamonoi.rai.it/puntate/protezione-civile/953/default.aspx

Interviews

Mr. Corrado Scolari, Head of Civil Protection in the province of Brescia 2000-2009

Member of fire-fighters Salo'

Member of Garda volunteers

Member of Garda volunteers

Member of Civil Protection volunteers, kennel club unit

Member of first response group

B.5 Haiti Earthquake Case Study

Identify the Focus of and the Boundaries for the Case Study

h. What is the level of analysis? (e.g. Individual, Team, Organization, or Collective)

The analysis is conducted at the collective level.

i. **Who or What Organizations are included in the case study? (e.g. the Collective responding to the Haiti** Earthquake Crisis, Air-Ground Control Strike Teams in Iraq and Afghanistan)

This case study will examine the Collective (i.e. everybody who participated in the overall effort) of organizations and individuals who responded to the Haiti Earthquake Crisis. This group includes entities within the US government, specifically USAID and the military (SOUTHCOM), UN cluster organizations and missions, and international NGOs.

j. What temporal boundaries are included?

a. When does the case begin and end?

The case study begins with the start of the earthquake on January 12 and the subsequent arrival of relief entities (Icelandic contingency), on January 13, 2010; it ends once the primary effort is focused upon reconstruction, which we assign to the period following the lowering of US troop presence below 200 in mid-April.

Jan 12 - The earthquake of magnitude 7.0 struck Haiti, just outside of Port-au-Prince, at approximately ten-minutes-till six in the evening of 12 January 2010.[2] The devastation was wide-spread and especially acute in the densely populated areas surrounding the capital. Much of the critical infrastructure, particularly government and healthcare, was destroyed, drastically reducing the capacity of the Haitian people to recover without outside support. Moreover, prior to the earthquake, Haiti had already been receiving international humanitarian support through the United Nation Stabilization Mission in Haiti (MINUSTAH), but even this entity was extremely affected by the disaster, as several senior officials were killed,[3] and required time to recuperate, as well, thus setting the stage for one of the most comprehensive international relief efforts ever.

Within hours of the earthquake President René Preval was in touch with American Ambassador Merten and Lieutenant General Keen of US Southern Command, asking for emergency assistance.[4] In Washington, President Barack Obama met with several agency heads to work out a coordinated response from the United States Government.[5]

[2] OCHA Situation Report #1
[3] Report of the Secretary-General on the United Nations Stabilization Mission in Haiti, 1
[4] Keen *et al*, 85
[5] Taft-Morales and Margesson, 15 January, Summary

Jan 13 – In the early hours of the morning following the earthquake, heads of state and various charities and international organizations were calling emergency meetings to assess what type of response was needed and possible from their respective states and organizations. Notably, Dominican President Leonel Fernández put together an emergency aid commission,[6] and the Search and Rescue team from the Dominican Republic was the first to be reported on the ground by the United Nations Office for the Coordination of Humanitarian Affairs.[7] Teams from Iceland and the United States were also reported to be on the ground, while twenty-six other countries had offered to send Search and Rescue teams.

The United Nations dispatched a Disaster and Assessment Coordination team, which began arriving that day. The UN also adapted its Cluster System for application to the Haiti response and initially organized five clusters: Logistics, Shelter, Water and Sanitation, Health, and Food.[8] The clusters were organized around various international organizations that often partnered with the UN, including the World Food Program, the International Organization for Migration, and the World Health Organization. The United Nations Stabilization Mission in Haiti also began to rebound from the initial shock of the earthquake and set up an emergency humanitarian coordination center at the Toussaint L'Overature International Airport and began clearing the main roads in Port-au-Prince in order to aid in the Search and Rescue effort.

The United States military was also able to quickly assess and open the international airport, allowing an initial flow of humanitarian aid and workers to flow into the country.[9] At this point, flight control was being performed via line-of-sight radio transmissions from the ground at the Port-au-Prince airport.[10]

Jan 14 – On the second day following the disaster, much of the focus was on organizing the search and rescue effort, which was being coordinated by the United Nations. By the end of the day, as many as twenty-one search and rescue teams were on the ground in Haiti. Representatives for all five of the OCHA clusters were able to meet on the ground in Haiti and organize the collective SAR effort. [11]

The United States Air Force continued to provide emergency assistance in coordinating incoming flights to Port-au-Prince by assigning slot-times to planes wanting to offload in Haiti. The United States Southern Command also officially formed the Joint Task Force – Haiti, in order to manage the combined effort from the United States armed services.[12] In an effort to aid collaboration among the many actors involved in the response effort, the United States Defense Information

[6] Diaz
[7] OCHA Situation Report #2, 2
[8] *ibid*
[9] Keen, *et al*, 86
[10] OCHA Situation Report #2, 2
[11] OCHA Situation Report #3, 1
[12] Ryan, Goehring, and Hulslander, 8

Systems Agency opened its information portal, the All Partners Access Network, to any organization that was supporting the effort in Haiti.[13]

b. Are there phases involved? If so, what are their boundaries?

The Haiti Earthquake Relief Effort was separated into three major phases: Saving Lives, Stabilization, Reconstruction.

Phase 1: Search and Rescue – January 13-22, 2010 "The government has declared the search and rescue phase over,'' the UN's Organisation for the Co-ordination of Humanitarian Affairs (OCHA) said in its January 22 situation report on the relief effort. Improvised urban search and rescue (USAR) would have begun immediately, being carried out by local authorities and individuals on an uncoordinated basis and with limited effectiveness. The first international search and rescue team arrived from Iceland via Washington, DC, on January 13. By the end of the week, there were a total of twenty-seven USAR teams on the ground in Haiti, which had successfully performed fifty-eight live rescues and covered over half of the "worst affected" areas.

Phase 2: Stabilization – January 23 – mid April, 2010

The deployment level of US SOUTHCOM has dropped below 200 troops.

k. Other boundaries (e.g. separate analyses of the collective and of specific organizations within the collective).

The approach for this case study is aimed at studying a series of stories in order to gain an understanding of the broader context. Thus, in this case, we found it useful to separate out efforts *analytically*, though *realistically* they are not independent of one another.

Describe the Challenge or Opportunity that gave rise to the need for C2 Agility.

The need for C2 Agility arose from the level and extent of the destruction in Haiti. As both the Government of Haiti (GoH) and the already present UN Mission were incapacitated by the earthquake, a swift deployment of international aid was necessary. Furthermore, there was limited access to up-to-date information on the social and economic conditions in Haiti for many of the entities involved in the response, as well as uncertainty over the pre-existing Haitian infrastructure. Therefore, relief teams needed to be flexible and able to adapt quickly to conditions once they were on the ground. Moreover, as the response was an international effort, all the entities involved needed to coordinate and adapt in a quickly changing environment under uncertain leadership.

The salient factors driving the need for C2 Agility were the complexity and urgency of the situation. For some organizations, such as the United States military, the requisite level cooperation with international entities presented a particular challenge, as they were more comfortable with independent operations. For others, such as the United Nations, responding quickly to the demanding situation was unfamiliar territory, as most

[13] Defense launches online system

humanitarian operations typically involve long, drawn-out operations. Hence, many of the actors involved in the Earthquake Response were operating outside of their comfort zones.

What would have been the consequences of a failure to act in a way that demonstrates C2 Agility?

The stakes associated with failing to act in a manner associated with C2 Agility were significantly high. As both the government and already-present UN Mission (MINUSTAH) had been incapacitated by the earthquake, the response lacked a central, coordinating actor. Thus, if the response did not at least resemble an Agile response, then the efforts of the multitude of international responders could easily have become conflicted and counter-productive. Furthermore, by the nature of the disaster, as more time wasted away, more people were dying as they waited for help.

Was C2 Agility Manifested? If so, how? (Be as clear and precise as possible, but keep this simple so that it does not require repetition in the next steps.)

C2 agility was manifested in the Haiti relief effort, albeit in a limited capacity. Mobilization of support was remarkably rapid, especially in comparison to previous cases. However, due to a lack in a clear humanitarian leadership and the restrictive nature of the cluster system, the international response effort was not able to translate this early effort into a sustained, agile response. Several issues arose due to poor planning assumptions, in particular.

Which Enablers and Inhibitors of C2 Agility were observable? (Remember that the basic six may not be independent. Include discussions of the relevant Agile Behaviors, but try to tie them to one or more Enablers. Specify inhibitors that impacted C2 Agility)

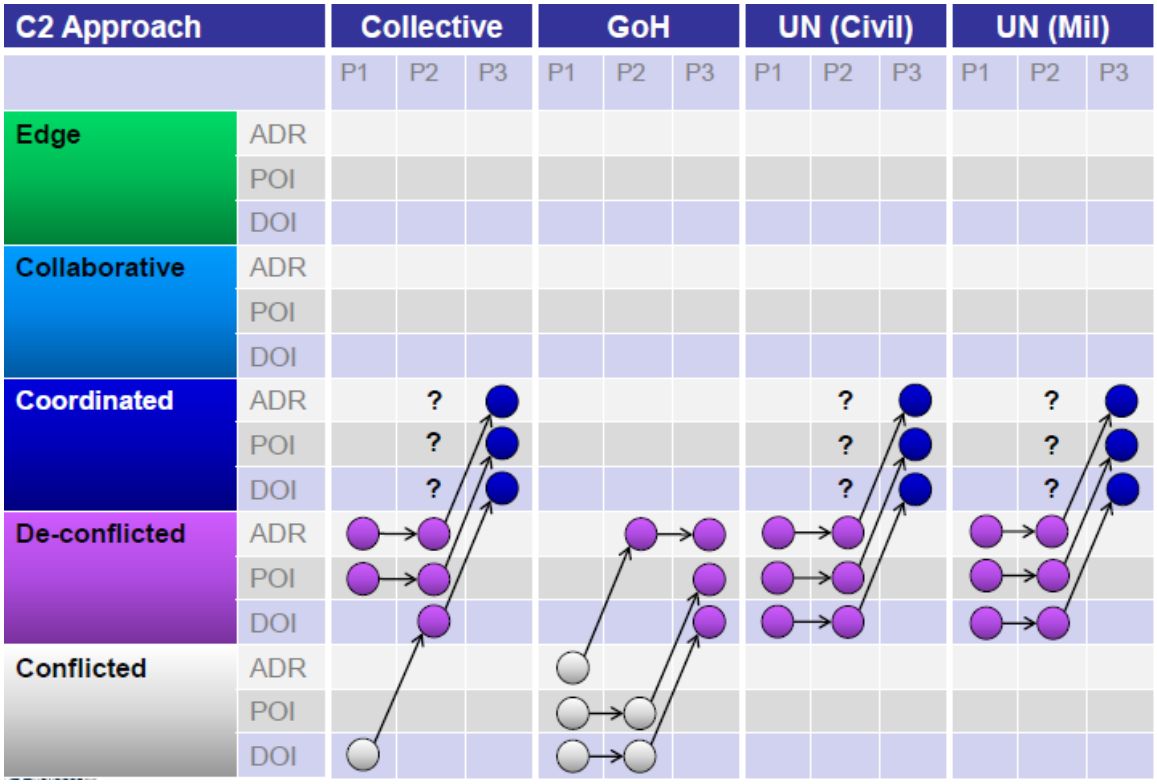
h. Robustness – UN cluster system proved to be less than effective due to improper planning and incorporation of best-practices that would have allowed a smoother translation of the 2005 Pakistan approach to the Haiti response.
i. Responsiveness – quick deployment of USSOUTHCOM
   - quick deployment of field hospitals (i.e. Israel)
j. Resilience
k. Innovation – wiki mapping
l. Flexibility – military used non-classified, open-source material, i.e. Google maps
   - Firms began creation of an emergency ad-hoc satellite communication system within hours of the earthquake
m. Adaptation – wiki open street mapping

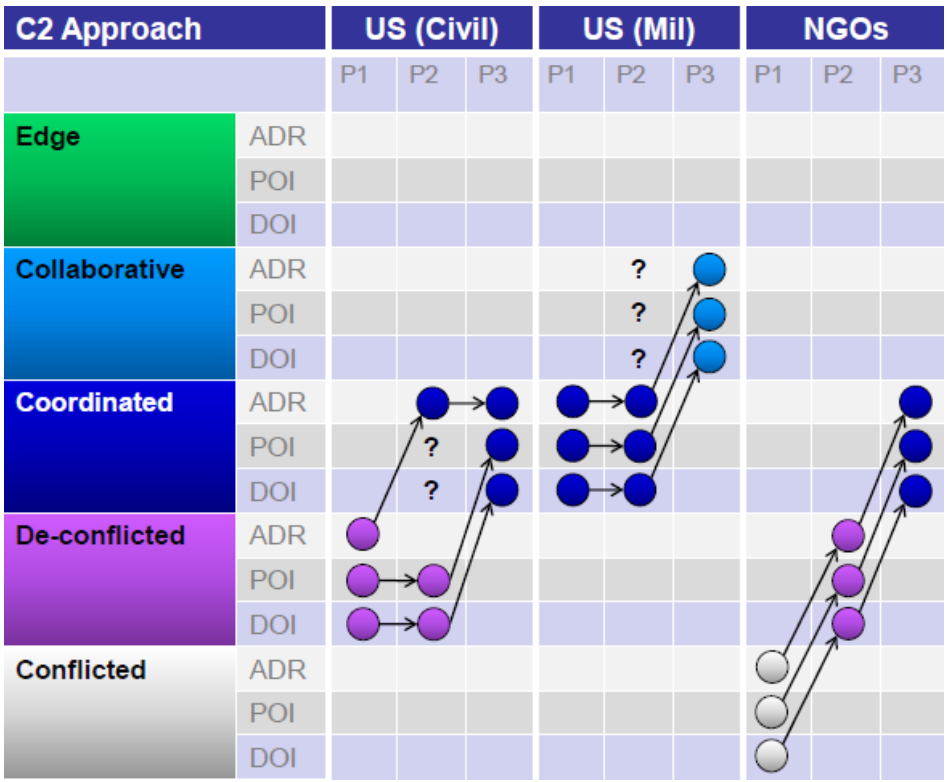
What C2 Approaches were relevant? (How can C2 Approach Agility be inferred from what was reported or observed?) Did C2 Approach change, either for a collective, organization, team or one or more individuals?

There was no indication regarding the Appropriate C2 Approach. So since the situation complexity decreases from High through Medium and settles between Medium and Low during the Transition phase 3, it is assumed that the required C2 approach would start off as Edge and then move along the diagonal in the C2 Approach Space and end up somewhere between Coordinated and De-conflicted (maybe closer to Coordinated).

The Tables below show a few off-diagonal C2 Approaches (e.g., DOI is at the Conflicted level, while ADR and POI are at the De-conflicted level). But for the most part, ADR, DOI, and POI remain on the diagonal of the space.

None of the organizations reached the appropriate levels of Edge in Phase 1, but managed to hover around the De-conflicted and Conflicted level except for the US Military that was Coordinated. However, by Phase 3, most organizations were Coordinated, again except for the US Military that was Collaborative. The Government of Haiti also reach only a De-conflicted level by the end of Phase 3.





What interesting and important vignettes are included or can be derived from the case study to help create illustrative stories?

e. Open Street Map ('Geek' video)
One of the more salient issues initially faced by search and rescue workers as the lack of clear and authoritative mapping at the street level in Port-au-Prince and its environs. An early solution to this dilemma was the utilization of open-source technology via the internet, specifically Open Street Map. Like the popular internet-based encycopedia, Wikipedia, Open Street Map gathers input from a variety of users. In this particular case, the use of open-source technology allowed users to download maps of Port-au-Prince, for example, and incorporate their own knowledge into a continously changing map. Within twenty-four hours, hundreds of users had uploaded edits to road maps, and the level of detail included a number of side-streets and minor roads.
Open Street Maps were used by many of the search and rescue teams, including UN responders. Moreover, mappers were also able to use OSM to create interactive maps which a number of points of interested, including collapsed buildings and temporary housing. By incorporating information garnered through text messaging, Creole translators in the United States were also able to tag locations of trapped individuals; in turn, rescue workers could more efficiently locate distressed persons and provide aid as applicable.

f. UNHABITAT (becoming 'lost' in the cluster system)
The UNHABITAT relief group arrived in Haiti within the first week of the relief effort and quickly developed a strategic report in French on the housing situation on the ground in Haiti. As the report was in French, it could have been a useful tool for collaboration among the predominately English-speaking relief workers and the French-speaking Haitian Government. However,

UNHABITAT was organizationally placed as the lead of the "housing" working-group within the Early Recover Cluster, rather than being incorporated into the Shelter Cluster. Consequently, the impact of the UNHABITAT report was rather limited.

g. Near real-time translation of Creole texts
h. Early establishment of a central information sharing center between military and other US actors and use of open-source material for continuity of info

i. Establishment of the Israeli Field Hospital 89 hours after earthquake (special assessment team dispatched within 11 hours)
j. Establishment of an ad-hoc satellite communications network

Case Study Assumptions and Limitations:

a. What constraints did you encounter that might limit the case study or the evidence supporting it?

b. What assumptions did you make when carrying out or documenting the case study?

Conclusions

a. This is not a summary – that is in the Executive Summary
b. Conclusions relate to the purposes of the case study
  a. Enablers, Constraints, and Behaviors identified
  b. Language – Clarity and Definitions
  c. Applicability of the SAS-085 Concepts and Model
  d. Statements about Validity

Bibliography

Bridges, Mary, Robert Greenhill and Ian Rogan. *Innovations in Corporate Global Citizenship: Responding to the Haiti Earthquake*. World Economic Forum: 2010.

Brewin, Bob. 2010. *Defense Launches Online System to Coordinate Haiti Relief Efforts*. NextGov: Technology and the Business of Government. 15 January 2010. 1 October 2010. http://www.nextgov.com/nextgov/ng_20100115_9940.php .

Connell, Christopher. *In Haiti's Hour of Need, Texting "4636" Became a Lifeline*. America.gov. 19 February 2010. 10 December 2010. http://www.america.gov/st/develop-english/2010/February/20100219131612berehelleK5.066395e-06.html .

Defense launches online system to coordinate Haiti relief efforts. NextGov.com. 15 January 2010. 6 December 2010. http://www.nextgov.com/site_services/print_article.php?StoryID=ng_20100115_9940 .

Fraser, General Douglas M. and Major Wendell S. Hertzelle. *Haiti Relief: An International Effort Enabled through Air, Space, and Cyberspace*. Air and Space Power Journal 24. 4 (Winter 2010): 5-12.

Grünewald, François and Andrea Binder. *Inter-agency real-time evaluation in Haiti: 3 months after the earthquake*. Global Public Policy Institute; Broupe Urgence Rehabilitation Développement. 31 August 2010.

Guha-Sapir, D., T. Kirsch, S. Dooling, and A. Sirois. *Haiti Earthquake Interagency Lessons Learned: Workshop Report*. 22 June 2010.

Hayes, Dr. Margaret D. (Interviewer) and Lieutenant General Ken Keen (Interviewee).

Hume, Brit (Interviewer), Lieutenant General Ken Keen and Dr. Rajiv Shah (Interviewees). *Update on Haiti Relief Effort* [Interview Transcript]. Fox News. 18 January 2010. 18 November 2010. http://www.foxnews.com/story/0,2933,583273,00.html .

Joining Forces in an Emergency – Logistics Emergency Teams (LET). WFP.org. 15 November 2010. 21 January 2011. http://www.wfp.org/logistics/blog/joining-efforts-emergency-logistics-emergency-teams-let .

Joint Task Force Haiti. *Humanitarian Assistance Coordination Center: Command Brief*. 2010.

Keen, Lieutenant General P.K., Lieutenant Colonel Matthew G. Elledge, Lieutenant Colonel Charles W. Nolan and Lieutenant Colonel Jennifer L. Kimmey. *Foreign Disaster Response: Joint Task Force-Haiti Observations*. Military Review 40. 6 (2010): 85-96.

Lynch, Colum. "Top U.N. aid official critiques Haiti aid efforts in confidential email." *Turtle Bay: Reporting from Inside the United Nations*. 17 February 2010. 6 December 2010. http://turtlebay.foreignpolicy.com/posts/2010/02/17/top_un_aid_official_critiques_haiti_aid_efforts_in_confidential_email .

Provencher, Kaitlin. *Crowdsourcing Crisis Response*. Tufts E-News. 5 February 2010. 10 December 2010. http://enews.tufts.edu/stories/1621/2010/02/05/crisismapping .

Ryan, Colonel John, Russ Goehring, and Robert Hulslander. *USSOUTHCOM and Jint Task Force-Haiti…Some Challenges and Considerations in Forming a Joint Task Force*. Joint Center for Operational Analysis Journal 12. 2 (2010): 1-20.

Taft-Morales, Maureen and Rhoda Margesson. *Haiti Earthquake: Crisis and Response*. Congressional Research Service. 15 January 2010.

Taft-Morales, Maureen and Rhoda Margesson. *Haiti Earthquake: Crisis and Response*. Congressional Research Service. 2 February 2010.

Taft-Morales, Maureen and Rhoda Margesson. *Haiti Earthquake: Crisis and Response*. Congressional Research Service. 8 March 2010.

Tomasini, Rolando and Luk Van Wassenhove. *Helping Out Haiti*. Forbes.com. 22 February 2010. 21 January 2011. http://www.forbes.com/2010/02/22/humanitarian-relief-haiti-global-opinions-contributors-tomasini-wassenhove.html .

United Nations. *Report of the Secretary-General on the United Nations Stabilization Mission in Haiti*. New York, 22 [April] 2010.

USAID Fact Sheets

OCHA Situation Reports

B.6 Munich Olympics Case Study

Data Sources

This section describes the data sources that were used to conduct the evaluation of the C2 Agility model:

1. Film

   MacDonald, K. (Director) (1999). *One Day in September*. United States: Passion Pictures.

   Synopsis: One Day in September is a 1999 documentary film directed by Kevin Macdonald examining the September 5, 1972 murder of 11 Israeli athletes at the 1972 Summer Olympics in Munich, Germany. Michael Douglas provides the sparse narration throughout the film. The film won the Academy Award for Best Documentary Feature in 2000. Besides footage taken at the time, we see interviews with the surviving terrorist, Jamal Al Gashey, and various officials detailing exactly how the police, lacking an anti-terrorist squad and turning down help from the Israelis, botched the operation.

   http://www.youtube.com/watch?v=UftbXtupuBo&feature=fvw

2. Television

   Clarke, S. (Director) (2007). *Olympic Massacre: The True Story*. United Kingdom: Channel Five.

   Synopsis: The documentary series exploring infamous historical events continues with an examination of the horrific events of 6 September 1972, when Palestinian terrorist group Black September took nine members of the Israeli athletics team hostage. Using new footage, archive material and eyewitness testimony, this gripping documentary provides a unique perspective on that day's bleak events.

   http://www.youtube.com/watch?v=yZx6PcQG-hY&feature=related

3. Report

   Pro Sport München (1972). Die Spiele: The official report of the Organizing Committee for the Games of the XXth Olympiad Munich 1972. Volume 1: The Organisation.

   Synopsis: The official report of the Organizing Committee for the Games of the XXth Olympiad Munich 1972 describes in detail the events leading up to and during the events of 6 September 1972. In addition, the report gives a detailed account of the security arrangements put in place for the Games as well as a detailed description of the organization and their roles.

   http://olympic-museum.de/o-reports/report1972.htm

4. E-Book

   Schiller, K., and Young, C. (2010). *The 1972 Munich Olympics and the Making of Modern Germany*. University of California Press.

   Synopsis: The 1972 Munich Olympics—remembered almost exclusively for the devastating terrorist attack on the Israeli team—were intended to showcase the New Germany and replace lingering memories of the Third Reich. That hope was all but obliterated in the early hours of September 5, when gun-wielding Palestinians murdered 11 members of the Israeli team. In the first cultural and political history of the Munich Olympics, Kay Schiller and Christopher Young set these Games into both the context of 1972 and the history of the modern Olympiad. Delving into newly available documents, Schiller and Young chronicle the impact of the Munich Games on West German society.

   http://www.ebooks.com/ebooks/book_display.asp?IID=566752

5. Book

   Reeve, S. (2001), One Day in September: the full story of the 1972 Munich Olympic massacre and Israeli revenge operation "Wrath of God". Arcade Books.

Synopsis: Based largely on exhaustive investigation for the Oscar-winning documentary, One Day in September is the definitive account of the tragedy. Simon Reeve has gathered extraordinary information from a number of sources, including recently released Stasi files and interviews with key figures, including the families of the hostages, politicians, policemen, advisors, fellow athletes, media figures, and even the lone surviving member of the group that carried out the attack. Reeve's control over his material is admirable. He vividly paints images of the individuals involved, humanizing a narrative that cracks and buzzes with the compact tension of those 24 hours. At the same time, he provides the background to the attack, filling in vital historical context from the distant and recent past, such as the Arab-Jewish dispute that produced this and other terrorist actions and their responses. Reeve conveys the public horror of Jews being incarcerated on German soil, which led the German authorities to make crucial judgments, with tragic results. Fatal errors were made that can only be fully understood through the underlying dynamics of not only Middle East.

Identify the Focus of and the Boundaries for the Case Study

I. What is the level of analysis? (e.g. Individual, Team, Organization, or Collective)

The Collective

Defining the Collective is difficult because during the Munich Olympics the size of the collective varied with time. That is, the Allocation of Decisions Rights (ADR), Patterns of Interaction (ADR), and Distribution of Information (DoI) were applied to different sets of people and organizations at different times. Figure B.6.1 illustrates this point.

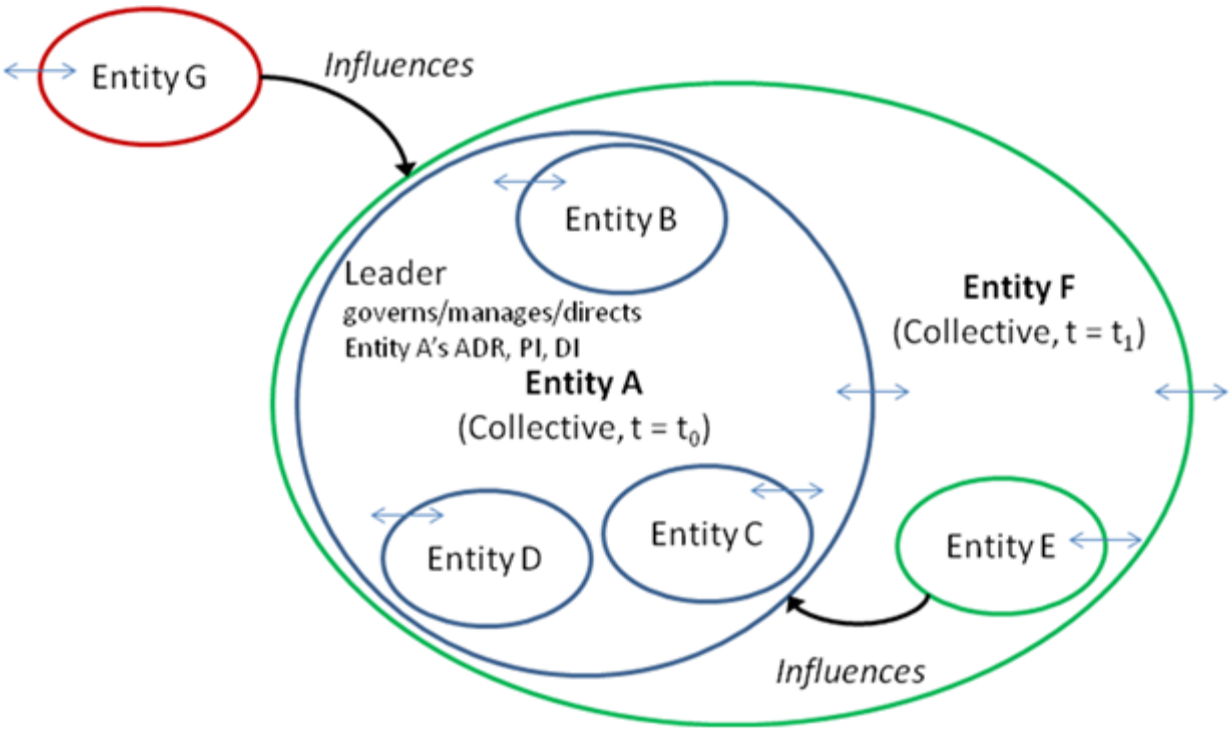


Figure B.6.1: Entities Expands and Contracts over time

An entity may be an individual, a team, an organization, a collective, a set of collectives, and so on. Thus, the entity concept is scalable (SAS-065, 2010). For illustrative purposes, in Figure 41 Entity A is a collective that includes Entities B, C, and D at $t = t_0$, which are likely organizations. Entity A also includes a Leader entity whose role is to govern, manage, and direct the Entity A's ADR, PoI, and DoI as the collective transitions from one C2 approach to another. The Leader entity may be stand alone or a member of one of the sub-entities. Each entity is likely to have a leader entity – whether it is a formal appointment or the leader emerges as normal part of group dynamics.

At $t = t_0$, Entity E is outside of the collective (Entity A) because it is not part of Entity A's ADR, PoI, or DoI. Rather, Entity E may be a governing body or stakeholders that influence the direction that the collective might pursue in resolving a conflict. Sometime later ($t = t_1$) Entity A expands to include Entity E and becomes Entity F. In this example, the governing body or stakeholder may feel it necessary to take on a leadership role for Entity F. Note that Entity G influences Entity F in the same manner that Entity E influenced Entity A at $t = t_0$.

It is important to define the collective boundary (who's in and who's out) at the various phases in time in order to make an assessment of the collective's C2 Approach agility during that phase. Unfortunately, the Munich Olympics media sources were not clear enough to determine the collective's boundary at each phase of the Olympics.

The approach transition model in (Farrell, 2011) takes into account for a change in the entity size. This change in size is added to the resistance term such that if the entity grows then the overall Resisting Force becomes larger, and visa-versa.

In summary, the level of analysis was at the collective level but defining the collective boundary was difficult because it varied throughout the event.

m. Who or What Organizations are included in the case study? (e.g. the Collective responding to the Haiti Earthquake Crisis, Air-Ground Control Strike Teams in Iraq and Afghanistan)

The five media sources were used to collect data regarding the collectives' key entities. It was not clear which entities were in the collective and outside of the collective at any particular time. The role of each entity is described below:

1. *Three Territorial Governments:* The Federal, State, and Municipal German Governments were responsible for planning, executing, and financing the Olympic Games. Key players within the three territorial governments included the following:

    - Hans-Dietrich Genscher (Federal Minister of the Interior): Key decision maker and negotiator used during the disturbance who offered himself as a hostage;

    - Bruno Merk (State Minister of the Interior for Bavaria): Assigned as Head of the Crisis Management Team with highest authority ranking. Negotiated with the terrorists and was involved in all decision making processes regarding rescue plans and attempts;

    - Dr. Hans-Jochen Vogel (Mayor of Munich). Heavily involved in the initial Munich bid, as well as the planning for the Games. Member of the Crisis Committee formed immediately after the terrorist attack;

    - Willy Brandt (German Chancellor): Involved in freeing the hostages by attempting to contact and communicate with Egyptian Heads of State during the disturbance;

    - National Army: Assisted in the preparation and execution of the Olympic Games but did not play an active role during the disturbance;

    - West German Border Guards: Provided Security Service in order to maintain peace and intervene as unobtrusively as possible. During the disturbance the Border Guards were recruited to be part of operation "Sunshine" where the collective attempted to ambush the terrorists in the Israeli sleeping quarters;

    - City of Munich: Responsible for the examination of previously documented Olympic hosting issues from both the IOC Statutes and the Official Reports on the Olympic Games;

    - Munich Police: Pre-Olympics, officers were responsible for ensuring that the Olympic Village was safe and secure. Pre-disturbance, policing roles were limited to protecting from outside the Olympic sites. Immediately following the initial disturbance, the police officers arrived on scene at the Olympic Village and from that point on the Policing roles included negotiating with terrorists, participating in the all organized rescue attempts, and the final open-fire event at the airfield. key players within the Munich Police included:

- Manfred Schrieber, Chief of Police: assumed leadership of the police efforts which included negotiation attempts with the terrorists and decision making upon organized rescue attempts;

- Georg Wolf: deputy commander of the Munich Police and was given responsibility over the rescue attempt at Fürstenfeldbruck airfield; and

- George Sieber: Police Psychologist, worked with police force pre-Olympics with the intension to prepare them so that they could react efficiently and effectively towards security threats.

2. *International Olympic Committee (IOC):* The IOC (Chairman: Avery Brundage) was responsible for selecting the Olympic host city and ensuring that the winner is compliant with all of the IOC's statutes. Pre-disturbance, the IOC was involved in the decision making process which determined that the Olympic Venues would not be policed. During the disturbance the IOC placed intense pressure upon the German Government to expedite the hostage crisis.

3. *[Olympic] Organising Committee (OC):* The OC, governed by the IOC, would stipulate its duties and regulate the collaboration of the federal government, municipal governments, and the sports federations (3). Overall responsibilities assigned to the Organizing committee included organizing and financing Olympic facilities and organizing preparations to ensure the smooth execution of the Olympic Games including security. Prior to the disturbance the OC was involved in the decision that policing of the Olympic Venues would not occur. The Organizing Committee was led by Willi Daume (President), Vice- President Hans-Dietrich Genscher, who was Federal Minister of the Interior and Dr. Hans-Jochen Vogel, who was Mayor of Munich. Additionally, Herbet Kunze fulfilled the role of the General Secretariat, and Walther Tröger was the Major of the Olympics village (who also was one of the negotiators). The organizing committee also consisted of a General Assembly, which was the highest body of the committee and included the full assembly of the members of the OC, the Executive Group who was to ensure that the Olympic Games would operate smoothly and encountered no significant obstacles and a Leadership Center tasked with keeping the executive group informed about any current developments at all facilities. Civil Security Service was hired by the Olympic Organizing Committee and lead by Manfred Schreiber and comprised of officers who were sportsmen and women or interested in sports and were recruited from the ranks of the police or border patrol and who had volunteered for this position. They were to fulfill the following roles during the Olympics: 1) ensure peace was maintained, 2) if required to settle minor disrupts, interventions were to be performed as unobtrusively as possible, 3) protect the Athletes Village from trespassers, 4) control traffic, 5) ensure police present was not found on the Olympic grounds and 6) if criminal activities were identified, pass such activity information over to the police. The Security service arrived on scene when the hostage crisis initially began, but they soon lost their power to that of the Police as the hostage crisis unfolded.

4. *Government of Israel*: During the disturbance the Israeli government was responsible for the requests from the terrorists, refusing to release the prisoners held captive in their Israeli jails. The Israeli Government did offer the support of their expert hostage negotiators to the German Government. Conflicting evidence as to whether or not the Israeli Government additionally offered the services of the Sayeret Matkal (Special Forces Team) during the hostage crisis

remains controversial. The main representatives acting on behalf of the Israeli Government were Prime Minister (Golda Meir), the Ambassador of Israel, Israeli's Minister of Defense (Moshe Dayan), two Israeli Hostage Negotiators and the Chief of Mossad, Israeli Secret Service (Zvi Zamir).

5. *Arab League:* During the hostage disturbance, two individuals represented the Arab League. Magdi Gohary, the Advisor to the Arab League, and Mohammed Khadif, Head of the Arab League in Bonn assisted the German Government with the negotiations.

6. *Key Players from other countries (Egypt and Tunisian Republic):* Two Egyptian representatives were involved during the hostage crisis in Munich. El Chafei, the leader of the Egyptian Team, provided advice to the German Government upon the hostage crisis. Whereas, the Egyptian Prime Minister was involved in communications with the Federal Chancellor. The Tunisian Ambassador, Mahmoud Mestiri and an employee of the Tunisian Embassy were available during the hostage crisis as well. The Tunisian Ambassador, Mahmoud Mestiri provided advice and guidance to the German Government upon ways to handle to hostage crisis. The employee of the Tunisian

n. What temporal boundaries are included?
   a. When does the case begin and end?
   b. Are there phases involved? If so, what are their boundaries?

1. *Pre-Event.* The collective have in their C2 toolbox a number of C2 approaches, the collective possesses a certain comfortable C2 approach and size and may have demonstrated in past events one or more control methods;
2. *During-Event.* This can be decomposed further into the following sub-phases:
   a. Pre-Disturbance. During the event (e.g., Olympic Games), but prior to the disturbance (e.g., terrorist attack) the collective may require a de-conflicted C2 approach;
   b. At the point of Disturbance (and immediately following it). The collective may require a collaborative C2 approach. Evidence for stiffness and resistance might also be seen. Evidence for one or more control methods should be observed. Evidence for one of more of robustness, responsiveness, resilience, and disturbance rejection should be observed.
      i. *Hostages in Apartment*. This includes events that took place within the time that the hostages were held in the apartment on Connollystrasse;
   c. Hours after Disturbance. Still during the event, the situation might subside due to collective intervention and may require a de-conflicted C2 approach. Evidence for stiffness and resistance might also be seen. Evidence for one or more control methods should be observed. Evidence for one of more of robustness, responsiveness, resilience, and disturbance rejection should be observed.
      i. *Apartment to Airfield* Move. This includes events leading up, and during, the time the terrorists and hostages left the apartment on Connollystrasse, up to until their arrival by helicopter at Fürstenfeldbruck airfield;

ii. Airfield Take-Down. This includes events between the time that the terrorists and hostages touched-down by helicopter at Fürstenfeldbruck airfield, up until the resolution of the operation; and,

iii. *Post-Disturbance*. This includes events that occurred after the failed rescue attempt at Fürstenfeldbruck airfield.

3. *Post-Event*. The collective returns to an Independent C2 approach following the termination of the event (e.g., completion of the Olympic Games).

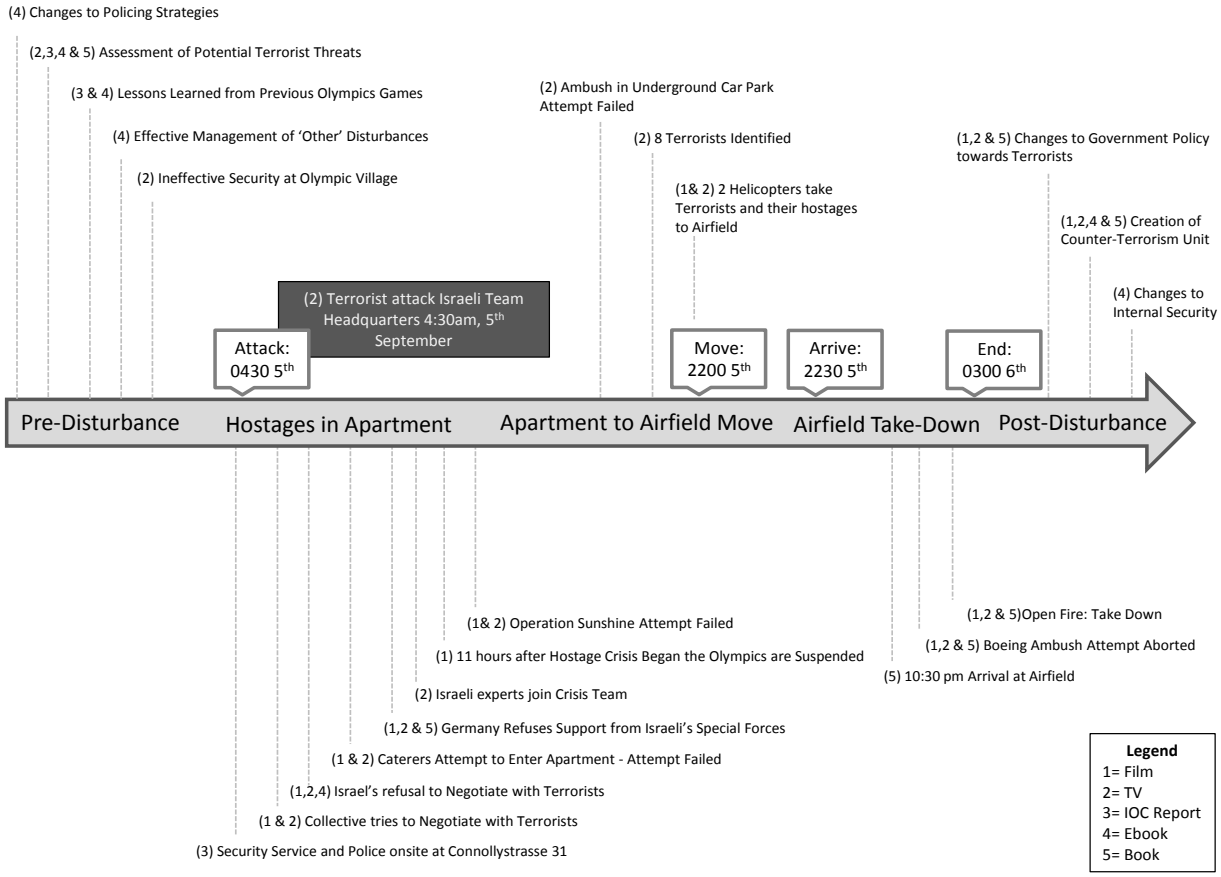


Figure B.6.2: Timeline of Events Relating to the Munich Olympics Massacre

The numbers found beside each event in parentheses represent the source of the data (1 through 5 listed below).

o. Other boundaries (e.g. separate analyses of the collective and of specific organizations within the collective).

None

Describe the Challenge or Opportunity that gave rise to the need for C2 Agility.

Based upon the 5 resources reviewed, it became evident that the major events associated with the Munich Olympic Massacre could be analyzed within 5 chronological periods. 1) The pre-disturbance period, contains the major preparation actions performed by the collective prior to the disturbance. The major preparation actions include altering of policing strategies, understanding challenges associated with hosting the Olympics and instilling appropriate measures that specifically targeted problems encountered in previous Olympics. Prior to the disturbance, such preparation measures proved to be sufficient as demonstrated by the collective's success at handling various minor disruptions. Shortly after however, these same preparation measures proved to be flawed, as demonstrated by the almost effortless, terrorist invasion of the Olympic Village on September 5th, 1972.

After the Israeli Olympic team members were taken hostage by the terrorists, numerous major events, which can be categorized by time and location (hostages in apartment, apartment to airfield move and airfield) demonstrated the collective's ineffective and inefficient attempts to resolve the hostage situation. With the Israel Government's unwillingness to release Palestinian prisoners, the collective, realizing that they had little negotiating power, hastily planned and orchestrated several different rescue attempts which included; trying to enter the Olympic building with police officers concealed as caterers, as well as three manpowered ambush attempts (operation "Sunshine", underground car park and the Boeing 747). A combination of errors increased the failure rate of the collective, which eventually led to the open-fire standoff at Furstenfeldbruck; where the deaths of all the remaining Israeli hostages, 5 terrorists and 1 German police officer occurred. This incomprehensible outcome resulted in focused post-disturbance events which aimed to improve strategies associated with terrorism policies and security measures.

Figure B.6.3 shows a number of photographic images taken during the Munich Olympics (clockwise from top left):

- Olympic village security guard armed with nothing more than a walkie-talkie, and dressed informally in line with the image of the "Happy Games";
- Outside 31 Connollystrasse terrorist leader Issa (far right) begins dictating terms to Munich police chief Manfred Schreiber (far left), German Interior Minister Hans-Dietrich Genscher (second from left), and Olympic Village Mayor Walther Tröger (middle, with back to camera);
- Members of the security force that were part of the aborted rescue plan, Operation "Sunshine". Live television coverage of this force making its way into position was seen by the terrorists in the apartment; and,
- After leaving the Olympic village the nine surviving hostages and eight terrorists were flown in two helicopters to Fürstenfeldbruck airfield outside Munich. After a German rescue plan collapsed when officers abandoned their positions, a firefight ensued that ended with the deaths of all the hostages.

Figure B.6.3: Images from the 1972 Munich Olympics

What would have been the consequences of a failure to act in a way that demonstrates C2 Agility?

The Munich Olympics analysis shows clearly the consequences of a failure to act and a failure to transition from de-conflicted to an appropriate collaborative C2 approach. In this case, the consequences were the death of 11 members of the Israeli team and ongoing tensions between Israel and Palestine. Unfortunately, the case study cannot find a correlation between C2 agility and mission success (or being in the bounds of success) because it was concluded that the event was not successful nor did the collective transition from one approach to another.

Was C2 Agility Manifested? If so, How? (Be as clear and precise as possible, but keep this simple so that it does not require repetition in the next steps.)

No. There is no evidence that the collective transitioned from one approach to another. In terms of the broader definition of C2 Agility there was no evidence that the collective was able to cope with changes in circumstances and/or exploit these changes by operating in the most appropriate region of the C2 Approach Space.

Which Enablers and Inhibitors of C2 Agility were observable? (Remember that the basic six may not be independent. Include discussions of the relevant Agile Behaviors, but try to tie them to one or more Enablers. Specify inhibitors that impacted C2 Agility)

Discussions are still ongoing on whether these six are enablers of agility or they are by-products of agility. The case study did not yield any evidence that the collective intentionally used responsiveness, versatility, flexibility, resilience, innovation, or adaptive to cope with the situation or transition from one C2 Approach to another. On the other hand one observe these variables (or lack thereof) as by-products of (the lack of) agility. Note that the definitions are quotes from SAS-065 which are quoted from (David S. Alberts & Hayes, 2003).

- Flexibility: "The ability to employ multiple ways to succeed and the capacity to move seamlessly between them."
    - The Munich Collective tried several plans – all failed
- Versatility (Robustness): "The ability to maintain effectiveness across a range of tasks, situations, and conditions."
    - Case study did not indicate versatility over the range of situations.
- Responsiveness: "The ability to react to a change in the environment in a timely manner."
    - Collective was either slow to respond or responded poorly
- Adaptiveness: "The ability to change work processes and the ability to change the organization."
    - The Collective did not take advantage of opportunities to adapt
- Resilience: "The ability to react to a change in the environment in a timely manner."
    - There were indications of regrouping after plans failed miserably
- Innovation: "The ability to do new things and the ability to do old things in new ways."
    - It is not clear if there was any innovation, although with poor outcomes

Given that the collective showed no indications of agility it is difficult to make any correlation between agility and these six enablers. The question is, was the collective non-agile because of the lack of versatility, responsiveness, etc. or did the collective lack versatility, responsiveness, etc. because it was not agile. This becomes a classical "chicken-or-egg" problem.

(Farrell, 2011) provides an analogy between the transition from an initial approach to the required approach and a mass-spring-damper system that moves from an initial position to the required position. The transition model proposes three key parameters that enable/inhibit the dynamic transition between one C2 Approach and another (i.e., enable/inhibit C2 Agility): size (mass), resistance (resistance), and comfort level (stiffness).

Carrying this analogy to its logical extent, the size of the organization is equivalent to the mass of an object. The resistance that impedes the C2 Approach transition is equivalent to the resistance that impedes the object's motion. The comfort level or familiarity with a C2 Approach(es) has the same properties as an object attached to a spring (with a certain stiffness) forcing it to an un-stretched position. This analogy leads to a number of concepts including:

- Entity Momentum – An organization has momentum when moving in the C2 Approach space
- Resisting Force – There are internal and external forces that resist movement in the C2 Approach space.
- Restoring Force – There is a restoring force that pulls the entity back to a comfortable C2 Approach.
- Forcing Function – There is a force based on the situation complexity that compels the entity to transition to the required C2 Approach.

These forces along with the change of momentum determine the dynamics (time and amplitude) as the entity moves within the C2 Approach space. Thus, in theory the size, resistance, and stiffness parameters fully define the dynamic response of the transition from one approach to another. Thus, in addition to finding evidence for the six enablers, the case study also found evidence for the three parameters size, resistance, and comfort level (stiffness).

Size

The size of the entity is related to organizational "momentum" as the entity moves from one C2 approach to another. The entity gathers momentum when a change in the situation forces a new required C2 Approach and the leader directs the entity to adopt the new required C2 Approach. The entity begins to move at a certain speed towards the new approach. Resisting and restoring forces may slow the transition such as broken technology or wanting to return to a comfortable approach. Just before the organization reaches the required approach, the entity takes the necessary measures to converge onto the required approach and, in effect, reduces its momentum. Conceptually, a large organization would have long start up and braking phases while a small organization could make quick momentum shifts.

It was hypothesized that the size of collective could be determined by the number of people, resources, equipment, infrastructure, and finances. Personnel, infrastructure, resources and equipment, and funding were analyzed in order to investigate the collectives' size. These dimensions were analyzed in the case study.

The size parameter becomes important for agility if 1) comparing across events or 2) size changes thus changing the resisting force (an increase in size contributes to the resistance). There will be an opportunity to compare the Munich Olympics with the Vancouver Olympics in the next report. However, there was evidence of the security collective growing in the Munich Olympics. For example, the Israelis provided two people for the crisis management team. However, as one can imagine, there were trust issues that contributed to the resistance.

Resistance

Resistance (high, medium, or low) represents factors that impede the movement from one C2 Approach to another – while in motion (e.g., broken information technology, bureaucracy, policy, weather, different traditions, cultures, lack of trust, etc). Resistance factors were identified and included; lack of trust, legal constraints, individual and organisational traditions and cultures, and limited resources and inappropriate/poorly/non-functioning equipment. These four factors are discussed in detail in the following sections.

Trust

The data was analyzed for trust issues within the collective. It was identified that Manfred Schreiber did not consider the work of the Police Psychologist to be important or beneficial (2 & 4), the Crisis Committee had very little trust in the Arab negotiators (4) and the Israeli Government had very little trust in the German Government to handle the crisis situation (1 & 5). This data suggests that the level of trust between the entities within the collective was very low.

Trust in economic and organisational theory is the most efficient mechanism for governing transactions with high levels of trust benefiting both individual members of the collective who maintain trust relationships with one another, and the collective as a whole (Gavrieli and Scott, 2005). Critically, organisations with high levels of trust can take advantage of increased cooperation, coordination, control, and overall effectiveness.

Gavrieli and Scott argue that a major factor that emerges as an enabler of knowledge flows, especially in dynamic environments such as those in which Edge organizations operate, is trust. While trust holds great promise in enabling knowledge flows in Edge organizations, it is very challenging to achieve. Gavrieli and Scott cite two major findings that emerge from their review of the social psychological literature on trust. The first is that trust is a history-dependent process (e.g., experience of working together), and the second is that homophily (e.g., shared values, status, culture) tends to breed trust.

Thus, the two conditions necessary for trust – history and homophily – were most likely missing from the Munich collective because the individuals and units were not able to develop long acquaintances that are necessary for trust development, and cultural diversity (e.g., across federal and provincial lines, and international partners and organisations) and functional diversity (e.g., across technical fields or specialist specialisations) was readily apparent by the manner in which members of the collective behaved. Furthermore, it could be inferred that this low level of trust actually equated to a high level of resistance within the collective. This high level of resistance within the collective may have hindered the collective's ability to transitioning quickly and effectively into another GM approach.

Legal Constraints

Legal constraints may have played a significant role in the collectives' agility. Internal (federal versus provincial) and external (Germany versus Israel) battles of German jurisdiction during the hostage disturbance is evidence for the resistance placed upon the entities within the collective. This evidence clearly identifies that such legal constraints placed upon the entities within the collective was a resisting force that affected the collective's ability to transition quickly and effectively into a more appropriate GM approach.

Traditions and Cultures

There was sufficient evidence to suggest that the collective experienced several resisting forces prior to and during the disturbance. Evidence of resisting forces include; attitudes towards terrorism, Germany's guilt of past war crimes and now failure to protect Israelis during the Olympic Games, political personalities and agendas and, IOC stubbornness. It can be inferred that due to the nature and extent of such resisting forces placed within the collective, the collective's ability to transition effectively and efficiently between GM Approaches was detrimentally affected by the traditions and cultures of individual entities (i.e. IOC, German and Israeli governments).

Resources and Equipment

Evidence suggests that the equipment available to the security team (e.g., lack of walkie-talkies, weapon sights, helmets and telescopic weapon sights) was insufficient during the initial hostage disturbance as well as at the Fürstenfeldbruck airfield. Having insufficient equipment (especially communications equipment at Fürstenfeldbruck) was another resistive force acting on the collective and making it more difficult for the collective to transition to the appropriate GM approach required by the situation.

Stiffness (Comfort Level)

The stiffness of the collective was investigated to determine whether the entity exhibited low stiffness (comfortable with any number of approaches), medium stiffness, or high stiffness comfortable with only one approach). Evidence found was divided into the first four phases of the event.

Phase 1: Pre-disturbance

The situation complexity was categorized as low, pre-disturbance, and the GM effectiveness was deemed to be good requiring a Coordinated GM approach based on the analysis. However, the data suggests that the collective was initially operating within an Independent GM approach. The evidence also suggests that the collective may have been working with "a false sense of security" (4) blinding the collective from identifying the need to plan for and practice a transition into the required Coordinated GM approach if the complexity of the situation demanded. Thus, the collective felt most comfortable at independent GM approach.

Phase 2: Hostages in Apartment

The situation complexity was categorized as medium while the disturbance was situated in the Olympic village apartments, and the GM effectiveness was deemed to be poor requiring a Coordinated GM approach based on the analysis. The data suggests that the collective was operating within a de-conflicted GM approach, outside of its neutral and thus uncomfortable position. It can be inferred that since the collective was already working outside of its comfortable GM approach, they were less inclined to deviate farther from their most comfortable GM approach, hindering their ability to transition into the Coordinated GM approach required.

Phase 3: Apartment to Airfield Move

The situation complexity was categorized as high, during the move to the airfield, and the GM effectiveness was deemed to be very poor. Based on the analysis it was determined that the situation

required at a minimum a Coordinated GM approach while the data indicated that the collective was operating within an Independent or Conflicted GM approach, suggesting a very "uncomfortable", and ineffective, position. As the collective was working outside of most comfortable GM approach position, it can be inferred that they were less likely to deviate farther and be able to transition to the required higher-level Coordinated GM approach.

Phase 4: Airfield Take-down

The situation complexity was categorized as very high during the airfield take-down, and the GM effectiveness was deemed to be non-existent. This situation required at a minimum a Collaborative GM approach based on the analysis. Testimonies as to the police feeling "paralyzed" (5) and evidence identifying how "out of control" (5) the hostage crisis had become during the final phases of the disturbance, suggests that the collective was operating in an extremely uncomfortable, and ineffective, position within an even greater autonomy driven GM approach called Anarchic (5). As the collective was working outside of their most comfortable GM approach position, it can be inferred that they were less likely to deviate farther and be able to transition to the required higher-level Collaborative GM approach.

What C2 Approaches were relevant? (How can C2 Approach Agility be inferred from what was reported or observed?) Did C2 Approach change, either for a collective, organization, team or one or more individuals?

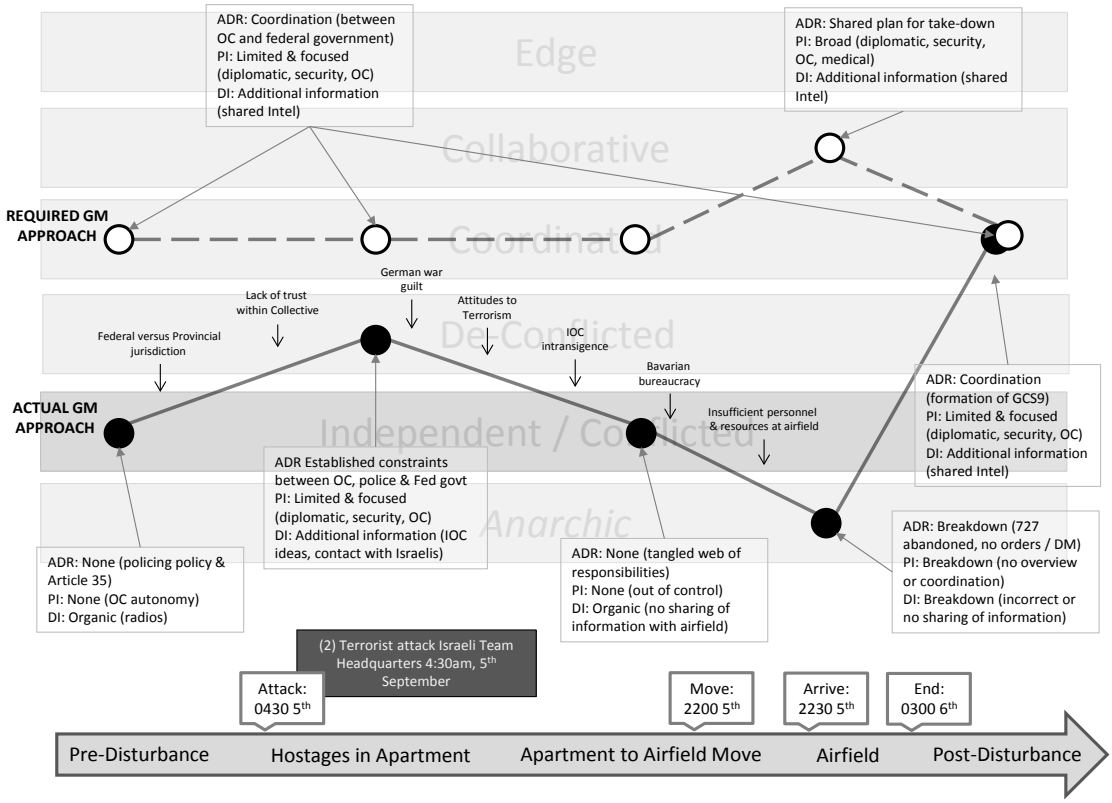


Figure B.6.4: Actual and Required C2 Approach plotted for each time phase.

Figure B.6.4 provides an excellent summary of these questions. The white dots represent the required C2 Approach over time while the black dots represent the actual C2 Approach for the collective. The required C2 Approach positions are roughly based on the complexity of the situation, while the actual C2 Approach positions are the analysts' best guess of the values of ADR, DoI, and PoI at a given point in time. Given that C2 Approach Agility is the transition from one C2 Approach to the required C2 Approach, one may conclude from this figure that the collective was not agile except after the event where detailed postpartum was conducted from which policies were developed not only in Munich but for all Olympic games and major sporting events.

What interesting and important vignettes are included or can be derived from the case study to help create illustrative stories?

The case study analysis was divided into primarily 5 phases or vignettes. Within each phase, one could identify, for example, ADR, PoI, and DoI. But it is only in the context of how these variables change over time can one make any assessments about C2 Approach Agility. In terms of the six enablers, there are key vignettes that highlight a particular enabler (see report). For example, when the Crisis Management Unit (CMU) botched the sniper attempt at the Apartment as it was broadcast on television, the CMU was able to regroup and come up with an alternative plan. This showed signs of resilience and flexibility.

Case Study Assumptions and Limitations:

a. **What constraints did you encounter that might limit the case study or the evidence supporting it?**
    1. The source materials do not talk in the language of SAS-085. Therefore there was a heavy reliance on the analysts to translate media terminology into agility terminology.
    2. There was no evidence for agility. In fact, one might say there was evidence for the lack of agility. Thus, one should have asked the question in this case what were the inhibitors.
    3. The collective (unit of analysis) was/could not be clearly identified.
    4. The Olympic case studies focused on the movement from region to region within the C2 Approach Space, and not the agility within a single region.
b. **What assumptions did you make when carrying out or documenting the case study?**
    1. Assumed a fairly linear relationship between the complexity of the situation and the required C2 Approach.
    2. Assumed that 1972 technologies and infrastructure could support all the approaches up to Edge. We know that this assumption is not true. With only radio technology and relatively long delays in distribution of information (compared to 2011 capabilities), one would hazard to guess that coordinated C2 would be the best one could hope for.

X: Conclusions

c. **This is not a summary – that is in the Executive Summary**

d. Conclusions relate to the purposes of the case study

a. Enablers, Constraints, and Behaviors identified

Constraints to agility included attitudes about the games (supposed to be the friendly games, no terrorist event could ever happen at the Olympics), significant mistrust due to atrocities of WII, ambiguous communications, information kept close hold.

b. Language – Clarity and Definitions

Conflicted C2 did not sufficiently describe the origin of the Approach Space. Non-conflict, conflict, as well as anarchy were observed at the origin. The notion that edge and anarchy look similar provided a lot of food for thought.

Patterns of Interaction anchors need clarification. It was helpful to change from "tightly constrained" to "completely constrained" as the complete opposite of "unconstrained".

c. Applicability of the SAS-085 Concepts and Model

Although SAS-085 Concepts and Model are still in flux, the agility definition does talk about the dynamic transition from one C2 Approach to another, and this case study focuses on this aspect of agility.

The evidence does not produce any further insights into the circular nature of agility and the six enablers. It would be useful to go over the case study, but this time ask the question in reverse in terms of inhibitors to agility.

d. Statements about Validity

There was evidence to show the existence of a C2 Approach Space with dimensions ADR, DoI, and PoI. This is vitally important in order to be able to identify and track the C2 Approach over time.

There was evidence to legitimize the size, resistance, and comfort level concepts. However, it is difficult to say definitively the impact of these three parameters on the time evolution of the actual C2 Approach. One expects that a controlled experiment is needed to discover this impact.

There was no evidence to determine the relationship between agility and the six enablers primarily because of the lack of agility by the collective.

Bibliography

Alberts, D. S., & Hayes, R. E. (2003). *Power to the Edge: Command...Control...In the Information Age*. Washington, D.C.: CCRP Publication Series.

Banbury, S., Kelsey, S. R., & Kersten, C. (2011). *Evaluating C2 Approach Agility in Major Events: Final Report* (CONTRACT #: W7714-083663/001/SV No. DRDC CR 2011-004). Scientific Authority Dr. Philip S. E. Farrell. Centre for Operational Research and Analysis (CORA), Ottawa, Ontario, Canada: Defence R&D Canada.

Farrell, P. S. E. (2011). *Organizational Agility Modelling and Simulation*. Paper presented at the 16th International Command and Control Research and Technology Symposium: Collective C2 in Multinational Civil-Military Operations. Quebec City, Canada.

Farrell, P. S. E., & Connell, D. (2010). *Organizational Agility*. Paper presented at the 15th International Command and Control Research and Technology Symposium: The Evolution of C2.

SAS-065. (2010). *NATO NEC C2 Maturity Model Overview*. Paris: NATO RTO. CCRP Publication series.

B.7 Vancouver Olympics Case Study

Data Sources

This section describes the data sources that were used to conduct the evaluation of the C2 Agility model:

Based on availability and classification, the following eight reports were used as a basis for evidence in this analysis:

- 3350-1 (DCOS ops) (August 2010). *Canada Command Joint Task Force Games Post-Operations Report – Op PODIUM*.

- Smith, D. G., Genik, L., & Maceda, G. E. (2010). Command and control analysis of the South West Provincial Regional Emergency Operations Centre during Vancouver 2010. *Proceedings of the 16th International Command and Control Research and Technology Symposium*, Québec City, Canada.

- Smith, D. G. & Maceda, G. E. (2010). *Strategies for ad-hoc data collection and analysis during major event interagency exercises and operations*. Paper presented at Knowledge Systems for Coalition Operations 2010, Vancouver, Canada.

- Goodwin, G. F., Essens, P. J. M. D., & Smith, D. (2011). Multiteam systems in the public sector. In S. J. Zaccaro, M. A. Marks, & L. DeChurch (Eds.), *Multiteam systems: An organization form for dynamic and complex environments* (Part I: Introduction). New York: Routledge Academic.

- Smith, D., McLellan, L., & LCol Hobbs, D. (2010). *Cultural differences between the Canadian Forces and the Royal Canadian Mounted Police*. Paper presented at the NATO Workshop on Collaboration in a Comprehensive Approach to Operations, Toronto, Canada.

- Billyard, A. & Collin, I. (2008). *Vancouver 2010 Olympics – Identifying CF communication issues associated with the CH-146 acting as an interceptor* (Secret). Defence R&D Canada – CORA TM 2008-064. Ottawa, Canada.

- Carson, N., Caron, J., & Bourdon, S. (2010). *Vancouver 2010 Winter Olympics – A spatial and temporal analysis of the asymmetric air threat* (Secret). Defence R&D Canada – CORA TR 2010-119. Ottawa, Canada.

- Carson, N. & Caron, J. (2010). *Vancouver 2010 Winter Olympics – Intercept and engagement platform option analysis* (Secret). Defence R&D Canada – CORA TM 2010-118. Ottawa, Canada.

Identify the Focus of and the Boundaries for the Case Study

p. What is the level of analysis? (e.g. Individual, Team, Organization, or Collective)

The Collective

The level of analysis was defined similarly to the Munich Olympics for ease of comparison to be at the organizational level. However, unlike the Munich Olympics, the organizations within the ISU remained fairly constant.

q. Who or What Organizations are included in the case study? (e.g. the Collective responding to the Haiti Earthquake Crisis, Air-Ground Control Strike Teams in Iraq and Afghanistan)

The ISU for V2010 was led by the RCMP and was comprised of the following organizations:

- RCMP
- CF
- Vancouver Police Department
- West Vancouver Police Department

Several liaison officers were also employed in the ISU to coordinate with other organizations or teams not included in the ISU (e.g., NORAD, Public Safety Canada, Emergency Management B.C.) but these outside teams were not considered part of the ISU.

r. What temporal boundaries are included?
   a. When does the case begin and end?
   b. Are there phases involved? If so, what are their boundaries?

The analysis reported in the present document focuses on the 2010 Vancouver Olympics. In February and March 2010, the city of Vancouver, British Columbia hosted the Olympic and Paralympic Winter Games (V2010). The Vancouver Organizing Committee for the 2010 Olympic and Paralympic Winter Games (VANOC) led Games operations, the Integrated Security Unit (ISU) led security operations, and Emergency Management British Columbia (EMBC) lead public safety operations.

The present analysis focused specifically on the ISU in charge of security for V2010. The RCMP was tasked as the lead organization in providing security during the Games. Considering the magnitude of the operation, security efforts involved multiple entities in charge of different aspects of security, including several municipal and provincial police forces, civilian government departments, and the Canadian Forces (CF).

Organizations involved in providing security for major operations are faced with many challenges that stem from the need to coordinate the activities of multiple supporting organizations and the necessity to be prepared and ready to respond quickly to a variety of incidents. In order to achieve their goal and maintain an adequate level of security, these organizations must display agility and adaptability to changes and unexpected events.

Therefore, the V2010 ISU constitutes an interesting and valuable focus for analysis evidence of GM Approach agility, as it involves a well-defined collective in charge of security for a major international sporting event.

As complex endeavours take place in dynamic environments, more than one GM Approach might be required throughout the course of a given endeavour. (Banbury, Kelsey, & Kersten, 2011) proposed that complex endeavours have three main phases: before the event, during the event, and after the event. If significant disturbances occur during the event, one can further decompose this phase into just before the disturbance, during the disturbance, immediately after the disturbance. Each phase and sub-phase may require different GM Approaches, depending on the time evolution of the situation complexity. An agile collective should be able to transition from one GM Approach to another as required, so as to cope with disturbances and achieve mission success.

During phase 1 – before the event – the collective is likely to engage in learning and/or anticipatory behaviours (or control methods). These methods aim to help the collective reach, maintain, and be comfortable with the ADR, DoI and PoI values of the GM Approach(es) required for the event.

Learning methods can take such forms as training, exercises and education, while anticipatory methods could consists in contingency planning, mission analysis, etc. A larger question is whether the collective learned from previous events and improved their ability to transition to the required GM Approach.

Anticipatory methods are focused on planning and development rather than execution. Plans and contingency plans are developed based on the anticipated event, and therefore one can anticipate the Required GM Approach. It is important to note that if the collective anticipates incorrectly then Compensatory methods need to be deployed immediately in order to avoid any destabilization of the transition.

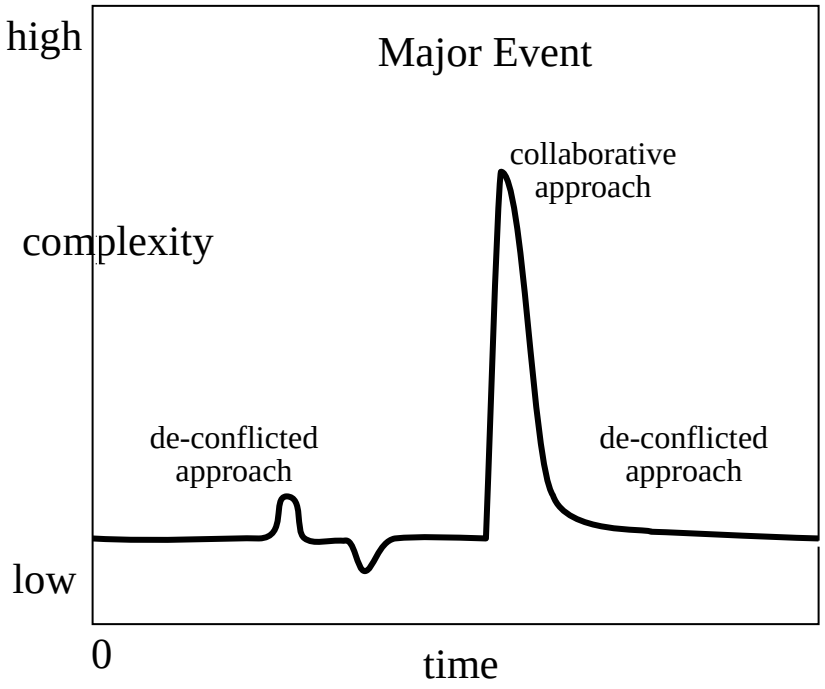


Figure B.7.1: Hypothetical Complexity Profiles for a Major Event

SAS-085 decided to characterize the case study complexity during each phase based on a set of the dimensions fully described in (David S. Alberts, 2011; SAS-065, 2010). For this case study, a single statement is made for each dimension and for each phase, and then the case study lead (as the SME for the case study) a single value (high, medium, low) that represents an aggregated judgement of the situation complexity level for that phase.

- Effects Space (PMESII, diversity (competency, cultural, values) of entities)
    - The ISU was designed to have direct lines to all PMESII elements in anticipation to incidents in any or all of these domains. The ISU exercised a wide variety of situations from the simple to the complex
- Dynamics (time pressure, stability)
    - This phase involved exercising and training. Time pressure and stability were tightly controlled.
- Uncertainty (predictability, familiarity)
    - White cell knew all injects, while the players were uncertain about when they would appear.
- Risk (likelihood, consequences)
    - NA
- Number of entities and their relationships
    - Very difficult to determine in an exercised situation.
- Cognitive Complexity (smart and not so smart adversaries, degree of intent)
    - Experimental control was intelligent.
- Therefore, complexity varied systematically from low to high during phase 1, in my judgement.

During phase 2, which takes place during the event, significant disturbances might occur that will change situation complexity, which will require shifting to a new GM Approach (Figure 1). In that case, the collective will adopt new values of ADR, DoI, and PoI, and potential changes in size and resistance might also take place. Assuming that the GM Approach adopted in phase 1 is the "comfortable" GM Approach, moving away from that approach may produce a restoring force causing organizational stress that pulls the collective away from the required GM Approach and back towards the comfortable GM Approach.

- Effects Space (PMESII, diversity (competency, cultural, values) of entities)
    - ISU collective involved an number of political, economics, social, and infrastructure effects, although the military was ready to respond if a military effect was needed. From this perspective the situation was quite complex.
- Dynamics (time pressure, stability)
    - Because the ISU had 3 years to plan, and the plan was executed on schedule without incident, the time pressure is deemed to be low and the situation was quite stable
- Uncertainty (predictability, familiarity)
    - Although there was continuous monitoring for the unexpected, events unfolded as predicted and practice.
- Risk (likelihood, consequences)
    - Information on Risk not available
- Number of entities and their relationships

    - It is difficult to determine the number of entities in the environment. It could be individuals, (1's) the Olympic Village (1000's), the city (100,000's), the country (10,000,000's). Only if an event occurred could there be a better idea of the number of entities. Otherwise,
- Cognitive Complexity (smart and not so smart adversaries, degree of intent)
    - They assumed the adversary was very intelligent with ill intent. Thus the situation could become complex quickly. However, there were no major incidents. Thus, the complexity was low.
- Therefore complexity was low during phase 2, in my judgement.

The GM Approach agility model posits that the collective can use various methods (entity behaviours) to move from one GM Approach to the next (Farrell, 2011; Farrell & Connell, 2010). During the second phase, these control methods can be:

- Compensatory: methods that aim to decrease the difference between the actual and the required GM Approach by monitoring the transition in real-time (i.e., feedback) and making real-time decisions based on the difference.
- Anticipatory: execution of the anticipatory measures planned in the first phase (e.g., contingency planning) as needed to reach the new GM Approach.
- Adaptive: methods that aim to adapt the parameters of stiffness and resistance over time.

It is during the second phase that the collective may display signs of robustness, responsiveness, resilience, and disturbance rejection. That is, the collective may show the "ability to maintain effectiveness across a range of tasks, situations, and conditions", "the ability to react to a change in the environment in a timely manner", and "the ability to recover from or adjust to misfortune, damage, or a destabilizing perturbation in the environment" (David S. Alberts & Hayes, 2003). If no significant disturbances occur, it is unlikely that any of these agility variables are observable.

Phase 3 takes place once the event is over. At that point, organizations comprising the collective should go back to an independent GM Approach posture unless they decide to continue to work together as a 'standing collective' and adopt a, say, coordinated GM Approach. The third phase is also an opportunity to learn for the next event.

- Effects Space (PMESII, diversity (competency, cultural, values) of entities)
    - With respect to the event, the parties dispersed and the situation was normal where everyday policy allows the individual entities to carry out their jobs in a de-conflicted matter. Occasionally there may be some coordination involved.
- Dynamics (time pressure, stability)
    - Time pressure and stability returned to normal everyday levels (low and stable).
- Uncertainty (predictability, familiarity)
    - Although there is uncertainty in everyday life, it is no more than normal.
- Risk (likelihood, consequences)
    - The likelihood of a high impact event is that of everyday life (which is less than when a major event is happening).
- Number of entities and their relationships

    - NA
- Cognitive Complexity (smart and not so smart adversaries, degree of intent)
    - NA
- Therefore complexity was low during phase 3, in my judgement.

s. Other boundaries (e.g. separate analyses of the collective and of specific organizations within the collective).

None

Describe the Challenge or Opportunity that gave rise to the need for C2 Agility.

As it turns out there was no significant safety and security event that required a need for agility. At the same time, the Government of Canada (GoC) considered the safety and security of the even a 'no fail' mission. We do see some evidence of agility in the 'storming, forming, and norming' phase 1 of the Olympics where complexity in self is high and mechanisms are put in place to reduce this complexity to manageable levels.

What would have been the consequences of a failure to act in a way that demonstrates C2 Agility?

Referring only to phase 1, the failure of not being able to reduce the complexity in self would be catastrophic.

Was C2 Agility Manifested? If so, How? (Be as clear and precise as possible, but keep this simple so that it does not require repetition in the next steps.)

Yes in phase 1, no in phase 2, and no in phase 3 although this is a trivial phase. For phase 1 the ISU collective was able to cope with the complexities related to "self". The ISU comprised of police and military organizations primarily. These two types of organizations have very different organizational cultures. For example, in a military construct the commander has significant responsibility and authority to make life and death decisions. Conversely for police organizations, the officer at the scene must react immediately and make key decisions on the spot. This aspect alone makes for a fairly complex situation on how C2 is conducted.

Which Enablers and Inhibitors of C2 Agility were observable? (Remember that the basic six may not be independent. Include discussions of the relevant Agile Behaviors, but try to tie them to one or more Enablers. Specify inhibitors that impacted C2 Agility)

Note that the definitions are quotes from SAS-065 which are quoted from (David S. Alberts & Hayes, 2003).

- Flexibility: "The ability to employ multiple ways to succeed and the capacity to move seamlessly between them."
    - No opportunity to observe flexibility during the event.
- Versatility (Robustness): "The ability to maintain effectiveness across a range of tasks, situations, and conditions."

    - There were indications of versatility as the collective was exposed to a number of vignettes during the exercise phase, as well as a few relatively minor incidents that did not require a change in C2 approach.
- Responsiveness: "The ability to react to a change in the environment in a timely manner."
    - No opportunity to observe responsiveness during the games, except during the exercises.
- Adaptiveness: "The ability to change work processes and the ability to change the organization."
    - No opportunity to observe adaptiveness
- Resilience: "The ability to react to a change in the environment in a timely manner."
    - No opportunity to observe resilience
- Innovation: "The ability to do new things and the ability to do old things in new ways."
    - No opportunity to observe innovation.

As with the Munich Olympics, it is difficult to make any correlation between agility and these six enablers since the collective did not show any signs of agility during the actual event. Unlike the Munich Olympics, there was no major disturbance requiring agility. All operations went to plan. If there was a need for these six enablers, it would have been during the pre-event phase. Certainly, ISU staff needed to be flexible as they worked with other members from very different work cultures.

(Farrell, 2011) provides an analogy between the transition from an initial approach to the required approach and a mass-spring-damper system that moves from an initial position to the required position. The transition model proposes three key parameters that enable/inhibit the dynamic transition between one C2 Approach and another (i.e., enable/inhibit C2 Agility): size (mass), resistance (resistance), and comfort level (stiffness).

Again, for the V2010 Olympics, there was no need to transition from one approach to another. In fact, it seems that a high-level decision was made to adopt a coordinated approach which was more than enough for the event. The collective size remained relatively constant. The resistive elements (policies, technical problems, etc.) were pretty well minimized during the pre-event phase. The collective became comfortable with a coordinated approach after 3 years of exercising, which would lead one to believe that the stiffness parameter was fairly high. Any excursion away from coordinated would likely meet with significant restoring force back to coordinated.

What C2 Approaches were relevant? (How can C2 Approach Agility be inferred from what was reported or observed?) Did C2 Approach change, either for a collective, organization, team or one or more individuals?

Figure 2 provides a summary of the approaches' position during each phase. It is constructed from the inferred values. That is, the source documents do not use the same language that is found in (SAS-065, 2010) that describes the Approach Space and the three key dimensions: Allocation of Decision Rights (ADR), Patterns of Interaction (PoI), and Distribution of Information (DoI). Furthermore, the analysts felt much more comfortable using the more generic descriptions of the approaches found in pages 52 – 63 in (SAS-065, 2010) in order to make a judgment on naming the approach based on the evidence found in the source documents. Nevertheless, this is a powerful result confirming the notion of movement within the GM Approach space. It also produced a new notion of the Desired GM Approach is a key driver (forcing function) for this transition.

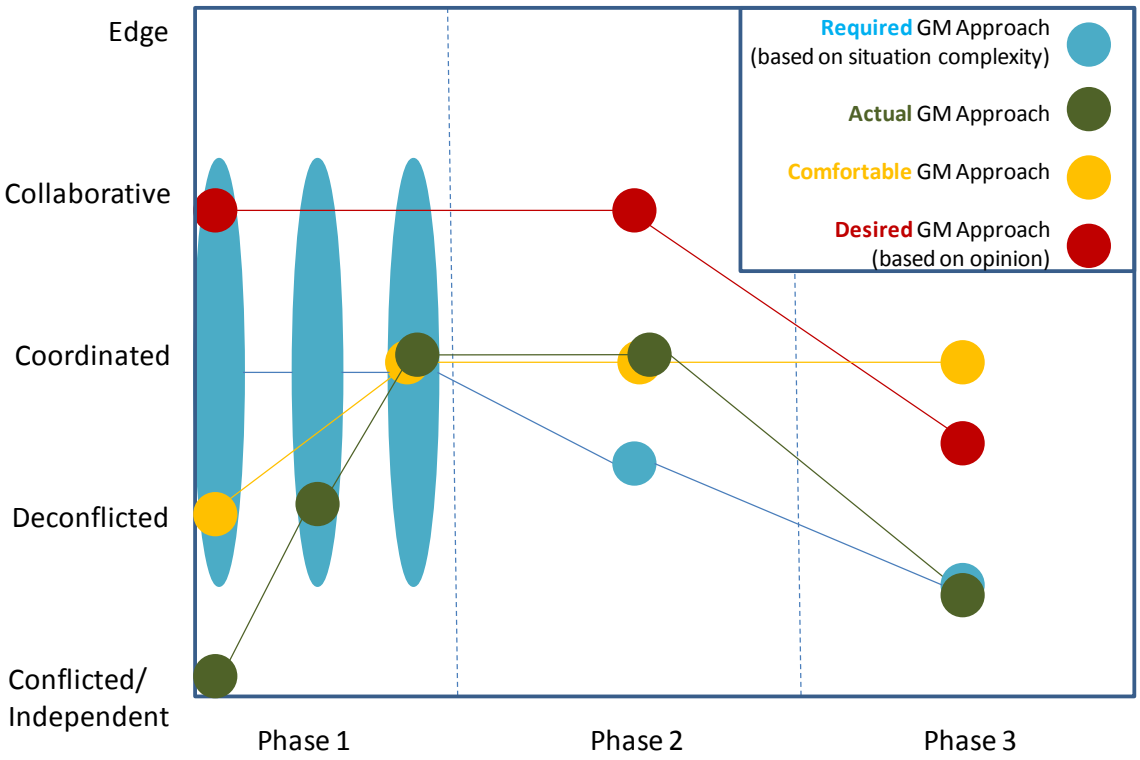


Figure B.7.2: Required, Actual, Comfortable, and Desired GM Approaches over time

What interesting and important vignettes are included or can be derived from the case study to help create illustrative stories?

The case study was divided into 3 phases as described earlier. Phase 1 was important in understanding the notion of Desired Approach and the willingness for governments to insist on an 'overmatch' approach at any costs for 'no fail' missions.

Case Study Assumptions and Limitations:

c. What constraints did you encounter that might limit the case study or the evidence supporting it?

5. The source materials do not talk in the language of SAS-085. Therefore there was a heavy reliance on the analysts to translate media terminology into agility terminology.
6. There was no major disturbance that required agility. Therefore the concepts that the analysts could find evidence for was limited.
7. The Olympic case studies focused on the movement from region to region within the C2 Approach Space, and not the agility within a single region, although coordinated, collaborative, and edge approaches inherently have elements of the six enablers (flexibility, responsiveness, etc.).

d. What assumptions did you make when carrying out or documenting the case study?

3. Assumed a fairly linear relationship between the complexity of the situation and the required C2 Approach.

4. Assumed that the relationship between C2 Approaches and ADR, PoI, and DoI is completely described in Table 15 on page 64 of (SAS-065, 2010).

Conclusions

e. This is not a summary – that is in the Executive Summary

f. Conclusions relate to the purposes of the case study

a. Enablers, Constraints, and Behaviors identified

A key enabler was the government of Canada providing direction that the security for the V2010 Olympic games was to be a 'no fail' mission. A key constraint was forming the ISU with two (and more) very different organizational cultures, predominately a military culture and a police culture.

b. Language – Clarity and Definitions

Conflicted C2 did not sufficiently describe the origin of the Approach Space. Before and after the event, organizations carry out missions independent of each other without being in conflict. At best, their roles and responsibilities are de-conflicted by government legislation. Thus, they are de-conflicted from a government perspective, but independent from the ISU perspective.

The analysis yielded a new term/modifier for C2 Approach: Desired C2 Approach. This approach is typically dictated by the collective leadership. It is preferable if the desired and required C2 approaches match to minimize any tension within the collective.

c. Applicability of the SAS-085 Concepts and Model

Although SAS-085 Concepts and Model are still in flux, the agility definition does talk about the dynamic transition from one C2 Approach to another as well as higher C2 Approaches being more agile than lower ones. This case study supports the transition notion but does not provide any further insight regarding higher approaches being more agile.

d. Statements about Validity

The case study sought evidence for a number of concepts/variables associated with C2 Agility. Figure B.7.2 summarizes the analysis across all three phases. A check mark means that a reference was found that supports the concept. Two variables – Required Approach and Comfortable Approach are inferred to exist based on knowledge of the situation. If the right column is left blank, then the analyst did not have any evidence nor felt comfortable in making a judgment.

Even harder for the analyst was to infer values for each of the concepts/variables. This met with extreme reluctance because the language of SAS-085 simply was not part of the vocabulary of the source documents. Some documents used the word "coordinated" or "collaborative" but not in the context of C2 Approaches necessarily. One way of finding values for the variables is through an interview/survey activity (not part of the scope of this work). The interviewer may expose the SME interviewee to the SAS-085 lexicon, and then ask them to comment on concepts and their values.

Figure B.7.2: Evidence for Concepts Summary

Concept	Evidence?
Required GM Approach	inferred
Desired GM Approach	√
Comfortable GM Approach	inferred
Actual GM Approach	√
Allocation of Decision Rights	√
Distribution of Information	√
Patterns of Interaction	√
Size	√
Resistance	√
Stiffness	
Compensatory	
Anticipatory	√
Adaptive	
Learning	√

Note that there was no evidence for the collective having a compensatory behaviour. However, (Farrell, 2011) argues that compensatory is a fundamental behaviour required to transition from one approach to another. In phase 1, one could infer (not from any source document) that the ISU understood that most ISU members were coming from organizations that rarely if at all worked with each other (Independent actual approach), and that they needed to at least train together in order to achieve the desired collaborative approach. They proceeded to plan and practice together over 3 years to achieve the target approach. This, in fact, is a compensatory behaviour.

In phase 2 during the event, there was no need for compensatory behaviour because the collective chose to maintain Coordinated throughout the event, and no disturbance was large enough to require a transition to Collaborative or Edge. During phase 3, the compensatory behaviour was trivial as organizations returned to their pre-Olympics natural and stable posture (somewhere between independent and de-conflicted.

Bibliography

. (2011). Retrieved from http://www.cyberconflict.org/

Alberts, D. S. (2011). *The Agility Advantage: A Survival Guide for Complex Enterprises and Endeavors*. Washington, D.C.: CCRP Publication Series.

Alberts, D. S., Garstka, J. J., & Stein, F. P. (2000). *Netwrk Centric Warfare - Developing and Leveraging Information Superiority*: CCRP.

Alberts, D. S., & Hayes, R. E. (2003). *Power to the Edge: Command...Control...In the Information Age*. Washington, D.C.: CCRP Publication Series.

army, c. (Producer). (2011). Retrieved from www.carlilse.army.mil

Banbury, S., Kelsey, S. R., & Kersten, C. (2011). Evaluating C2 Approach Agility in Major Events: Final Report (3 ed.). Scientific Authority Dr. Philip S. E. Farrell. Centre for Operational Research and Analysis (CORA), Ottawa, Ontario, Canada: Defence R&D Canada.

Enisa (Producer). (2011). enisa europa. Retrieved from www.enisa.europa.com

Farrell, P. S. E. (2011). *Organizational Agility Modelling and Simulation*. Paper presented at the 16th International Command and Control Research and Technology Symposium: Collective C2 in Multinational Civil-Military Operations. Quebec City, Canada., Quebec City, Quebec, Canada.

Farrell, P. S. E., & Connell, D. (2010). *Organizational Agility*. Paper presented at the 15th International Command and Control Research and Technology Symposium: The Evolution of C2, Santa Monica, US.

The free dictionary. (2013). Retrieved from http://www.thefreedictionary.com/

Moffatt, J., & Alberts, D. S. (Dec. 2006). Maturity Levels for NATO NEC Command.

PCMag.com. (2013). Retrieved from http://www.pcmag.com/encyclopedia_term/0,2542,t%3DHTTP&i%3D44501,00.asp

SAS-065. (2010). NATO NEC C2 Maturity Model Overview. Paris: NATO RTO. CCRP Publication series.

Small Wars Journal. (2013). Retrieved from http://council.smallwarsjournal.com/

Software Updates. (2013). Retrieved from http://longmilecomputers.ie/IE/software_update.html

Thomas, T. L. (2010). RUSSIAN INFORMATION WARFARE THEORY:THE CONSEQUENCES OF AUGUST 2008 *THE RUSSIAN MILITARY TODAY AND TOMORROW:ESSAYS IN MEMORY OF MARY FITZGERALD* (pp. 282).

Wikipedia (Producer). (2013). Wikipedia, the free encyclopedia. Retrieved from http://en.wikipedia.org/wiki/Botnet

B.8 Battlespace Helmand Case Study

Executive Summary

a. Focus and Boundaries

Military C2 organizations and structures involved in conducting warfighting operations in Helmand, Afghanistan, faced with many challenges that stem from the need to coordinate the activities of multiple supporting commands and assets and the necessity to be prepared and ready to respond quickly to a variety of incidents in a counter insurgency (COIN) environment. In order to achieve their objective in terms of desired effects and maintain an adequate level of security, these organizations must display a high degree of agility, and adapt to changes and unexpected events characteristic of a complex battlespace. Lives depend on it daily.

On the time and space continuum this study examines data collected from a specific NATO/ISAF battlespace in the Upper Gereshk Valley (UGV), Helmand Province, Afghanistan from August 2010 to January 2011, and area of responsibility belonging to Task Force Helmand (TFH.) It involves a variety of specific military commands and sub-commands operating within this battlespace with primary focus on a Danish Battlegroup (DK BG) and its five Component Commands (CCs), as well as five Special Operations Forces (SOF/SF) of different varieties operating in the same battlespace. This includes mentored Afghan SOF units as well as Coalition Forces (CF) SOF units.

b. Challenge or Opportunity for C2 Agility

The Battlespace Helmand study constitutes an interesting and valuable study for finding evidence of C2 Agility as it involves a real time battlespace and clearly delineated C2 structures for measurement, assessment, and reference, in a high-speed, high risk, complex environment over a sustained period of time. Through a framework of hierarchal C2 vs. informal networked C2, the case provides very good examples of the role bureaucratic norms imbedded in conventional C2 organization play in promoting or inhibiting the development of operational agility.

c. Was Agility Manifested? If so, How?

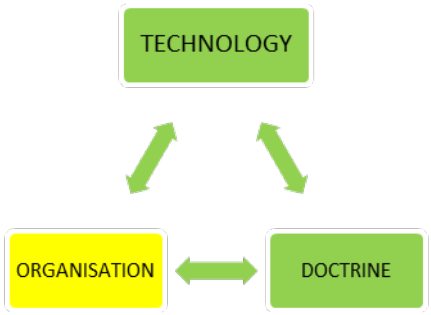
Agility manifested itself distinctly in the case study through a bottom-up driven adaption of information sharing and planning processes through the development of an *informal networked collective* to increase situational awareness and understanding of the COIN battlespace. As the ability to manage the complexity in a timely manner increased, the ability to take the correct actions in a timely manner increased. This was interpreted as an indication of the emergence of organizational agility in the battlespace. Furthermore, the case study provided some very key insights into the dynamics behind the development of organizational agility and the challenges in transitioning to an agile organization from the standpoint of a conventional warfighting organization.

d. Enablers and Inhibitors of C2 Agility

Alberts and Hayes (2003) provide definitions for six enablers for agility: flexibility, resilience, versatility (formerly robustness), responsiveness, adaptiveness, and innovation. The framework of this study has its origins planted solidly on the foundational works of Albert and Hayes agility research, but was developed specifically to fit the Danish focus on sensemaking (intelligence) within a military organization engaged in warfighting in a complex battlespace. In this regard, a delineation of agility was determined for the field study under the Danish Defence

project designation *Kitae*[14]. A working definition of battlespace agility was developed specifically in line with the operational planning philosophy used by NATO in Helmand, known as effects based thinking (EBT), and the conversion of knowledge to actions for desired effects in the battlespace. Battlespace agility was then defined for the study as the speed at which the organization turns knowledge into actions for desired effects. (Necessity for *speed* identified directly in the definition while the necessity for precision and appropriate actions to the situation is reflected in the production of *desired* effects.) This delineation allowed for sensemaking variables from NATO SAS-050 such as information richness, information currency, and information accuracy to be used to reference improvements in battlespace agility (as defined above) over the 6 month study period. For the purposes of this project to directly support NATO SAS-085, an assessment has been undertaken to assign the various issues identified within the battlespace agility framework to the appropriate agility enabler as defined in NATO NEC C2 Maturity Model. It is with great confidence, due to the concrete processes behind the targeting cycles used for our own "intelligence" focused battlespace agility assessment, that this study can present some key insights with respect to the established enablers and inhibiters of C2 agility in question. From the Danish side, this study placed the results of battlespace agility within a Danish military framework for understanding a military in balance with itself, where technology, doctrine, and organization must be in synch with each other. For example, the model applied in its simplest understanding would allow one to ask "*What element of the triadic model is currently most inhibiting to agility*?" In this case the answer was clearly '*organization'*.

Figure b.8.1: Danish Triadic Model for Effective Warfighting



Royal Danish Defence College, KITAE I, 2012

e. Summary of Observations/Conclusions about C2 Approach Agility

There was a clear progression of the C2 approach through the six-month period. After the official collective failed to respond sufficiently to the complex environment in phase 1, and phase 2, it began to sub-divide into two C2 collectives for warfighting in the AO by phase 3. Here we experienced the emergence of an *informal networked sub-collective* responding effectively to the complex environment, while the official general collective C2 became increasingly irrelevant. As the C2 approach related to the *informal networked sub-collective* driving the targeting matured, it incrementally assumed more independence from the official C2 collective of the conventional BG C2 organization. The *informal sub-collective* progressed steadily from phase 3 to phase 6 with increasing agility, evaluation in the language of NEC works fine here – as does the 50 odd variables from SAS 050 to assessment of allocation of decision rights and information sharing. However, as the anchoring of observations in the formal targeting processes will show, one can describe the progression of the *informal*

[14] Japanese: Art of forming the sword blade.

networked sub-collective as independent than one would have explain the C2 approach progression from the point of view of the *official collective* C2 becoming incrementally irrelevant. However it was as if a new specialized organization, facilitated by flat-lining technologies, within an organization began emerging where issues concerning the delegation of authority were resolved after the principle of '*having an effect*.' (Calling it a sub-organisation is somewhat misleading as it included authorities not in the official collective C2 organisation)

f. Important stories or vignettes in the case study.

(1) Realtime vs. Organizational: In terms of optimality within an EBT context, the hierarchical structure was having a significant negative effect on the conversion of 'knowledge to action' processes both in terms of timeliness and quality. The most extreme example from this period was a real-time video showing an explosives cache being buried in a field a relatively short distance from a main operations base. Though perfectly located for a quick reaction force pick-up and neutralization, dealing with the explosives cache was turned into a required 17-day 'concept of operations' process that resulted in nothing except angry local farmers demanding compensation for fields which had been torn up by a plethora of heavy vehicles.

(2) Deliberate vs. Current Ops: The vast majority successful targeting was carried out within the context of framework or current operational planning and not cyclic deliberate planning. As agility developed in the AO through informal networked C2, it perpetuated more agility until capacities were reached for actions and prioritization of targets (kinetic/non-kinetic became the main challenge.

(3) Freedom of movement understandings on one self and well as the enemy forces is an essential element of both being agile and understanding how agile one must be. What took 4 hours for armored conventional forces to travel due to TTPs, took enemy forces 35 minutes on a motorcycle.

(4) Conventional battlespace topographical division's vis-à-vis organization a structure had a very negative impact on warfighting agility for the organization. As the enemy forces did not have the same geographical divisions as the BG, the tendency to ignore some outside of you designated battlespace was great. In this regard, the enemy forces could move across hundreds of kilometres in a matter of an hour or two, while the conventional component command formations could not move over respective battlespace lines without great bureaucratic burden. One example was an insurgent who commuted 17 km every day to place IEDs in one ISAF battlespace – while he stayed quiet around his home two battlespaces away – and therefore was not recognized as an insurgent by that battlegroup.

Identify the Focus of and the Boundaries for the Case Study

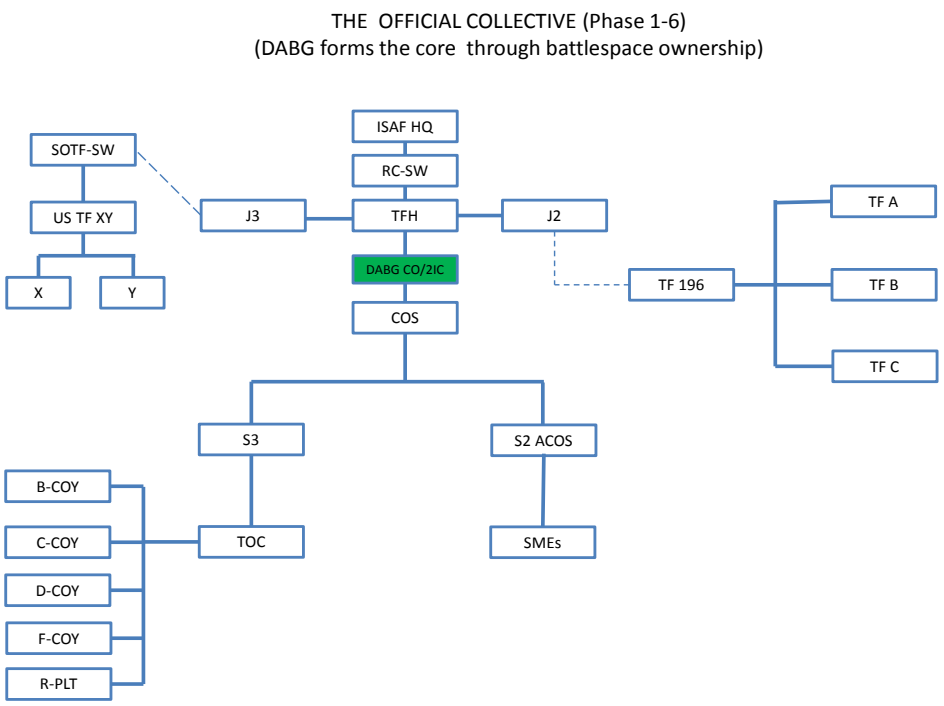
a. What is the level of analysis?

The official collective C2 level is reinforced Battlegroup, warfighting (**not** a provincial reconstruction team - PRT) for 6 months in Helmand, Afghanistan.

b. Who or What Organizations are included in the case study?

- North Atlantic Treaty Organisation (NATO)
- International Stability Assistance Force (ISAF)
- Task Force Helmand (UK)
- Danish Battlegroup (DABG) and Component Commands
- Combined Joint Special Operations Task Force (US & ISAF)

Figure B.8.2:- Official Targeting C2 Collective



Royal Danish Defence College 2012

c. What temporal boundaries are included?

a. When does the case begin and end?

The case begin in August, 2010 and ends in January 2011.

b. Are there phases involved? If so, what are their boundaries?

The MoEs are tied *directly* to the *targeting cycles* of the BG/SOF/SF and assessed at the end of each month. Therefore each month is a phase. The geographic battlespace remained the same for all 6 phases, and there were no changes to the official AO. Only a generic geographical representation of the AO is presented below as it could not be an intervening variable in itself as it remained the same for all phases and specific grid references would be classified.

d. Other boundaries (e.g. separate analyses of the collective and of specific organizations within the collective).

The informal sub-collective developed steadily from phase 3 to phase 6 with increasing agility, so in this sense the results of the informal sub-collective also belonged to the official collective. However this progression is in relation to being an effective targeting organisation as a sub-element of the official C2 organisation. If one does not wish to describe the informal networked sub-collective as 'independent' than one would have explain the C2 approach progression from the point of view of the official collective C2 becoming incrementally 'irrelevant'. Both approaches have implications beyond the scope of this reports focus and would need a comparative MoP analysis to determine what aspects of the official C2 collective organization were in fact needed to produce the more effective informal collective. (This is of course assuming that we cannot form an organization to be as effective as the informal collective from the start.) To further complicate the understanding of this relationship, the informal collective only developed as a result of the official collective inability to be effective. It was as if a new specialized organization, facilitated by flat-lining technologies, within an organization began emerging where issues concerning the delegation of authority were resolved after the principle of '*having an effect*.'

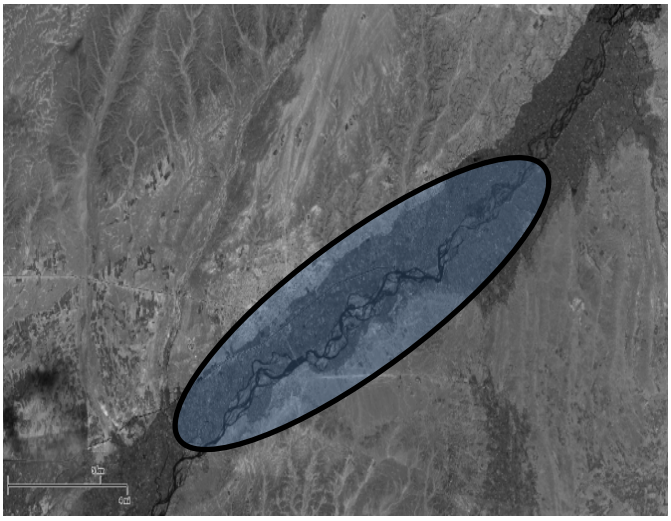


Figure B.8.3 Area of Operations (AO) Upper Gereshk Valley

Informal Networked Sub-Collective C2

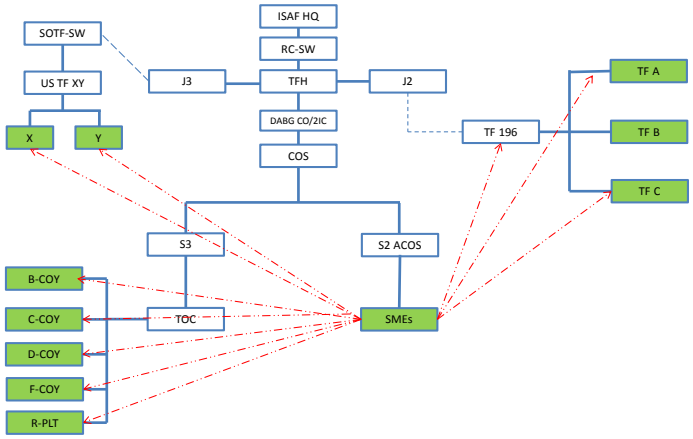


Figure B.8.4 Informal Targeting C2 Collective

Royal Danish Defence College 2012

Describe the Challenge or Opportunity that gave rise to the need for C2 Agility.

During the period of this study, the main objective for the Taskforce Helmand (TFH) was to promote the influence of the Government of the Islamic Republic of Afghanistan (GIRoA). This task was to be accomplished within and throughout one of the most violent and complex battlespace areas of Afghanistan (AFG), which involved mapping[15] and engaging the local nationals (LN).

It was apparent from the start that if the BG wanted to be able to engage and influence the local population, our freedom of movement (FoM) in the battlespace would have to be re-established. In short, a high degree of kinetic activity would be necessary to degrade the insurgent (INS) network to a sufficient degree so that the conventional forces/Afghan National Special Forces (CF/ANSF) could again engage and influence the local population. In summary:

The Commander's intent for the 6 months was to re-gain CF FoM in order to access the local population for human terrain mapping, and to set the foundation for expanding GIRoA influence.

The observations for this study are taken from daily warfighting activities in one of the most violent areas of Afghanistan (AFG), namely the upper Gereshk valley (UGV) in Helmand province, located within the area of responsibility belonging to TFH and the Danish Battle Group (DABG). The UGV is one of the most complex battlespaces[16] in AFG due to the concentration of narcotics and the various competing forms of governance,

[15] Refers to Human Terrain Mapping (HTM)
[16] For methodological foundation see Johnson & Levis (1988, 1989); Alberts & Czerwinski (1997); S. Metz (2001) For battlespace definitions see Smith(2006); Mitchell (2008, 2009; 2010)

known to TFH as: (i) the *official* (GIRoA[17]), (ii) the *traditional* (tribal), (iii) the *shadow* (Quetta based Taliban insurgence), and (iv) the *dark* (narcotics cartels). Therefore, for studies of agility in complex battlespace, this context provides extreme (and most valuable) conditions for testing our organizational C2 capacities with regard to their ability to promote agility in a complex battlespace.

The core of the effects evaluation is the ability of the BG to generate kinetic and non-kinetic targets for action in order to produce a desired effect. This is a measure of battlespace agility that we can monitor as it is the actual physical representation of battlespace agility defined as the speed at which knowledge is turned in actions for desired effects in the battlespace.

To manage the generation of targets for comparative analysis *a* ***Quantity effects quotient (QEQ)*** is needed for the purposes of a comparative analysis of C2 organization. This QEQ has been obtained by multiplying the ***number of targets generated (TG)*** by the ***number of targets actioned (TA)***.

Using the formal targeting (kinetic and non-kinetic) process as the basis for the measure provides the most concrete measure of actions produced, as it is based completely on the principles of actionable intelligence. Essentially the more targets produced, the more opportunities for action towards desired effects. Success is not measured in this calculation, and therefore it is not a MoE vis-à-vis commander's intent. The QEQ does not account for *quality of knowledge* in the process.

QEQ = TG x TA

Figure B.8.5 Example of Target Cycle Tracking

AUG 2012 (Phase I) **Targets: Compounds of Interest (COIs), Persons of Interest (POIs), Battle Group (BG), Special Operations Forces/Special Forces (SOF/SF)**			
Targets Generated for BG	**Targets Generated for SOF/SF**	**Exploited by BG**	**Exploited by SOF/SF**
59	**18**	**9**	**12**
TG = (59+18)		**TA=(9+12)**	
QEQ=TGxTA **= 1617**			

In this example speed at which knowledge is turned into actions is represented by 1617 and can be used to compare the different months, the issue of achieving desired effects will be an MoE based other factors relative to Commanders Intent.

What would have been the consequences of a failure to act in a way that demonstrates C2 Agility?

[17] Government of the Islamic Republic of Afghanistan

The consequences would have been a failure of the BG to run effective targeting processes, and failure to re-establish coalition forces (CF) freedom of movement (FoM) to conduct human terrain mapping in support of running an effective population centric campaign.

Was C2 Agility Manifested? If so, How?

Battlespace agility was manifested by the informal C2 collective ability to dramatically shorten the knowledge to actions for desired effect continuum in terms of both time and space. With respect to the variables defined for collective C2 approaches[18], the allocation of decision rights to the collective changed, inter-entity information sharing behaviors changed, as did the distribution of information.

Which Enablers and Inhibitors of C2 Agility were observable?

Figure B.8.6: C2 Overview of Observable Enablers/Inhibiters

Edge =1; Collaborative=2; Coordinated=3; De-conflicted =4; Conflicted=5

PHASE	1	2	3		4		5		6	
	Off. C2	Off. C2	Off. C2	Informal Sub-C2	Off. C2	Informal Sub-C2	Off. C2	Informal Sub-C2	Off. C2	Informal Sub-C2
Flexibility	4	5	5	3	5	2	4	1	3	1
Versatility	4	5	5	3	5	2	4	1	3	1
Responsiveness	5	5	5	3	5	2	4	1	3	1
Adaptiveness	5	5	5	3	5	2	4	1	4	1
Resilience	4	5	5	3	5	2	4	1	4	1
Innovation	5	5	5	3	5	2	4	1	4	1

Note: Measures are qualitative estimates to illustrate improving agility. It is assumed the informal networked targeting C2 that developed during the period of study is a sub-collective of the official collective and not an independent collective. Improvements in the sub-collective are not represented in the official collective. Phase 5 & 6, "1" measurements reflect the targeting process moving from target generations issues to target prioritization issues.

- Flexibility: "The ability to employ multiple ways to succeed and the capacity to move seamlessly between them."
    - *During the first 2 periods of conflicted C2 , there was clearly the lack of flexibility from the conventional planning organization that frustrated effective targeting. Insistence on time consuming staff processes severely hindered the exploitation of actionable intelligence. Primary weakness – uncertainty as to allocation of decision rights.*

[18] NATO NEC C2 Maturity Model

- *By phase 3, an informal networked collective began having success in terms of targeting operations; flexibility existed by mere absence of staff processes associated with a traditional military BG organization.*

- Versatility (Robustness): "The ability to maintain effectiveness across a range of tasks, situations, and conditions."
  - *There were indications of versatility as the collective was exposed to a number of scenarios before actual deployment to theatre, as well as a few relatively minor incidents that did not require a change in C2 approach. However once in theatre uncertainty as to the allocation of decision rights hindered the development of shared situational awareness and understanding. Reality of war created greater degrees of uncertainty.*
  - *As the informal networked collective developed, versatility increased with a broader understanding for the exploitation of various capacities available to the network.*

- Responsiveness: "The ability to react to a change in the environment in a timely manner."
  - *Within the first week in theatre, it was clear that the official C2 collective could not respond in a timely fashion to the speed and diversity of insurgent activities in the AO in a timely manner due to the inherent organization processes for a conventional BG structure and component command roll.*
  - *The development of the informal network was largely based on the need for responsiveness particularly when exploiting intelligence in a timely manner.*

- Adaptiveness: "The ability to change work processes and the ability to change the organization."
  - *The official C2 collective displayed no signs of proactive adaptiveness and very few signs of reactive adaptiveness near the end of the study period. Traditional staff processes continued without consideration for effect in the external environment but was self-focused on routines.*
  - *The informal networked C2 was adaptive in its fundamental nature and improvements to that adaptiveness came with shared situational awareness across the range of entities plugged into the targeting processes.*

- Resilience: "The ability to react to a change in the environment in a timely manner."
  - *The official collective C2 did display signs of reactive resilience in the sense it could absorb a great deal of punishment. This however might be viewed as a negative resilience that would further hinder efforts for change. Proactive resilience was non- existent.*
  - *The informal collective C2 was able, by the end of phase 4, to be proactive resilient particularly where it concerned supporting the establishment of village stability operations in the AO.*

- Innovation: "The ability to do new things and the ability to do old things in new ways."
  - *For the official C2 collective, innovation did not exist. Primarily illustrated by the insistence on trying to focus on long planning cycles to support deliberate operations instead of moving to framework and current operational support. This approach was simply not suited for a counter insurgency conflict.*
  - *The informal collective C2 was constantly innovative with regards to operational planning, and a clear understanding of the effect generation objectives for that planning.*

Figure B.8.7 Official Collective C2 + Informal Networked C2 Collective (Assessment)

Official Collective C2 + Informal Networked C2 Collective						
Indicators	**Phase**					
(1)Allocation of Decision Rights; (2)Inter-Entity Information Sharing; (3) Distribution of Information	**1 (Aug)**	**2 (Sept)**	**3 (Oct)**	**4 (Nov)**	**5 (Dec)**	**6 (Jan)**
Sub-Indicators relevant to Kitae Study						
Decision Accuracy						
Decision Completeness						
Decision Congruence						
Decision Currency						
Decision Participants						
Decision Precision						
Decision Relevance						
Decision Speed						
Decision Style						
Decision Timeliness						
Decision Type						
Decision Uncertainty						
Information Accuracy						
Information Completeness						
Information Consistency						
Information Correctness						
Information Currency						
Information Distribution						
Information Networks						
Information Pedigree						
Information Precision						
Information Relevance						
Information Richness						

Information Service Characteristics						
Information Timeliness						
Information Transfer Approach						
Information Uncertainty						
Plan Consistency						
Plan Currency						
Plan Timeliness						
Planning Speed						
Response Speed						
Responsiveness						
Restriction of Decision rights						
Restriction on Information Distribution						
Shared Awareness Accuracy						
Shared Awareness Completeness						
Shared Awareness Consistency						
Shared Awareness Correctness						
Shared Awareness Currency						
Shared Awareness Precision						
Shared Information Completeness						
Shared Information Consistency						
Shared Information Correctness						
Shared Information Currency						
Shared Information Precision						
Shared Information Relevance						
Shared Information Timeliness						

B.8.8: **Official Collective C2** (Assessment)

Official Collective C2						
Indicators	**Phase**					
(1)Allocation of Decision Rights; (2)Inter-Entity Information Sharing; (3) Distribution of Information	**1 (Aug)**	**2 (Sept)**	**3 (Oct)**	**4 (Nov)**	**5 (Dec)**	**6 (Jan)**
Sub-Indicators relevant to Kitae Study						
Decision Accuracy						
Decision Completeness						
Decision Congruence						
Decision Currency						
Decision Participants						
Decision Precision						
Decision Relevance						
Decision Speed						
Decision Style						
Decision Timeliness						
Decision Type						
Decision Uncertainty						
Information Accuracy						
Information Completeness						
Information Consistency						
Information Correctness						
Information Currency						
Information Distribution						
Information Networks						
Information Pedigree						
Information Precision						
Information Relevance						

Information Richness						
Information Service Characteristics						
Information Timeliness						
Information Transfer Approach						
Information Uncertainty						
Plan Consistency						
Plan Currency						
Plan Timeliness						
Planning Speed						
Response Speed						
Responsiveness						
Restriction of Decision rights						
Restriction on Information Distribution						
Shared Awareness Accuracy						
Shared Awareness Completeness						
Shared Awareness Consistency						
Shared Awareness Correctness						
Shared Awareness Currency						
Shared Awareness Precision						
Shared Information Completeness						
Shared Information Consistency						
Shared Information Correctness						
Shared Information Currency						
Shared Information Precision						
Shared Information Relevance						
Shared Information Timeliness						

Figure B.8.9: Informal Networked C2 Collective (Assessment)

Informal Networked C2						
Indicators	**Phase**					
(1)Allocation of Decision Rights; (2)Inter-Entity Information Sharing; (3) Distribution of Information	**1 (Aug)**	**2 (Sept)**	**3 (Oct)**	**4 (Nov)**	**5 (Dec)**	**6 (Jan)**
Sub-Indicators relevant to Kitae Study						
Decision Accuracy						
Decision Completeness						
Decision Congruence						
Decision Currency						
Decision Participants						
Decision Precision						
Decision Relevance						
Decision Speed						
Decision Style						
Decision Timeliness						
Decision Type						
Decision Uncertainty						
Information Accuracy						
Information Completeness						
Information Consistency						
Information Correctness						
Information Currency						
Information Distribution						
Information Networks						
Information Pedigree						
Information Precision						

Information Relevance						
Information Richness						
Information Service Characteristics						
Information Timeliness						
Information Transfer Approach						
Information Uncertainty						
Plan Consistency						
Plan Currency						
Plan Timeliness						
Planning Speed						
Response Speed						
Responsiveness						
Restriction of Decision rights						
Restriction on Information Distribution						
Shared Awareness Accuracy						
Shared Awareness Completeness						
Shared Awareness Consistency						
Shared Awareness Correctness						
Shared Awareness Currency						
Shared Awareness Precision						
Shared Information Completeness						
Shared Information Consistency						
Shared Information Correctness						
Shared Information Currency						
Shared Information Precision						
Shared Information Relevance						
Shared Information Timeliness						

What C2 Approaches were relevant? (How can C2 Approach Agility be inferred from what was reported or observed?) Did C2 Approach change, either for a collective, organization, team or one or more individuals?

The most relevant C2 approaches were identified in relationship to the steady progression of the informal networked collective for de-conflicted to edge C2. The official collective C2 did illustrate significant any change in C2 approach throughout the 6 month period. However this is fully dependent on if one considers the informal networked collective a component part of the official collective.

What interesting and important vignettes are included or can be derived from the case study to help create illustrative stories?

There are several available from phase 1 and phase 2 concerning the inadequacy of the official collective to deal with complex counter insurgent environment, mostly to do with conventional staff processes being too slow to be effective in the counter insurgency environment.

There are several available from phases 3-6 on the reaction of the official C2 collective to the progressively more effective informal networked collective.

The vignettes will require sanitizing both in terms of security and of course - politics.

Case Study Assumptions and Limitations:

a. **What constraints did you encounter that might limit the case study or the evidence supporting it?**
The politics surrounding the balance between generic C2 evaluation and what can be perceived as efficiency or command evaluations. Every effort has been made to maintain the case study as a generic look at C2 issues and an evaluation of a particular command or leadership.

b. **What assumptions did you make when carrying out or documenting the case study?**
One key assumption was that the C2 structure for the BG and TFH operational planning processes (OPPs) were not corrupted by comprehensive approaches.(Ex. ISAF OPP and not UK Afghan Road Map was the driving force behind the generation of Lines of Operations and effects cascades.)

Conclusions

g. **This is not a summary – that is in the Executive Summary**
From the Danish perspective of warfighting, the agility language of the C2 Maturity model is an effective MoP framework for ensuring the optimal balance between organization, technology, and doctrine.

h. **Conclusions relate to the purposes of the case study**

a. **Enablers, Constraints, and Behaviors identified**
Key enabler of the analysis was in fact the ability of the language to incorporate directly the role of informal networked collectives. This allowed an easy comparative framework to be established in order to evaluate C2 approaches.

b. **Language – Clarity and Definitions**
On the conversion of the study from focus on' battlespace agility' as defined for the Danish Kitae study to the focus on generic agility approaches was facilitated by the clarity and definitions of the maturity model. There were no issues of concern. However, it would have been more complicated if the maturity model had not identified the informal networks as a concept.

c. **Applicability of the SAS-085 Concepts and Model**
Very applicable. In this case, combined with the Danish triadic model for warfighting, it provides a viable framework for agility MoPs. Though not detailed here, the SAS-085 model will likely be used to tackle the issue of agile warfighting organization at the Royal Danish Defence College. It will be done with a heavy focus on sense-making capacities being as directly connected as possible to authorities with capacities to act (decision allocation rights). Approaches identified by SAS-085 can act as the framework for improvements.

d. **Statements about Validity**
The indicators of C2 approach, particularly related to 'information sharing' can be tied directly to a plethora of sub-indicators first defined in SAS 065. This high number of sub-indicators creates a high level of confidence in observations and conclusions drawn from them when assessing maturity levels.

The above observations are limited to warfighting C2 organization, a unified military C2 structure, and should not be confused with Comprehensive Approach C2 involving non-

military actors who do not participate at the operational planning processes based on military doctrine.

Bibliography

Abell, Peter (1991). Rational Choice Theory. Aldershot, UK: Edward Elgar.

Alberts, D. S., & Hayes, R. E. (2003). *Power to the Edge: Command...Control...In the Information Age*. Washington, D.C.: CCRP Publication Series.

Alberts, David S., and Thomas J. Czerwinski.(1997) "Complexity, Global Politics, and National Security". June 1997.

Alberts, David S., and Richard E. Hayes (2007) *Planning: Complex Endeavours. DoD Command and Control Research Program*, Washington, D.C., 1998

Checkel, Jeffrey (1999). "Social Construction and Integration," *Journal of European Public Policy* Vol.6, No.4, September

Coleman, James S., & Thomas J. Fararo (eds.) (1992). *Rational Choice Theory: Advocacy and Critique*. Newbury Park: SAGE.

Coleman, James S. (1990). *The Foundations of Social Theory*. Cambridge: Belknap

Czerwinski, Tom. (1998) *Coping with the Bound: Speculation on Nonlinearity in Military Affairs*. DoD Command and Control Research Program, Washington, D.C., 1998

Czerwinski, Tomas J. (1996) "Command & Control at the Crossroads," *Parameters*, Autumn 1996:121-132

Henrotin, Joseph & Tanguy Struye de Swielande. (2004) "Ontological –Cultural Assymetry and the Relevance of Grand Strategies," *Journal of Military & Strategic Studies*, Winter 2004, Vol. 7, Issue 2

Johnson, Stuart E., and Levis, Alexander H. (eds.) (1989) *Science of Command and Control: Coping with Complexity*. Fairfax: AFCEA International Press, 1989.

Johnson, Stuart E., and Levis, Alexander H. (eds.) (1988) *Science of Command and Control: Coping with Uncertainty*. Washington, DC: AFCEA International Press, 1988

Mattis, Gen. J.N. USA DOD Doc. (2008) *USJFCOM Commander's Guidance for Effects-Based Operations*, Norfolk, VA: US Joint Forces Command, August 14, 2008.

S. Metz, D.V. Johnson II, *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts*, London,Strategic Studies Institute, U.S. Army War College, January 2001

Mitchell, William. Kitae I. *Battlespace Agility in Helmand*, Royal Danish Defence College, 2012. http://forsvaret.dk/fak/publikationer/research%20papers/Pages/Forsvarsakedemiet%20Working%20Papers.aspx#publication_b1399452-e6dd-4abb-b2e0-98633d9c089f

Mitchell, William. Kitae II. *Battlespace Intelligence* , Royal Danish Defence College, 2012. http://forsvaret.dk/fak/publikationer/research%20papers/Pages/Forsvarsakedemiet%20Working%20Papers.aspx#publication_b1399452-e6dd-4abb-b2e0-98633d9c089f

Mitchell, William. Kitae III. *Unit Construction for Effect in a Complex Battlespace*, Royal Danish Defence College, 2012.http://forsvaret.dk/fak/publikationer/research%20papers/Pages/Forsvarsakedemiet%20Working%20Papers.aspx#publication_b1399452-e6dd-4abb-b2e0-98633d9c089f

Mitchell, William. Ch.3 'The Comprehensive Approach Dilemma: No Unity of Command-No Unity of Effort'. *Comprehensive Approach*. Edited by Flemming Splidsboel Hansen. Spring 2010.

Mitchell, William. Agile Sense-Making in an Intersubjective Environment. *International C2 Journal* (IC2J). Spring 2010. http://www.dodccrp.org/html4/journal_v4n1.html

Mitchell, William. (2004) *Instrumental Friend or Foe? Constructivist Activism in Security Policy Means Analysis*. Politica, Arhus University, 2004

NATO (2007) *Bi-Strategic Command Pre-Doctrinal Handbook "Effects Based Approach to Operations"* 2007

NATO (2002) *Code of Best Practice of C2 Assessment Analysts Summary Guide*, Washington: CCRP

Nicholson, Peter. (2006) "Effects Based Strategy: Operations in the Cognitive Domain." *Security Challenges*. Volume 2, Number 1, 2006:133-146

SAS-065. (2010). *NATO NEC C2 Maturity Model Overview*. Paris: NATO RTO. CCRP Publication series.

SAS-050 CCRP/NATO. (2006) *Final Report: Exploring New Command and Control Concepts and Capabilities*

Scott, John (2000). “Rational Choice Theory”. Browning, Gary et al., *Understanding Contemporary Society: Theories of the Present*. London: Sage; pp. 126-138.

Smith, Edward A. (2006) *Complexity, networking, and effects-based approaches to operations*. Washington: CCRP.

Smith, Edward A. (2005) *Effects Based Operations: Applying network centric warfare in peace, crisis, and war*. Washington: CCRP.