POLITIHØGSKOLEN

THE GOLDEN HOUR

STRATEGIC COMMAND AND CONTROL DURING THE INITIAL RESPONSE TO TERROR ATTACKS

Jan Henrik Pappas

MASTER I POLITIVITENSKAP 2017 / MASTER OF POLICE SCIENCE 2017

(page intentionally left blank)

Table of contents

Full title:	The Golden Hour: Strategic command and control during the initial response to terror attacks
Student:	Jan Henrik Pappas
Academy:	Politihøgskolen (EN: *Norwegian Police University College*)
Supervisor:	Sissel Haugdal Jore, associate professor, Centre for Risk Management and Societal Safety, University of Stavanger
Year:	2017
Word count:[1]	41.700 (appx.)

[1] Excluding footnotes, abstract and appendixes. Word count with these included: 45.000 (appx.)

00 – Abstract

By its very nature, terror attacks in otherwise peaceful countries will come as surprises. Because the attackers are the ones with the initiative, choosing when, where and how, the emergency services will initially be reactive. In and of itself this is nothing new for these services, as they are meant to respond to incidents when they occur. What sets terror apart from many of these incidents, such as accidents, natural disasters etc., are the malicious intent of the attackers. The emergency services, and especially the police, has to regain the initiative from the attackers in order to stop the attack as soon as possible. This is what identifies the initial phase of the response to such an attack: the effort to regain the initiative and control of the situation. The tactical and operational parts of the system are the first to respond and to spring into action. They are by design meant to *respond* to a situation and *adapt* accordingly, and in the case of a large-scale and /or a complex attack, they are not necessarily equipped to identify the attackers' end-game and initiate means to counter this. Complex attacks that also are multi-pronged will require a level of coordination between the different operational commands, something they may neither have the capability or capacity to conduct. Here, it is vital to have a functioning strategic level. Because the typical strategic command in any given police or security force normally are not on a 24/7 standby or permanently operational, as operational and tactical commands typically are, due to their day-to-day responsibility, it cannot be expected that a full strategic command can be ready within the initial phase of an attack; the so-called "golden hour". However, parts of the strategic command, be that one person or a few, will always come first. They will therefore be required to fill more, and different roles, than they might otherwise would have. Regardless, someone must do the job.

The attacks on 11 September 2001, 7 July 2005 and 22 July 2011 all have several similarities. For one thing, they were all large scale attacks on a level that each country had not seen before, or at least in a long time. They were also complex attacks in that they encompassed multiple targets, required inter-agency collaboration from the responding forces, and caused a massive loss of life. Given the development of the security situation in Western nations, more such attacks must be expected. Attacks in, among others, Paris, Brussel, Nice, Berlin and London in the last few years, shows this to be the case. This thesis aims to look at the 2001, 2005 and 2011 attacks and see if there are similarities in what falls short in regards to the strategic levels' response. As this level have a special responsibility regarding the command and control structure in their respective organizations, it is this that will be studied here;

especially *communication* and *situational understanding*, as there are paramount for the strategic levels' capabilities and overall performance.

Because the chains of command in these situations are so complex and the situation so fluid, those who make up the strategic level during the initial response, are absolutely dependent on contingency plans, so that they may identify the proper chain of command and begin taking measures to regain the initiative. Because the strategic level communicates via *intent*, i.e. it relays its desired actions and desired outcome to the operational level, which then operationalises it, the strategic level have to make this intent known to the operational level. This intent also serves to show the operational level what information are to be relayed up to the strategic level. It is seen that if the operational level either does not receive anything from the strategic level, or if it is unsure as to whom are actually in command, it will begin to take action on its own, effectively leaving the strategic level out of the loop. This in turn will lead to fragmented or information reaching the strategic level, which in turn again decreases its capabilities, leaving the operational level forced to act on its own again, and so on.

In the situations where such a systemic error occurs, it is seen that the lack of usable contingency plans and a lack of understanding of ones role as the strategic command, are at least partly to blame. Proper contingency plans and proper understanding of the role the strategic level has in counter-terrorism response are there for seen as potential mitigating factors here, creating a systemic resilience. This resilience to some extent absent in the aforementioned attacks. Moreover, while all this may not be as pronounced in the smaller-scale attacks, proper contingency planning must take black swans and worst-case scenarios into consideration, if they are to represent a reliable emergency preparedness.

01 – Introduction

"*By three methods we learn wisdom: First by reflection, which is the noblest; second by imitation, which is the easiest; and third by experience, which is the bitterest.*"
Confucius (551 BC - 479 BC).

After a terror attack, such as those in the USA in 2001, England 2005 and Norway in 2011, the security services, counter-terrorism units, the police and the political leadership has been scrutinized in order to determine "where it went wrong", both in regards to the attack, and in regards to measure taken in order to mitigate potential future threats (de Graaf, 2012, p. 4). The goal has often been to find out both why the attacks were not averted, and why they were not confined once they first occurred. Challenges regarding the emergency preparedness, planning and command and control systems have often been found to be contributing factors in each of the attacks.[2]

Terrorists, both organized cells and individuals, are often described as learning entities (Hoffman, 2006, p. 250-252) (Bolz, Dudonis & Schulz, 2012, p. 12-13). Equipment and tactics are often tested in so-called dry-runs[3] before the actual attack takes place. As a result, the attack will often be well rehearsed, and the operatives trained in accordance with their specific tasks, such as was seen in the 11th September 2001 attacks in the US (9/11 Commission Report, 2004, p. 221-227, 234-236). When something goes wrong with the execution of an attack, or the attack is discovered, and subsequently prevented, by security services, terrorists often try to learn from that, and if necessary, adapt future plans and tactics accordingly (Bolz, Dudonis & Schulz, 2012, p. 32-34). Likewise, it is also seen that terrorist are capable of learning and gathering inspiration from other attacks that they themselves were not a part of. Lia uses the description of "*contagious*" to describe this effect (2005, p. 22). One such example is the "2006 liquid bomb plot" in England (Bergen, 2011, p. 206-209), which bear several similarities to Ramzi

[2] Se chap. 6 "The attacks" for an overview of the aforementioned attacks, and source references.
[3] A dry-run is a basically a rehearsal that consists of all or parts of the attack. It is effective in both training for the actual attack, as well as to identify problems with either equipment or tactics.

Yousef's so-called "Bojinka-plot" from the 1990's (9/11 Commission Report, 2004, p. 147) (Hoffman, 2006, p. 248, 283), although there are no evidence of contact between them.[4]

01.01 – Theme and problem to be addressed

As the security situation in Western countries[5] – and the entire world for that matter – continues to evolve, so do terrorism. As described by Hoffman (2006, throughout) terrorism, its causes, practitioners and methods change with the world they inhabit. Since the so-called *war on terror* began after the 11th September 2001 attacks, radical Islamic terrorism, carried out by such groups as al-Qaeda, ISIS, GICM[6] and others has been the most visible threat,[7] although right-wing and nationalist terror also continues to pose a threat in many regions, including the West. Groups will often combine several causes at once, as can be seen in the veritable mosaic of terrorist organizations and rebel groups operating in the Syria-Iraq theatre, and throughout both the MENA-[8] and Sahel-regions.[9] Particularly in splintered or failed states, where the lack of a central government, porous borders and a general disconnect from the nation-state as a primary identifier for the general public, acts as both a catalyst and breeding-ground for terrorist organizations.

In later years, and in accordance with the expressed strategy of both al-Qaeda and ISIS, many of the attacks in the West have been low-tech, often low-yield,[10] and opportunistic in nature (Etterretningstjenesten, 2015, p. 73), (Etterretningstjenesten, 2016, p. 70), (Etterretningstjenesten, 2017, p. 59-60), (Europol, 2016, p. 26). Shooting-sprees[11] or the use of vehicles as a means of attack against soft targets[12,13] appear to have taken priority over more

[4] It is worth noting that attacking commercial aviation, have for a long time been a principal tactic of AQC and its subsequent affiliates, such as AQAP and AQIM (Bergen, 2006, p. 31), (Hoffman 2006, p. 283), (9/11 Commission Report, 2004, p. 153-156), (Lindo, Schoder & Jones, 2011, p. 5), (Thornberry & Levy, 2011, p. 4)

[5] Defined here as: Europe, North America, Australia and New Zealand

[6] Group Islamique Combattant Marocain (EN: *Moroccan Islamic Combatant Group*)

[7] 11th September 2001 was not the "start" of radical Islamic groups' use of terror, but it can be argued that it was *the* attack that brought this threat to the centre stage of public discourse, news and politics in the Western world.

[8] Middle-East and North-African countries

[9] The belt between Sahara in the north and the savannas in the south. Consists of, *among others*; Mali, Algeria, Nigeria, Chad, Sudan and South-Sudan.

[10] The concept of *yield* are used throughout in this thesis (in "low-yield" and "high-yield") to define the effects of an attack in terms of causalities and (property) damage. Similarly, *tech*, are used to describe the complexity of the attack in regards to tactics and execution, and not the technical complexity of equipment used.

[11] Such as the *Charlie Hebdo* attacks in Paris 7th January 2015 or the 13th November 2015 attacks in Paris.

[12] Such as the 14th July 2016 attacks in Nice and the 19th December 2016 attacks in Berlin.

[13] A soft target is a target or area that is not "hardened" by anti-access or area denial measures such as walls, doors and other restrictions to access and/or (armed) guards, CCTV-surveillance etc. (*a paraphrasing of the A2/AD concept as described by Tangredi (2013, p. 33)*). See also Enger et.al. (2016, p. 72-74).

complex, “traditional” schemes such as the use of planes or attacks against heavily symbolic and hardened targets (famous landmarks, houses of parliament and so on). This trend to go after soft targets was once again made frighteningly clear by the attack against a concert in Manchester on 22nd May 2017, with eerily similarities – in regards to target selection – towards the Paris attacks in 2015 where a concert-venue also was targeted.[14] While both those groups still pose a significant threat in regards to complex high-yield / mass-casualty attacks (ibid.), for the time being, it seems like the smaller attacks are more of an imminent threat. The reasons for this can be many, for example that the continued military pressure against the groups forces them to focus their main operational and logistical capacity against the *near enemy* rather than the *far enemy*,[15] and therefor rely more on easier and low-cost attacks when attacking the West.

In that case, a shift in strategy on their part or a weakening of the military pressure against them can lead to a surplus of capacity and resources to once again plan and execute more complex and large-scale attacks. Likewise, a perceived victory over these groups, such as the retaking of territory previously held by ISIS in Syria and Iraq, can lead to a volatile situation where the central command of the group loses control over its fighters, and they decay in to splintered and more volatile cells. The risk of this happening, and the threat it poses, will not be the focus of this thesis, but it is mentioned here to show that by planning specifically to counter only the most current threat, instead of focusing on the entire threat-spectrum, one can be caught off guard by rapid changes. Likewise, as the terrorists learn from both experience and from each other, it befalls to the security services to do the same. Hard-earned experiences gained from one attack need not be learned the in the same way by neighbouring countries and their security services.

This thesis will deal with the following problem to be addressed: ***Looking at different terror attacks in different countries; are there similarities in what, on a strategic level, fails in regards the governments’ and security services’ immediate response to the attack, during the so-called “golden hour”?*** As this is a wide problem to address, the focus on this thesis will be towards command and control systems and contingency planning, primarily in regards to

[14] In citing an anonymous intelligence source, the New York Times reported that the attacker in Manchester may have had direct contact with, and potential coordination from, an ISIS-group called Katibat al-Battar al-Libi, which also was involved in the 2015 attacks in Paris (Callimachi & Schmitt, 2017).

[15] The concept of the *near* and the *far* enemy refers here to radical Islamic groups’ view that the Arab countries (*near*) are under the leadership of what they define as apostate rulers, and the western countries such as US (*far*) enables these regimes. This distinction is an important part in the groups’ strategic thinking in regards to planning and prioritizing – among other things – combat-resources (Bergen, 2011, p. 25-26). This is one of several things that separate the strategic thinking of more geographically localised terror groups such as the Taliban versus the more non-geographically confined groups such as al-Qaeda.

police and / or security forces. The attacks that will be compared here are the 11th September 2001 attacks in the US, the 7th July 2005 attacks in England and the 22nd July 2011 attacks in Norway.

As will be explained in greater detail later, command and control are chosen here because that is the primary "tool" of the strategic level when it comes to controlling and directing the response against an ongoing terror attack. The effectiveness of their capability to direct the forces and resources at their disposal is dependent on their ability to effectively communicate with the operational part of the command chain and receive information from them in order to form an as-correct-as-possible understanding of the situation at hand, and the threat it poses. This again is crucial to their ability to make the correct decisions, based on the situation at hand. The communicative abilities and the understanding of the situation is thus mutually dependent of each other, so it is just as crucial to safeguard against loosing parts of those capabilities as it is to increase their effectiveness.

Because of this, the fields of *communications* and *situational understanding* will be the focus here, including the importance of system resilience, because – as will be explained throughout – these fields are interdependent on each other. These two primary fields are chosen due to their importance in regards to the strategic function of a command and control system, especially in regards to its ability to function properly and to deliver the necessary service and security during the initial stage of a terror attack, as described in their respective chapters. To ensure a sufficient degree of understanding of the concept of command and control, theories regarding both that, and contingency planning / risk understanding will be discussed in their own chapters. The understanding of these two concepts are seen as necessary because they deal with the core of the problem to be addressed here, and they can be seen as "overarching theories" for communications (command and control) and situational understanding (contingency planning / risk understanding).

And as will be further explained in chapter 5, the inherent interconnectivity directly affects the commander's strategic ability to effectively direct forces and respond to the fluidity that are so often seen in the initial phase of a terror attack. Furthermore, on the grounds that it is easier to scale a response down rather than up, and because systemic structures and functions are the central theme, these three attacks, and the experience that can be gained from them are seen as relevant, in regards to the future response to both small-scale and large-scale / complex attacks.

This thesis are divided into five parts. Chapters 1 and 2 are the introductory part, dealing with the introduction, basic definitions, basic relevant research-theory, methodology and the likes. Chapters 3 through 5 are addressing the relevant theories regarding command and control, contingency planning, risk assessment and system resilience. These theories are discussed in their own, separate chapters because, while they are concepts that most people have at least a rudimentary understanding of, they are also vast and complex fields of theory. For the purpose of this thesis, it is therefore seen as important that the reader have the same understanding of these concepts as the author. Chapter 6 gives a brief recount of the specific attacks that are being studied and shows the author’s definitions and reasoning in regards to defining the golden hour for each attack. Chapters 7 and 8 are analysing the relevant incidents in the attacks, while chapter 9 will contain the conclusions of the study.

01.02 – Definitions and exclusions

In the immediate aftermath of a terror attack, or a similar incident, it is not only the police and security forces that responds. Equally important in the effort to minimize casualties and limit the damage and scope of an attack are the fire and rescue services and the medical services, and also often the civilians that are in the vicinity. Even though they are neither tasked nor equipped to directly confront an attacker or take direct steps to stop an ongoing attack, they are an invaluable resource in the response effort. As such, both command and control and contingency planning need to take them, and the interaction with them, into account. However, they will not be covered in this thesis, but merely mentioned where appropriate. The potential analytical challenge this exclusion represents is further debated in the chapter regarding methodological challenges (chapter 02.03).

01.02.01 – Defining “failure”

In regards to the use of the indicator “*failure*” in the response to an attack, it is important to note the following; Any military, police or counter-terrorism operation, whether it is pre-planned or not, will never go quite as planned. Things will happen that will deviate from the assumed course of events, and mistakes will be made. This is an unpleasant fact, and one that are to be expected, especially when dealing with situations where one is confronted with the so-called “fog of war”.[16] In the search for “failures” in this thesis, that will need to be taken into account. Every mistake, error of judgement or lucky strike can not, and will not, be assessed. The goal here is to identify indicators that can point to potential systemic problems in the organization of the response-systems.

Hammervoll (2014, p. 191-203) outlines several parameters that can be used to measure the performance in regards to the response of emergency preparedness resources, such as response-time, degree of response[17], response-certainty[18], reliability, information exchange and flexibility. It is not necessarily easy to specify measurable quantities in regards to these parameters, but these parameters can be used, where applicable, in helping to understand and assess the specific incidents. Likewise, the definitions will not be subject to a grading system, but rather a binary system,[19] as a system of grading is seen, in the contexts of this thesis, to be too inaccurate and far too subjective.

In addition to this, it is also necessary to look at whether the action or situation being assessed contributed towards or delayed the end of the golden hour. By doing so, the situations that did not have any effect in this regard will be excluded. This because they either did not affect the response any significant way (neither in a positive or negative manner), or because those actions were unrelated to the part of the response that had the potential to affect the initial response to the attack. While this is further defined in chapter 06.04, take the following example: During the 11th September 2001 attacks, there was a lot done by firefighters, police and other first responders in their attempts to save lives and prevent further destruction at the WTC (9/11 Commission Report, 2004, p. 285-311) and the Pentagon. However, these actions, and the potential failures, or successes, in the strategic leadership of them, will not be assessed here. This is because in regards to regaining the initiative and seizing control of the situation from the attackers, in this case the hijackers, their actions had no impact on this. It is important to note that these first responders, like many of those in the other attacks as well, often with great risk to themselves, likely saved many lives, but in regards to stopping the attack, they simply did not possess the capabilities to do so. Such as was the case on 11th September 2001,

[16] “Fog of war” is a metaphor for the inherent uncertainty (in military operations) because of the complexity of the situation (and difficulties in getting sufficient situational awareness), for both combatants and commanders. It is often, and somewhat erroneously in its form, attributed to von Clausewitz (Kiesling, 2001, p. 85-87). In day-to-day language is can be used to describe the *general situational uncertainty in a fast changing and fluid situation*.

[17] Refers to what extent an emergency resource is available when needed, i.e. to which degree the called upon resource is available and able to deliver (Hammervoll, 2014, p. 196).

[18] Refers to at what extent the *correct* resource, in the *right* amount and condition, reaches its intended destination (ibid., p. 197).

[19] As in; *failure*: yes or no.

the capacity to stop the hijackers rested with the military, as they were the only ones with the capabilities to forcibly intercept and stop hijacked planes. Still, as the attacks unfolded, those responding and those guiding these responding forces could not have known the full scope of the attackers. Also, considering the increase of "Mumbai-style" attacks in the later years (see chapter 06.05.02), diverting resources towards such responders (that in hindsight did not affect the regaining of the initiative) is still seen as a prudent move, both to prepare for a potential secondary or tertiary attack, and – most importantly of all – to attempt to save the lives of those directly affected by the attack.

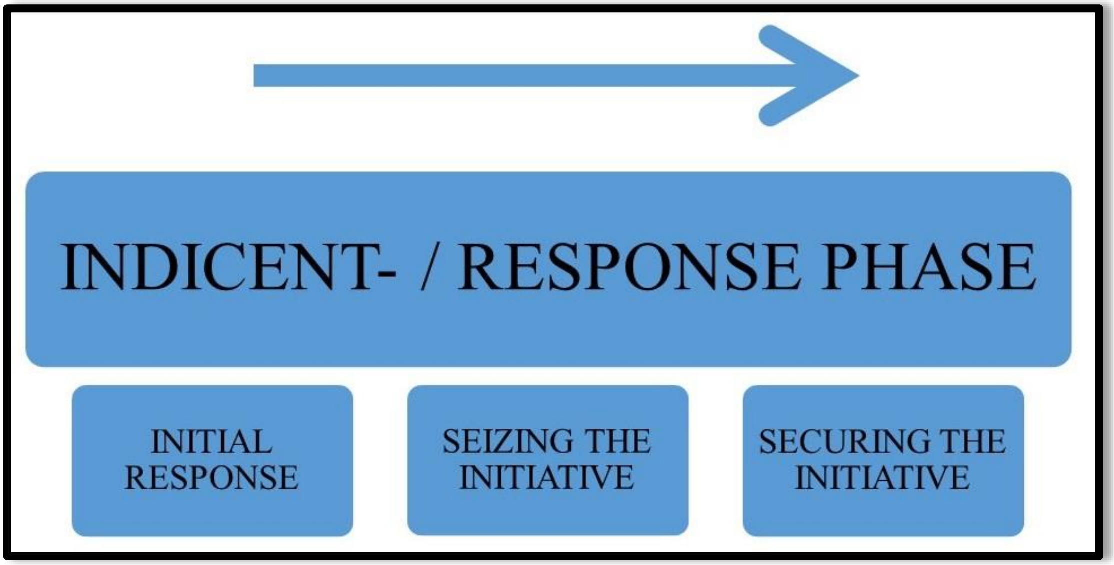
01.02.02 – Stages of a terror attack

As Bolz, Dudonis & Schulz (2012, p. 50) describes; terror defence planning can be divided into three main areas: *pre-incident*, *incident* and *post-incident*. Likewise, Hammervoll (2014, p. 31-34) defines the four phases of emergency preparedness as *mitigation*, *preparedness*, *response* and *recovery* (ibid., quoting Mileti et.al., 1975). The pre-incident planning is primarily "*what if*" scenario-based planning aimed at mitigating the risks of an attack, while incident and post-incident aims to make plans in the event of an attack, or for an immediate threat of an attack, and plans for the (immediate) aftermath of an attack. As this thesis focuses on the immediate response to an attack, the incident or response phase will be focus here. The post-incident or recovery phase is not considered to fall within the parameters of the *golden hour*, as described below.

01.02.03 – The "golden hour" and the initiative

The term "*golden hour*" that is being used here, is a paraphrasing of a rule of thumb in emergency medicine, that states that patients that have suffered severe trauma needs to receive emergency medical treatment within roughly an hour, in order to increase their chances of survival (Lerner & Moscati, 2001, p. 758-760). It is being used here to describe the initial and immediate response to an attack. And while it is not necessarily confined to the first *60 minutes* of an attack, it signifies the importance of having to neutralize the attack, begin the immediate life-saving response, prevent follow-up attacks, and harden potential high-value targets as soon as possible, i.e. during the *golden hour*, in order to minimize the loss of life and damage caused. The Coroner's Inquest into the London Bombings of 7 July 2005 (2006, p. 35) uses the phrase "the golden hour" to describe the "*initial response stage*".

Because there is no clear and absolute divide as to when the *incident / response* phase ends and the *post-incident / recovery* phase begins, that will have to be defined for each of the attacks being analysed here.[20] Furthermore, it is not the entire *incident / response* phase that will be analysed here, but rather the initial part of this phase. As a general rule of thumb, this divide will be at the point in which the responding forces have reached a state where they are able to start regaining the initiative of the situation. This is not to say that they have to regain it immediately, but simply that they are able to start mounting a proper response. In other words, when the initial response is over and the responding forces are beginning work to seize the initiative, as shown by the figure below (the arrow denoting time):



One often seen challenge is that security forces and other typical first responders are not present when an attack commences, but the “clock” in regards to the *golden hour* starts ticking the second an attack is commenced. Because of this, factors such as response-time and response-certainty, and likewise the readiness of these resources (in which factors such as risk-assessment and contingency planning)[21] will play a major factor in the ability to mount a timely and proper response.

Initiative, in this context can be defined the same way as it is in standard military doctrine, such as by Cherry (1921, p. 87)[22] as “*The power of making our adversary's movements conform to our own.*” He further argues that (ibid.) “*We can, therefore, see at once that the possession of the initiative is politically, strategically and tactically of immense value.*”

[20] See chap. 06.04.
[21] See chap. 04.
[22] While a very old reference, the basic conceptual understanding of *initiative* is still the same.

Standardising the definition even more, *initiative* is the ability to control a given situation to such an extent that the adversary are forced to respond to ones actions rather than the other way around, or simply to force the adversary to be reactive rather than proactive in their actions.

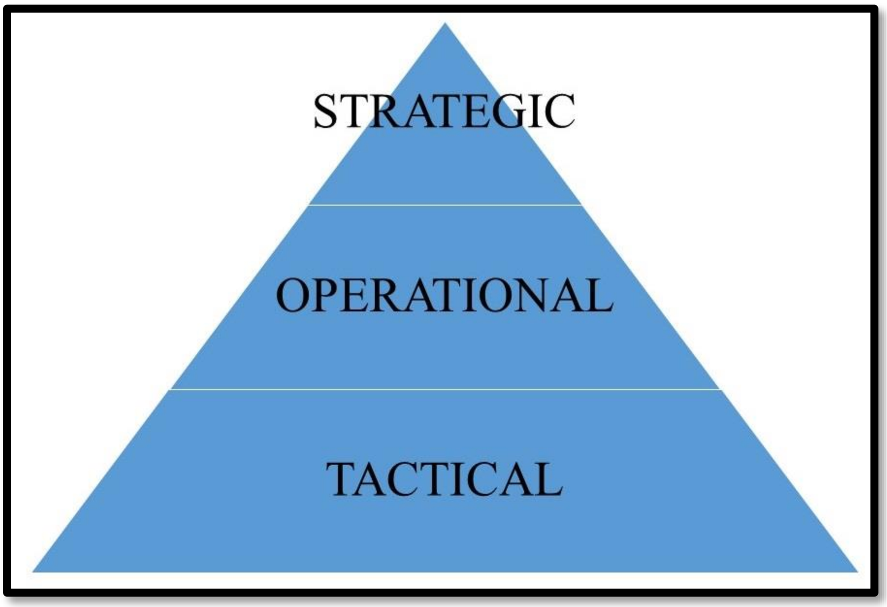
It can be argued that loss of initiative is a hallmark of the situation during the initial response to a terror attack. While loss of initiative to a certain degree can be prevented in military operations or pre-planned counter-terrorism operations, simply by ensuring to seize the initiative by striking first, this is not an option during a terror attack. Loss of initiative is a fact the moment an attack is commenced. This is because the adversary has already seized the initiative by initiating an attack on their terms, against targets of their choosing, with a method of their choosing and at a time of their choosing. The response from security services in the initial phase will be about regaining the initiative. Resilience against the effects of loss of initiative is therefore crucial in regards to security services' ability to mount an adequate response in the initial phase of an attack.

01.02.04 – Strategic, operational and tactical levels

Command and control structures (as will be explained in-depth in chapter 03) use a hierarchical structure in order to facilitate effective resource-management and -control. This means that the different "levels" of a command chain can be divided into three main sections: strategic, operational and tactical. These reflect the different areas of responsibilities that each level has. While most literature agrees upon that strategic is the top level, there are some differences to be found in regards to the levelling of, respectively, the operational and the tactical. Most place the operational level between the strategic (top) and tactical (bottom), such as in the Norwegian military's intelligence doctrine (Forsvaret, 2013, p. 9) and the Norwegian police's intelligence doctrine (Politidirektoratet, 2014, p. 21). The Coroner's inquest into the London bombings (Coroner's Inquest, 2011, p. 34-35) writes, referring to the 6th and 7th edition of the Major Incident Procedure Manual; "*To manage such incidents members of each of the emergency services are assigned as 'Gold', 'Silver' and 'Bronze'. These titles indicate 'strategic', tactical' and 'operational' roles.*" The Major Incident Procedure Manual (LESLP, 2015, p. 21) confirms this definition, by repeating this levelling.

Looking at the definitions in the military intelligence doctrine and the LESLP manual, the different levels are in and of itself defined similar, it is just the wording; operational v. tactical, that differs. As such, it is not seen to cause any methodological problems with adopting a fixed definition and setup of the levelling, in this thesis, so long as the chosen definition is used consistently throughout the thesis.

Therefore, to avoid any confusion regarding this mismatch in defining the operational and the tactical level, the levelling used in this thesis will be as follows: (i.e. the definition as in the aforementioned intelligence doctrines of the military and the police).



Here, the strategic level are responsible for (among other things) formulating a principal strategy, communicating this down the chain of command and adapt the strategy as needed on the basis of the bigger picture. The operational level are the link between the strategic and tactical level, with a responsibility of implementing the strategy from the strategic level and maintaining operational command over the forces / resources that are deployed. The tactical level have the responsibility of leading the direct response within their defined area, be that a specific AO[23] or a specific task. As such, the operational level will usually have command over several units, each on the tactical level. All in all this is can be seen in connection with the definitions of command, control and execution in command and control systems.[24] These definitions of each levels responsibilities are in line with what is described in both the military's intelligence doctrine (Forsvaret, 2013, p. 9) and the Major Incident Procedure Manual (LESLP, 2015, p. 21).[25]

[23] Area of Operations – This may refer to either a geographical or a thematically defined area of responsibility.

[24] These definitions / levellings will be further discussed in the chapter regarding command and control (chap. 3).

[25] With regards to the police's intelligence doctrine (Politidirektoratet, 2014), the definitions there are for the most part based on the definitions in the military version of the doctrine (Forsvaret, 2013).

01.03 – Previous research and literature

After each attack, there have been conducted extensive research into what happened, why it happened and what went wrong. Congressional hearings, investigative committees, and the likes, have been conducted in tandem with, or simultaneous with traditional investigations, in an effort to find out what happened. The question "How could this happen?" is often at the centre of these commissions and hearings. This reflects the question of why the perpetrators committed the attack and the road that lead up to the attack. Equally important, the goal of these hearings have also been to identify why the security and intelligence services were not able thwart the attack.

These investigations and commissions are then often followed by a more academic approach, and plenty of literature regarding the attacks have been written, with a multitude of focuses; from a more pure causality-view of the events, to the more sociological ones. However, the author has not seen a comparative study that focuses on similarities in failures in regards to the command and control preparedness of each country when faced with the attack.

In regards to studies of command and control in major incidents, there has been several studies of that, and Flin (1996, p. 21-37) lists and compares several of them. The selection of major incidents here was accidents, such as offshore-fires, railway- and aircraft-accidents and the likes. The difference between those kinds of incidents and the incidents that are being studied here (terror attacks) are notable in what parts of the states' apparatus that is responsible for the incident (police / security services versus fire, medical and rescue), and the fact that terror attacks are, unlike accidents and natural disasters, actively led by forces with an intent to cause maximum damage. This lack of malicious intent and the potential for an active response to the first responders' actions, makes these incidents less relevant for comparison in the scope of this thesis. However, this is not to say that lessons from those studies mentioned, are worth learning from, also in a counter-terrorism aspect.

01.04 – Thoughts surrounding the theoretical perspective

The three attacks that will form the base of the thesis have been selected because they took place in countries that are similar in culture, governmental structure and legal framework. All of the attacks were also seen as a watershed-moment in its own country, in regards to counter-terrorism work. At the same time, the attacks differ in several ways, especially in type and complexity of attack. As such, the three attacks will form a wide basis for comparison, as successful contingency plans and command and control systems should be, and are supposed to be, able to cope with a multitude of events, from natural disaster to both large- and small-scale terror attacks with a high variety of modus operandi.

It is also of importance that all the attacks occurred "*out-of-theatre*", meaning that they did not take place in an active, or a *de-facto*, warzone. Likewise that they occurred at a time when the country in question was not in a particular heightened state of alert, for fear of an imminent terror attack. This is important because in such situations, the contingency plans and command and control structure will not be representative of the normal peacetime situation (Bolz, Dudonis & Schulz 2012, p. 61). This is because in those situations, contingency plans will already be active, command and control structures will be reinforced – often by a military chain-of-command – or the system will be in a complete or partial state of breakdown. In addition, "*in-theatre*", it is often more difficult to differentiate between terror attacks and regular or asymmetrical military attacks that causes collateral damage. Also, the difference in response to those different types of attack are substantial.

01.05 – Research ethical considerations

As the focus of this thesis is the general methodology and strategy of counter-terrorism preparedness, and not individuals involved in this, the ethical considerations regarding individual's right to privacy, that often is an important consideration in social science studies, does not seem to apply here. Furthermore, this is emphasized as open sources and already well-publicized commission reports, rather than questionnaires or interviews, are the primary source of data.

However, in gathering and analysing open-source information, especially on a subject such as this, there is always a risk that the end-product can turn out to contain something that should not come to public knowledge, as described by Buckley (2014, p. 387) in debating the dissemination of open-source intelligence:[26] "*It is not just raw information; it is information that has gone through a process and has had value added to it.*" Searches for weak spots in counter-terrorism strategies could possibly be picked up and used by the very terrorists that one seeks to increase the systems'[27] ability to thwart. Terrorist organizations' study of, among other

[26] Intelligence compiled solely from sources that are publicly available, i.e. *open source*.

[27] By "*system*" it is here meant the entire counter-terrorism apparatus in any given country.

things, research regarding themselves, can for instance be seen by the discovery of two FFI-reports, found in bin Laden’s bookshelf following the 2011 raid against his compound in Abbottabad, Pakistan (Samuelsen, 2015). As such, this is something that has to be considered as a potential ethical dilemma here. Considering that the view in this thesis is towards the more general, strategical level, this is not seen as a major risk here. This is further underlined by the fact that the primary sources of information are from after-the-fact evaluations, and weak-spots identified here are likely to have been addressed already, or have been classified to such a degree that they did not appear in the public documents, and therefore not in the data-material for this thesis either.

02 – Methodology

As described by, among others, Johannessen, Tufte & Christoffersen (2011, p. 361-370), the methodology in social science can be divided into two main schools of thought: the *positivistic* one and the *hermeneutic* one. While positivism draws its methodological pedigree from the natural sciences, with a focus on observing the existing ("what is", hence the *positive*) and a primary focus on quantitative data, hermeneutics looks in the other direction. There, the focus is on understanding "why it is", rather than "what is". This often requires the researcher's more or less active participation in what is being studied, such as participant observation, or in-depth interviews for example. It also focuses on interpretation and attributing meaning to what is being observed, often trying to identify the underlying causes (ibid., p. 233-236) or the "deeper meanings", as described by Fjelland (2009, p. 44), in that "*The sentence gets its meaning from the meaning of the words (but the meaning of a sentence is not equal to the sum of the words' meaning), (...)*"[28] For this, a qualitative approach is the primary method. It is the methodological principles of hermeneutic that will be used in this thesis.

02.01 – Methodology used

The methodology used in this thesis will be qualitative, comparative literary analysis. The main sources here will be the official reports and inquiries into the attacks. The US and Norway have gathered this into one report each, while the UK have them divided into several smaller reports. Using the theories regarding command and control systems, contingency planning and their operations in crises, in addition with the assessments and outcomes of incidents described in the reports; *failures* in each of the attack will be attempted identified. At the end, they will be compared against similar or otherwise relevant findings in the other attacks, to see if there are similarities between these. As the three attacks were extremely high-profile incidents it has been written much about them. With police investigations and parliamentary inquiries / committees on one side, and extensive academic and journalistic work on the other side, there is a large amount of data available to build a complementary base of data, in addition to the main sources.

[28] Author's translation. Original text in Norwegian: "*Setningene får sin mening fra ordenes mening (men setningens mening er naturligvis ikke en sum av ordenes mening), (...)*"

The choice of using this qualitative method, instead of a quantitative approach is because the purpose of this thesis is to assess *how* the system performed, and more importantly, *why* the system failed where it did. The system, in this case, being the strategic leadership level. Moreover, as described in chapter 02.01.02, the attacks chosen here are large-scale attacks that can be said to have had a powerful impact on the countries in which they occurred. Also, because the attacks was of such a size, they "stress-tested"[29] the systems, making factors relevant to potential failures easier to identify and subsequently analyse. While these attacks are not of newer date, and the fact that they somewhat differ from the latest set of attacks in Western countries in regards to size and complexity,[30] this is exactly the point for why they are the primary attacks being studied here; Low-yield attacks, while putting a heavy pressure on the responding forces and the strategic leadership of these, may not reveal underlying systemic challenges, simply because these do not become visible unless the system is put under extreme stress, as further described in chapter 02.01.02.

Furthermore, the strategic levels within government, police, security services or the military are not easy to get access to and information from, in regards to counter-terrorism. The committees that have dealt with these attacks had, for the most part, this access both in regards to personnel and information, and also the authority to collect the information they deemed necessary to conduct their investigation. The qualitative analysis of the data they were able to collect are therefore seen as more fruitful in regards the question to be addressed here, instead of either in-depth interviews with participants, or a more quantitative analysis of either a multitude or attacks (the vast majority then being "smaller" in terms of scope-of-attack) or questionnaires directed towards participants, as these committees have had a level of access to information that far surpasses what the author of this thesis would have been able to get.

The primary sources for this thesis is thusly the 9/11 Commission report, the 7/7-reports[31] and the report from the 22nd July Commission (NOU 2012:14). In reviewing these reports in line with the theme of this thesis, first a set of definitions and limits are set; Strategic

[29] By "stress" it is in this in this thesis, unless stated otherwise, referred to the strain on a system and not a person.

[30] As noted in, among other places, chap. 01.01, the current strategy seems leaning towards low-yield attacks with a more "opportunistic" approach in regards to target selection and method of attack, rather than complex high-yield attacks. It can be argued that the larger 13th November 2015 attacks differs from this, as it was a low-tech but high-yield attack with a higher degree of complexity (being a multi-pronged attack). As a full after-action assessment of the government's response to such an attack takes time, this attack is not included as a "primary attack" in this thesis, though it fits in to the other criteria for it.

[31] The ISC Report into the London Terrorist Attacks on 7 July 2005 (2006), the London Assembly Report of the 7 July Review Committee (2006), the House of Commons report no. 1087 (2006) and the Coroner's Inquest into the London Bombings of 7 July 2005 (2011).

leadership has to be identified for each attack. Secondly, the "golden hour" has to be identified for each attack, with use of a common definition. This is to make sure that the same basic definitions are used for analysing each attack, thusly ensuring that the data are comparable. Then, in assessing the data from the viewpoint of communication and situational understanding, the definitions of "failure" are used to assess the data's validity for use in this study.

In regards to what could have been done different with the methodology and data-selection in this thesis, two things are especially worth noting. While the three attacks presented and analysed in this thesis represent a wide span in both time and method of attack, there has unfortunately not been a lack of possible attacks to consider for this thesis, in the later years. As the last few years have shown, low-yield attack of a more opportunistic nature seems to have been the method of choice for a more decentralised range of terrorist groups. Still, there have also been relatively complex high-yield attack, as the Paris-attacks of 13th November 2015 and the Brussels bombings of 22nd March 2016 was examples of. Both this and the Madrid-attack on 11th March 2004 were considered as events to be analysed in line with the other three main attacks of this thesis, as they represented two additional modus operandi of high-yield attacks.[32] The Paris-attack was excluded due to the relative short timespan between the attack and the writing of this thesis, while the Madrid-attack was excluded due to a lack of primary sources in English.

In addition to this, attacks occurring in Israel has also been under consideration for further analysis in this thesis. These could have given a high number of attacks with a large variation in modus operandi to analyse. This was however considered not applicable in line with the cornerstone of this thesis; that the attack would have to be "out of theatre". And while Israel are not considered a "theatre of war" in the sense used in this thesis, it is still in a heightened state of alert in regards to terrorism, and that would make the comparability difficult in regards to the other attacks, where the state of alert and all-round readiness are not at the same level.

These two points are thusly worth noting when considering the conclusions of this thesis; there are other attacks that, on the surface, also would have been potentially applicable for further study in this thesis; both in regards to variations in modus operandi and in regards to sheer volume of potential data. On the other side, limiting the analysis to a smaller number

[32] The use of multiple non-suicide IEDs, and "Mumbai-style" multiple assault teams acting independently of one another using asymmetrical tactics and going after soft targets.

of attacks gives the possibility for a more in-depth study than a higher number of attacks would have allowed.

02.01.01 – Reliability and credibility

Standardised reliability assessment in qualitative studies is usually not expedient (Johannessen, Tufte & Christoffersen, 2011, p. 229), or for that matter possible (Grønmo 2011, p. 228-229). Because of this, a credibility-assessment of the data-materials that forms the basis for this thesis becomes essential to ensure the reliability of the data, and the thesis itself. Because all these commissions and committee reports, that form the basis of the data-material, have been under intense public scrutiny for many years, including from the press and the research community, and that they still are considered generally sound, this is seen as a confirmation of their credibility, and with that, the reliability of the data in them. While there have been, and continues to be, debates regarding the commissions and their findings, this seems to focus on the commissions' conclusions and not their description of the attacks. Also, the specific fields that are studied here (situational understanding and communications) are defined clearly, so that it is possible to recognise them in regards to the specific incidents and parts of the attacks that are selected for further study.

02.01.02 – Validity and generality

In regards to validity, it is in this case important to assess the *generality*, or transferability; if findings from one attack is transferrable to the situation in another country, as this is a competitive study (Johannessen, Tufte & Christoffersen, 2011, p. 230-232). While the reports that form the base of data here are not purely academic in their form, and do not necessarily fill all the requirements to be considered a research project (ibid.), they can still be considered to be systematically collected and analysed data, and as such are subject to assessing generality, in regards to their data and their findings.

The validity of the data, with regards to objectivity and confirmability (ibid.), is also something that needs to be assessed. It is important to keep in mind that, as mentioned before and in chapter 02.02, the conclusions that are made in the different reports may be influenced by politics to a certain degree. The data in and of itself are considered to be objective, as they are gathered from a wide range of sources (mainly primary-sources), and it is referred to the sources of information. Defining failures, or successes for that matter, in this thesis does not rest solely on the analyses and assessments in the reports, and the objectivity of the data is thusly assured.

Still, there will always be an element of subjectivity in this regard. Even though the assessment of whether something was a failure will be considered independently from what – if any – definition the original reports has given it, this original definition and assessment will always carry some weight. Because if the validity of the data are to be trusted, the assessments made out from those data cannot be dismissed offhand. It is also prudent to assume that the definitions have to some extent affected the data that are included in the final reports. In addition to this, the definition in this thesis regarding failures will always be a subjective one, even though it is based on objective criteria. Because of this, it is important that each of these assessments are clearly explained, and that the reasoning that lies behind the definitions are clearly stated, as to ensure its verifiability and possibility for later re-examination.

In regards to the study's generality and its transferability towards similar situations, i.e. terror attacks, it is worth noting that as this study focuses on structural factors in one part of the response-chain, namely the strategic one. Had the study focused on the tactical approach, it would have been less transferable, as this can be rather specialised depending on what kind of attack one is facing, and also what country it happens in, as the operational and tactical parts of police and security forces are organized in a multitude of ways, even in otherwise rather similar Western countries. However, the strategic level and its need for communication and situational understanding will be more constant regardless of the kind of attack it is responding to. Where the chain of command leads to and what kind of resources the strategic levels will need to coordinate will change depending on the scenario, but the method of *how* this is done, will stay more constant. This is also why the three attacks that are studied here are three different attacks, namely to try to identify whether there are such similarities despite difference in attack-scenario and the country it happens in.

It is still worth nothing here that the 11th September 2001 attacks somewhat differs in this aspect, in regards to the two other attacks. During this attack, as will be explained throughout later chapters, the strategic level became entangled in both operational and tactical decisions in a way that did not occur in the two other attacks. The extreme scope and complexity of the attack contributed to this, and this attack can be viewed as a worst-case scenario. While some of the actions of the strategic level during 11 September therefore are not immediately comparable to the other two, it shows a system under extreme stress, and the effects this had on the comparable strategic responsibilities. The reasons for this extreme stress-level in the system should still be kept in mind when comparing this attack to the other two.

Also, since the attacks discussed here are large-scale and multi-pronged, it is seen as reasonable that systemic problems that otherwise would not be as visible or even decisive in smaller attacks will be more visible, due to the higher strain on the system large-scale attacks poses. On the other hand, since so-called "low-yield"[33] attacks have become more prevalent throughout the Western countries in the later years (see chapter 01.01) it can be argued that the transferability is somewhat limited because one is dealing with two different kinds of attack-strategies, and by extension; defence-strategies. While that is true, the nature of readiness and contingency planning (see chapter 04) shows that the systemic way the attack is being responded to are likely to be more similar than not, even though the practical approach, and the size of the response (also in regards to the size of the strategic level that is "activated") will differ. Furthermore, it can be argued that if something is a success-factor even when exposed to severe stress, as it would have been in a large-scale attack, it would surely also stand up to smaller-scale attacks. On the other hand, if something fails, potentially because of the stress it is exposed to in a larger-scale attack, it is not sure that would suffer the same kind of failure in a smaller-scale one. Nevertheless, a potential flaw in the system, and its inherent potential for failure, would still be there, and in regards to both a sound risk assessment and the entire thought behind contingency planning (see chapter 04) such an inherent systemic weakness would still need to be addressed. Likewise, it is not safe to plan only for the possibility of a small-scale attack, forgetting the potential for so-called "black swan" attacks (see chapters 01.01 and 04.05), or other high-yield attacks in the Mumbai- and / or Paris-style.[34]

It is also worth noting that, as described in chapter 01.02.03, the concept of the golden hour in counter-terrorism and emergency response is not a scientifically defined term in and of itself. As described, it is used to define the first part of the initial response phase in an incident response, as further described by Bolz, Dudonis & Schulz (2012, p. 50) and Hammervoll (2014, p. 31-34), and as seen used in the Coroner's Inquest (2006, p. 35). As it is not a scientifically defined term, it is important to be clear about the usage and definitions of the concept, if it is to have any function in a thesis. Because the understanding of the "time-slot" it is meant to represent is based on a more scientific definition of the different stages of an attack, the author's

[33] Low-tech and / or opportunistic attacks designed to cause fear and insecurity not by relaying in mass-casualties (although that still can be what the attackers attempt) but rather by being just that; opportunistic, and widespread by nature, creating a feeling of general insecurity by trying to instil the assumption that "no place is safe".

[34] Referring to the 26th November 2008 in Mumbai and the 13th November 2015 attacks in Paris.

definition and understanding of the concept,[35] and its clear definitions regarding the incidents that are being analysed here,[36] are seen as sufficient to ensure its validity in this thesis. It is also worth noting what while the Coroner's Inquest (ibid.) uses the term, they do not specify it further than "*the initial response stage*". Thusly their definition is seen as similar to the author's, but it is not specific enough to be used on its own, as it does not set a time-frame or any other specific "cut-off" point for the end of the golden hour.

02.02 – Methodological challenges

Using material as described above, as the basis for research comes with some challenges and potential risks that it is important to be aware of, during both the data-collection and the subsequent analysis. The primary challenges with the method and data used here have been identified as six different scenarios, and they will be further discussed in this sub-chapter.

02.02.01 – Pre-analysed or politicised data

What is seen as the main methodological challenge is that the data-material that will form the base of this thesis is not *raw material* as such. It is material that is already collected and analysed, not necessarily with scientific methodology and future comparative studies in mind. Commissions and committees tasked with assessing the aftermath of a terror-attack are more often than not politicised to a certain degree. Either by being tasked by, or consisting of, politicians, and operating under a mandate guiding their investigation, usually given to them by politicians. Likewise, a strenuous relationship between the commission and the politicians in charge at the time of the incident, can also lead to challenges and potential pressure upon the commission and its work, as with the 9/11 Commission and the Bush White House (Gill & Pythian, 2012, 156-158). While this, as mentioned above, is not considered to influence the credibility or validity of the data, it can have an effect on what data that the committees gathered for analysis. This risk is mitigated by the mere fact that independent actors, such as media and many different research communities have, extensively covered these events, and their subsequent reviews, often with a sceptical eye. This was seen in the first Intelligence and Security Committee (ISC) review of the 7th July 2005 attacks in London, in which the

[35] See chap. 01.02.03
[36] See chap. 06.04

shortcomings of the initial report led to a new and more thorough study (ibid., p. 183-184).[37] The additional use of complementary and comparative data (Grønmo, 2011, p. 239-240) also helps to mitigate this risk. However one must be aware about the potential that some complementary data may, to a certain extent, be based upon the same material that the primary data is.

02.02.02 – Observer selection bias and biased interpretation

The selection of data, and the subsequent interpretation and analyses of it, for example in defining *failure*, will have to be selected and interpreted by the researcher. As such, there is a risk that the preconceived notions or pre-existing knowledge and experience of the researcher will affect the selection and interpretation of data. Such a confirmation bias or "tunnel-vision" (Fjelland, 2009, p. 229-231) can thusly manifest itself in a biased selection of sample-events, or a biased interpretation of those events, for example in defining something as a failure or a success. Seeking to avoid this is seen as paramount in any thesis where hermeneutic methodology and the use of interpretive analysis are central. By discussing the data and the rationale behind those analysis' so as to give the reader the same base of understanding as the author are seen here as a good way of mitigating the risks of such biases.

Marshall & Rossman (2016, p. 43-59) argue that, in qualitative studies, it is important to consider the *trustworthiness* of the study and the interpretation of the data, i.e. the analysis and subsequent findings.[38] They argue that the qualitative approach needs to incorporate trustworthiness as a key methodological factor, because the researcher's experiences, opinions, etc., has the potential to affect the researcher's understanding of what he or she are observing. This because of the central part of qualitative research: to add (deeper) meaning to observed events. Simply choosing a topic for further study constitutes a potential bias:

[37] Gathered in the "Coroner's Inquest into the London Bombings of 7 July 2005", presented in 2011. The full transcripts of the hearings have been archived at the UK National Archives online at http://webarchive.nationalarchives.gov.uk/20120216072438/http:/7julyinquests.independent.gov.uk/ (archived and "frozen" on 16th February 2012).

[38] The concept of *trustworthiness*, as described by Marshall & Rossman, are, at its core, supposed to replace the traditional concepts of *validity* and *reliability* in qualitative studies. They argue that those concepts of methodological assessments are not sufficiently suited for qualitative studies. In the context of this thesis, trustworthiness are not meant to replace neither validity nor reliability, and the trustworthiness of the thesis will not be debated. However, their thoughts regarding the biases a researcher brings with him- or herself into a study simply by choosing a topic are relevant regardless, because these potential biases still need to be discussed, regardless of what methodological assessments are being used in debating the methodology of the study.

> “*Choosing the topic is, in itself, having or taking a view, standing somewhere (Haraway, 1991); so good proposals include the researcher’s standpoint, both in the literature review and in a section on the personal significance of the study, including the reasons for choosing the topic, presuppositions, previous experience with the topic, the setting, the participants, and an expression of the hope or expectations that the study will somehow contribute by changing knowledge assumptions and/or solving a societal challenge.*” (Marshall & Rossman, 2016, p. 44)

The importance of this when dealing with interviews, participant observation or the likes seems clear. This is not seen as equally relevant in the case of this thesis, as the data material, although identified and selected by the author, have been compiled by others than the author. The researcher’s standpoint and potential preconceptions, which comes into play already at the point of choosing a topic and a problem to be addressed, are however seen as relevant in this case. The topic is chosen because of, among other things, interests and curiosity regarding this specific theme. Possible preconceptions are also shown by the specific problem that are to be addressed, in this case: *What fails in the initial response*? One does not have to read many articles or news-reports about these attacks to realize that there were things that failed, and as debated in chapter 01.02.01, failures are an unpleasant fact when confronted with such attacks, despite the hard work and often heroic effort of those involved in the response. Still, this sets a precedent in the way the author selects and interprets the data, as the thesis itself is built upon the preconception that failures have occurred, one seeks to find and identify these failures.

02.02.03 – Spurious relationships

In analysing events and assessing whether they contributed to, damaged, or were did not affect, the outcome of the counter-terrorism response, there is also a risk that cause and effect will be misinterpreted, and that events that had no impact on the overall outcome can be misunderstood as having such, creating spurious relationships (Grønmo, 2011, p. 363-365). A solid understanding of both the systems that are being examined (here: command and control), and the actions and events that are being assessed in regards to these systems, are important to avoid such mistaken correlation. This is seen as especially important in defining the golden hour for each of the attacks (see chapter 06.04) This is also mitigated by the fact that this thesis aims to look at the strategic and systemic level of the command and control system, and on such a level, individual actions alone does not have the same impact as it would looking at the tactical level. The combination of several individual actions have an impact, but by looking at several actions, rather than one, this risk is diminished.

02.02.04 – Classified or redacted data

Counter-terrorism and emergency preparedness are topics that are closely linked to national security. Hence, due to the need for operational security, there is often widespread secrecy regarding these kinds of plans and framework. This mismatch between the need for maintaining a level of secrecy versus the public's need for a thorough examination of the events that took place are exemplified by, among others, Buckley (2014, p. 106). As such, this secrecy will naturally also come into play in the analysis and assessment of potential systemic weaknesses. The risk that undisclosed information will cause a potential distortion of the data seems somewhat mitigated by the fact that the attacks that are being analysed in this thesis are not brand new, and as such, it is not considered likely that withheld data will noticeably affect any findings and possible conclusions. This is reinforced by the fact that most of the information that is withheld seems to concern specific capabilities, methods or particularly sensitive intelligence-related information. Examples of this include the so-called "28 pages" from the 9/11 Commission (Smith & Ackerman 2016) (Mazzetti 2016), and the occasional redactions in the ISC reports from the UK (ISC, 2006, p. iv) (ISC, 2009, p. iii).

02.02.05 – Hindsight bias

As described by Gladwell (2003, p. 83-88), in analysing past events, and particularly when looking for "errors" in the handling of these events, one will always have the advantage of full hindsight when "connecting the dots". By having the full picture, it is easier to correctly identify systemic failures. But in regards to evaluating decisions made "in real-time" this full knowledge is not directly applicable. In such cases, when evaluating decisions, actions taken and such, and not the performance of a system, one has to account for *what information* were available to *what individuals* at *what time* during the process of decision-making. Otherwise, the basis for evaluating will be flawed, because the evaluation will take into account variables not available to the decision-makers at the time. Whether such information *should* have been available, but were not, is a point that must be considered when evaluating the systems performance as a whole. ISC, in their report regarding whether the 7th July 2005 attacks could have been prevented, also draws attention to this by noting: "*(...) we must be careful, when* *looking at whether past decisions and judgements were correct, to look only at the information available at the time.*" (ISC, 2009, p. 40). The 9/11 Commission Report (2004, p. 339) also notes: "*In composing this narrative, we have tried to remember that we write with the benefit and the handicap of hindsight. Hindsight can sometimes see the past clearly – 20/20 vision. But the path of what happened is so brightly lit that is places everything else in the shadows.*" Likewise, the report from the 22 July Commission have been the focus of several critical evaluations of its work and understanding of the scenario it was meant to assess, because of a perceived hindsight-bias.[39] Whether or not this is the case will not be debated further here, as it is not topical to the thesis, but it is noted as a potential example of this bias and the methodological challenges that follows it.

02.02.06 – Leaked data

As mentioned in chapter 02.02.04, the field of counter-terrorism and national security will, by its very nature, include classified data. As previously discussed, these classifications are probably more prevalent the more operationalised the information is, but still; information regarding strategic plans, programs and capabilities will also be susceptible to classification-regimes. Especially in the later years, leaks of such information have occurred time and time again. While the more extensive leaks are not considered relevant for the theme of this thesis – such as the Snowden NSA-leaks, the Afghanistan "war-logs" and US diplomatic cables leaked by WikiLeaks – it is reasonable to presume that other leaks can contain data that could be topical to this thesis. It has been a conscious decision to refrain from using such material in this thesis. This is because – in addition to the obvious ethical sides of it – it is not possible to assure the reliability of such data to the same degree as open / unclassified data. While much of the leaked data probably are reported correctly, the inability to verify this to the same extent as other sources of data would still be a point of concern.

Still, it is not unreasonable to assume that some of the sources used in this thesis can contain some parts of leaked data. This is, on the other side, not seen as a major problem as that data in those cases would be a part of a larger scientific text, and thus the subject of peer-review. In those cases, it is therefore not seen as a problem, regarding the reliability of the data.

[39] As an example, see "*På vår vakt*" by Malin Stensønes (2017) or "*Politiets handlingsplikt under «skyting pågår»*" by Juni Herjuaune (2014). Note that these are merely meant as examples for the public discourse regarding the commission's report, and they will not be further discussed in this thesis.

02.03 – Challenges regarding exclusions

As briefly mentioned in chapter 01.02, fire- , rescue- and medical services (abbreviated to FRM for the purpose of this thesis) will be excluded from the data-collection and analysis in this thesis. This is being done both to limit the scope of the study (Grønmo, 2011, p. 263), and because the police, security services and the command over these are the primary focus of the thesis. Noting Flin (1996) in the introduction (chapter 01.03), this exclusion is also based on the fact that the police and security services are the primary services responsible in the initial response to a terror attack. However, FRM-services are an important part of the initial response, also as potential sensors, in regards to contributing to the situational awareness (see chapter 03.02). Thusly they will have an effect on the command and control systems, as both contributors (i.e. sensors) and as parts of the overall chain of command. Being aware of this potential bias and noting this, when and if applicable, is sees as sufficient in dealing with this.

As mentioned in chapters 01.01 and 02.01, there are several other attacks that have occurred in both the US and in Europe that are of a newer date than the three attacks singled out here. In addition to these newer attacks, the IED-attacks[40] in Madrid on 11th March 2004 against the city's rail-commuter network[41] are also a highly relevant attack, in regards to the theme of this thesis. Due to their obvious relevance, they can still be considered as a complementary sources of information. These exclusions are not seen to cause a methodological problem, as it is the qualitative data, and not the quantitative, that are the key here. In addition to this, the three primary attacks already covers three different kinds of attack; plane hijackings and their subsequent use as missiles, multi-pronged attack against public transportation networks using PBIEDs[42] and the combination of a VBIED-attack[43] and a mass-causality shooting-spree.

In addition, the attacks are enough years apart for the respective governments and services to have a realistic possibility to draw experiences from the successes and failure of the previous attack(s). While this in no way is enough to qualify as any sort of longitudinal study, it still provides a possibility to see if there are signs of evolution in the way command and control reacts in regards to terror attacks / mass-causality incidents. Primarily this will be to see

[40] An IED is an Improvised Explosive Device; "home-made bomb"
[41] See chap. 06.05.01
[42] Person-Borne IED; the explosive device used by a suicide-bomber.
[43] Vehicle-born IED; "car-bomb"

if they consider the previous attacks and what happened there either in the updating of contingency plans or during the attack itself. Because of this it is important to be aware the possibility of, and to avoid, a biased interpretation of “old systems” with “new eyes”, i.e. assessing actions out of the context (here: the time) they occur in, because there is a longer time-frame to study. It is important to be aware of this possible bias when analysing and especially comparing findings from the different attacks.

Furthermore, as the 11th September 2001 attacks are generally seen as the beginning of the so-called “war on terror” (Bergen, 2011, p. 57), which can be argued to still be in effect to this day, there is also a possibility that security services in the later attacks have adapted to the new security challenges that have grown out of the war on terror. By having a wide timeframe between the first and last of the primary attacks, it is possible to see signs of such an adaption, if it has taken place within this field. Nevertheless, as mentioned above, since this is not a longitudinal study, absence of such findings cannot be seen as proof that it has not occurred (as the aphorism goes: *absence of evidence is not evidence of absence*), while it may give cause for further research into that specific topic.

03 – Command and control

Police forces, security services, and basically any organization that has a responsibility in case of a terror attack, are large and complex organizations, and because of this, there is a need for an effective way to lead and deploy these units. As time is of the essence in extraordinary situations, such as a terror attack, the normal chain of command which governs the day-to-day operations of these organizations may not be seen as rapid or fluid enough to enable the strategic leadership to adequately respond to the situation at hand and direct their forces and resources accordingly. Command and control is not a new concept, nor is it a novel method of leading or commanding over an organization, but it is a helpful method when looking at the way the normal chain of command differs when an organization, such as a police force, goes from normal day-to-day, general operations to a more singular, mission specific operation, i.e. responding to a terror attack (Trnka & Woltjer, 2014, p. 96-97); what Ablerts & Hayes calls the "*C2 approach*" (2006, p. 62-63 & 67). Looking at how the command and control structures functions in these situations are a good way of seeing how the organization and its command structure is coping with this sudden transition from general to mission-specific operations.

As seen in, among others, the works by Alberts & Hayes (2006), Allard (1996) and Builder, Banks & Nordin (1999), command and control, and the theory around it, is a vast field, with much in-depth theory. For the purpose of this thesis, the complexity and the depth of the different theories regarding command and control will not be the focus, but rather a basic understanding of the general concept, will. This is because the problem to be addressed in this thesis focuses on the performance of specific systemic functions that are a part of a basic model of command and control, instead of systemic performance in regards to different, specialised theories of command and control. This also helps in regards to the generality and transferability of potential results (as mentioned in chapter 02.01.02). It is because of this focus on the basic theories and the conceptual understanding that these basic theories are the ones used in this thesis. As will be described later, this understanding of command and control can be said to have originated out of military theory, and in addition, since much of the crisis management systems are to some extent modelled after the military, these theories and the focus on command and control on this level, seems prudent for the purpose of this thesis, and the basic understanding needed.

03.01 – Understanding command and control

Command and control, often abbreviated as C2,[44] is a wide, and a somewhat intangible concept. The name itself implies what is about. It is innately militaristic in its language and definitions, but it is a term and a concept with the possibility for a wide and general use. Vassiliou, Alberts & Agre (2015, p. 1) notes that their definition might as well be describing ordinary management. However, the risks involved in regards to the outcome is far more severe when looking at it from a military or security perspective. Nevertheless, as the theme of this thesis is more directed towards states' security apparatuses – in which the military, and similar organizational models, is an integral part – the interpretation will here be more towards the military side.

This is also natural considering the fact that military organizations – in addition to often having responsibilities in the event of a terror attack – are far more experienced in regards to C2 in fast-changing and volatile situations. As noted by Trnka & Woltjer (2014, p. 83 & 89) the fluidity and high degree of uncertainty of an emergency response operation demands much of the command, and its ability to function and be adaptive in multiple dimensions. Because of this, it is natural that services such as the police, tends to rely on the military's experiences in setting up their own crisis management systems. Because military forces are more experienced in both C2 and logistics under challenging conditions, they will also often be the "trendsetters" and the primary focal point of research into C2, combat logistics[45] and the likes (Hammervoll, 2014, p. 42-44). But, as Trnka & Woltjer (2014, p. 97) notes, one still needs to be aware of the differences in how civilian and military command and control structures are and managed, due to their different functions in society. One clear difference is to what extent the hierarchical structures are being strictly followed. It is a fair assumption to make that while police forces also are fairly rigid hierarchical structures, the focus on hierarchy, and its influence, are more prevalent in the military.

03.02 – Defining command and control

Allard (1996, p. 16) defines the concept of C2, in line with US military parlance, as: "*The exercise of authority and direction by a properly assigned commander over assigned*

[44] For convenience, the abbreviation "C2" will be used (rather than "command and control") from this point on.
[45] While the field of combat logistics, as the name entails, are focused on logistical operations in conjunction with military operations, then just like with C2, it is for the purpose of this thesis seen as a generalisation of logistical operations in conjunction with emergency response operations – and not just military ones.

forces in the accomplishment of the mission. (...)". He further differentiates between C2 as an act in and of itself and C2 as a system that is a prerequisite for that act. He defines C2-systems as: "*The facilities, equipment, communications, procedures, and personnel essential to the commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned.*"

Others, such as Builder, Banks & Nordin (1999 p. 11-12) relies on Allards definition, and subsequently uses it as part of their own conceptual understanding of C2. Alberts & Hayes (2006, p. 32) further builds on that in their definition of the concept of C2, which they describe as:

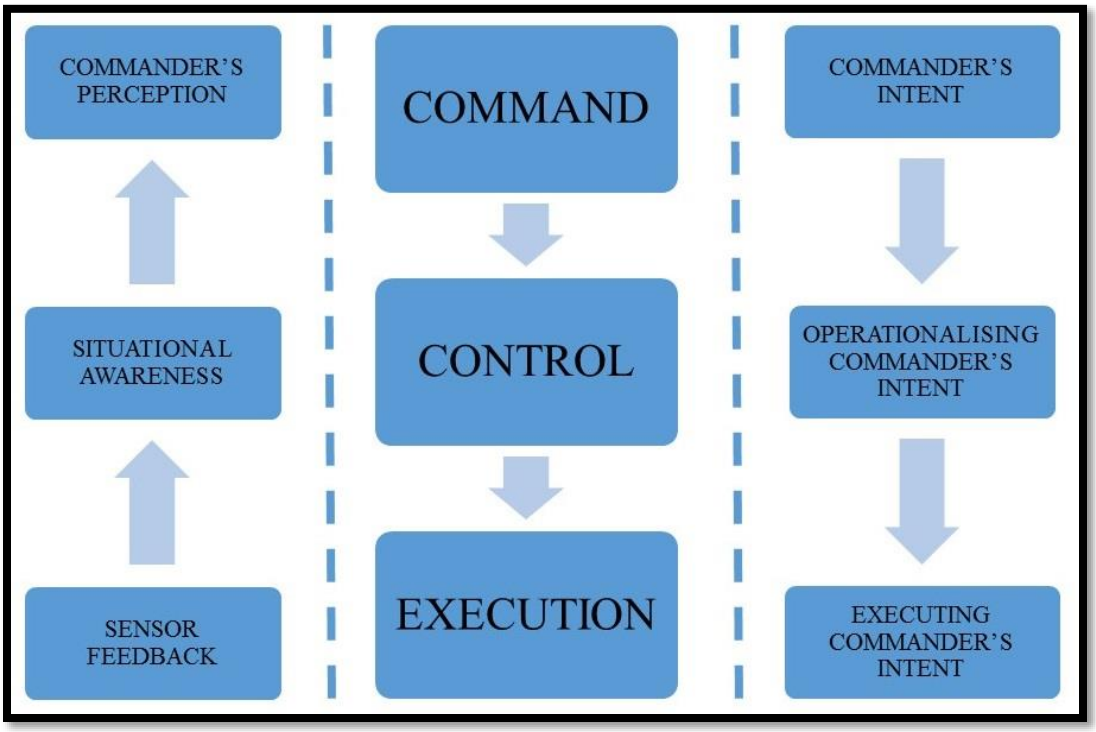
> *"Command and Control is not an end in itself, but it is a means towards creating value (e.g. the accomplishment of a mission). Command and Control is about focusing the efforts of a number of entities (individuals or organizations) and resources, including information, towards the achievement of some task. (...) Definitions of C2 are incomplete and potentially worthless unless a means is provided to measure existence (presence) or quality. (...)"*

Vassiliou, Alberts & Agre (2015, p. 1) chooses to define C2, as a more general and non-military way, as follows:

> *"Command and Control (C2) denotes the set of organizational and technical attributes and processes by which an enterprise marshals and employs human, physical, and informational resources to solve problems and accomplish missions."*

With these ways of seeing C2 as a foundation, the conceptual understanding of C2 in this thesis will be seeing C2 as *a system* rather than *an act*; as described, and differentiated, above with the two C2-concepts defined by Allard.

Depending on the detail and focus of the C2-model, it can be specified by adding additional factors, primarily *communication* (C3) and *intelligence* (C2I / C3I). The addition of communications and intelligence does not necessarily mean a *de facto* augmentation of the model, it merely serves to emphasise the importance of those two factors in the system's ability to exercise both *command* and *control* (Alberts, Garstka & Stein, 2000, p. 69). This is particularly important in regards to exercising commander's intent[46], and preventing information overload (Buckley, 2014, p. 198-199) – Both which are essential parts of a resilient C2-system. This can be schematically displayed as such:



As shown by the figure above, [47] and described by Alberts, Garstka & Stein (ibid. p. 157-165), a C2-system is more easily understood as a continuous process, rather than a locked hierarchical process. The successful execution of the commander's intent relies on it being communicated correctly from command to control, and that control is able to operationalise it in such a way that execution can focus on the task at hand, rather than either having to interpret what the commander's intent for their part is, or how to put it into action. Likewise, their feedback regarding the situation "*on the ground*" needs to be relayed back to control. They, on their hand, have to assess whether this information changes something in the operationalising of the commander's intent, something that they themselves can do, or whether it is information that is deemed essential to commands perception of the situation itself, and thusly needs to be relayed back to command. This filter-function that control has is essential in providing command with the necessary information regarding the situation, while at the same time preventing information overload (see chapters 03.02 and 08.02). It is worth noting the

[46] *Commander's intent* is what the commander defines as the "end-state" of the mission; i.e. what he wants to achieve, and how he wants to achieve it (Alberts & Hayes, 2006, p. 23)
[47] Conceptual similarities can be seen between the figure shown here and the figure Alberts, Gratska & Stein (2000, p. 57, figure 8) uses do illustrate the advantages of information superiority.

similarities between this conceptual figure regarding and the figure showing the different parts of a chain of command (in chapter 01.02.04), as in command - strategic, control - operational and execution - tactical. While this is a highly simplified way of looking at it, the similarities are still worth noting.

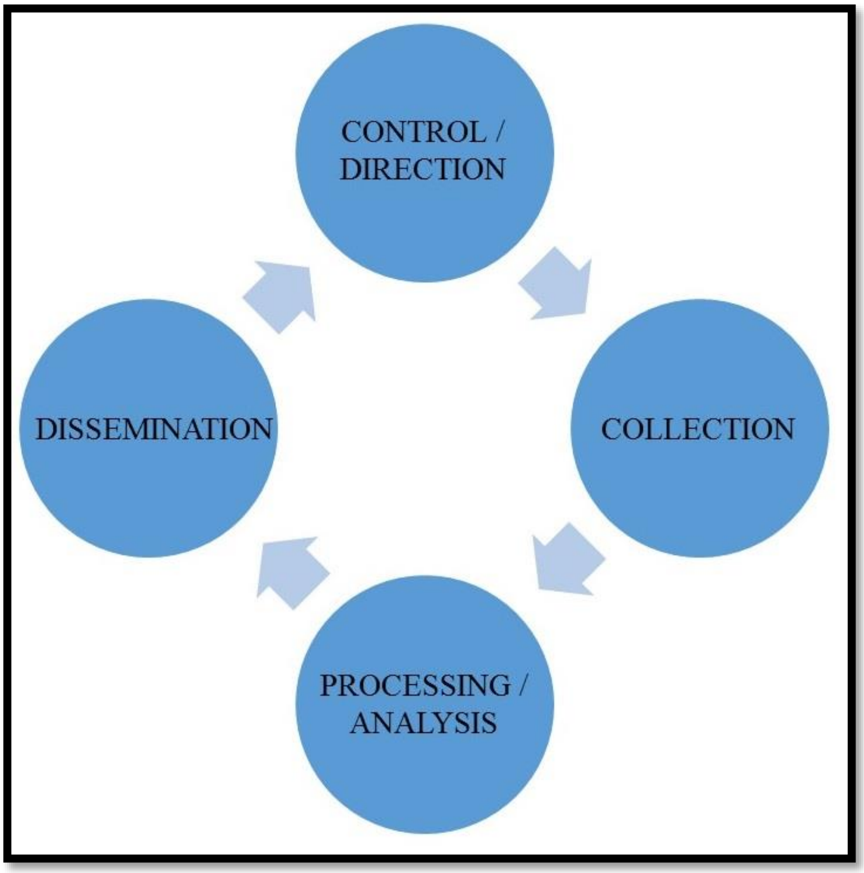
It is important to note that the schematic and the system explained above is not a complete and absolute description of an operational C2-system, but a simplified set-up designed to show the basic framework of a C2-system. The C2-system in place during any of the attacks mentioned in this thesis is vastly more complex, and consisted of many smaller, specialised C2-systems on different levels (Trnka & Woltjer, 2014, p. 88).[48] However, the basic framework of any of these C2-systems are based on the aforementioned architecture. In regards to systems-quality, Alberts & Hayes (2006, p. 188) notes "*(...) quality of command intent, quality of decisions, quality of planning and quality of execution*" as a set of indicators. These indicators define what they see as several key points in a C2-system, and in defining the potential of such a system. These indicators are seen to be in line with the basic framework used to explain the structure of a C2-system, as shown above.

03.03 – Command, control and intelligence

There are several systemic similarities between C2-systems and intelligence systems, in addition to intelligence being a part of C2 (as highlighted in the C3I-model). While intelligence already is an integral part of C2, the C2-cycle itself it can be said to be systemically similar to the way an intelligence system are conceptualised, commonly displayed by the intelligence cycle (Forsvaret, 2013, p. 17-18), (Buckley, 2014, p. 150-153), (Gill & Phythian, 2012, p. 11-17), (Quiggin, 2007, p. 52-53), as shown below:[49]

[48] Such as a system for operational control of the fire-brigades responding to the WTC in New York, a system for tactical control of the FRM-services in London, or a system for the strategic control of police forces in and around Oslo, to give a few examples.

[49] It is worth noting that the cyclic concept is a simplistic view, that does not reflect the complexity of an operational intelligence-process, as also noted by Gill & Phythian (2012, p. 11-17)



While this is also a simplified model, the same cyclic process can be seen repeating itself here. The intent of the command (be that a commander that issues intents and orders, an intelligence-leader requesting information or others) is communicated to the control that operationalizes it and gives the task to execution. The information from collected by execution (the situation on the ground, outcome of ordered actions or raw data) is transmitted back to those in charge of assessing the information, before it is being delivered back to command in a processed and interpreted form. Command can then, acting on that information, either stop the process (provided *end-state* is reached[50]), alter the intent and thusly going around the circle again, or request additional data in line with the established intent, going around the circle again.

This method, in its simplistic and schematic form, is similar to other bare-boned model of knowledge-based leadership or basic analytical (academic) models; identify hypothesis, devise experiment, conduct experiment, assess outcome and amend hypothesis.[51] Looking at C2 in this way can be beneficial in grasping the different stages of it, understanding is as a cyclical, rather than top-down process (Alberts, Garstka & Stein, 2000, p. 160). Moreover, it

[50] See chap. 03.02 regarding “end-state of commander’s intent”.

[51] A simplistic interpretation of the model-figures in Fjelland (2009) p. 91 and 92 (*outcome ~H and H*).

demonstrates that while all these systems are vastly more complex in their operationalised form, their basic methodologies are similarly based on an understanding of logic and knowledgebase understanding and / or decision-making.

04 – Contingency planning and understanding risk

Emergency response operations, whether related to terror, large accidents or natural disasters, are large and complex operations, comprising of a large number of involved personnel and an inherent insecurity of events, particularly during the initial response phase. Different incidents calls for different types of responses, as these incidents all pose their own risks and challenges, both to the safety of involved personnel and victims and possibly larger society. One key factor that is always recurring is the factor of time; emergency responses will always have to "fight the clock" in order to provide the best possible help to those inflicted and contain the situation at hand.

Therefore, in order to properly lead and direct the responding forces and other resources, those in charge are dependent on a set of contingency plans on which to base their course of action on. While no situation is identical, a set of scenario-based plans will still give the commander a severely heightened ability to rapidly initiate a wide range of measures, based upon the scenario they are being faced with. Furthermore, to increase the commander's ability to adapt the scenario-based plans to the specific situation at hand, it is important to have an understanding of risk and risk management. This because the commander most likely will be faced with several risk versus reward decision-making events that are specific to the current situation, and that is not possible to plan for in a set of contingency plans. As with C2, the focus on the theories presented here are to form a basic conceptual understanding, instead of going deep into the specifics of what – on a detailed level – are rather advanced and complex theories and systems.

04.01 – Defining contingency planning

Contingency planning in and of itself is not a difficult term to explain, nor is it sufficiently unusual in everyday speech, that it is seen as necessary to further define beyond: The act of planning ahead for one or more possible negative events, based on a prior risk- and capacity analysis. (Engen et.al., 2016, p. 284 & 287).

Engen et.al. (ibid., p. 282-283) in referring to Meld. St. nr. 29 (2011-2012) (2012, p. 39-40) notes that in readiness and contingency planning, four principles are seen as key to effective civil security work: responsibility, similarity, proximity and cooperation.[52] As Engen et.al. notes (2016, p. 283), these principles apply to both Norwegian and EU civil security and emergency preparedness organizations. In short, this means that:

- Whatever authority or department is responsible for an area (be that a physical area or an area of expertise) under normal conditions, also have responsibility for that area in the event of a crisis.
- The organizational structure during crisis' or mission-specific events should be as similar to day-to-day operations of an organization as possible.
- The crisis should be dealt with on an as low as possible organizational level, ensuring proximity between the affected area and those in charge of the response. [53]
- Each authority or department themselves are responsible for ensuring cooperation with relevant and competent authorities.

As further noted by Engen et.al. (ibid.) these principles are not without their own challenges, especially in regards to a clear distribution and division of responsibility. Likewise, in regards to terror and security-related operations, dealing with the problem on the lowest possible organizational level poses a set of problems on its own. Delegation of powers to declare states of emergencies (even locally), authority to requisition assistance from military forces and other measures that have the potential of a broader – even political – fallout, can be problematic to delegate to far down the chain of command. This both in regards to the ability to have a full overview over the bigger picture outside of the immediate event, and the more ethical question in regards to who should actually have the power and authority to authorise such measures (Dunlap, 2005, p. 793), (Enger et.al., 2016, p. 377-379). On the other hand, in being in close proximity to the event gives the ability to act and react rapidly to fluid events, and the lower down on the chain of command one looks, the more specialists (in regards to relevant expertise on the event at hand) one can expect to find. These challenges will have to be addressed in contingency planning, and a trade-off will sometimes need to be done. This is exemplified in chapter 06.04.01 regarding 11th September 2001, where the FAA Command Center saw the clear advantage of closing the entire airspace, and was able to rapidly act upon it, and in the

[52] Hammervoll (2014, p. 96) also refers to these four principles as central to emergency preparedness.

[53] Proximity does not exclusively refer to physical proximity (as in distance) here, but also a proximity in regards to day-to-day responsibility and professional experience.

debates regarding who had the authority to give the order to shoot down suspected non-compliant hijacked planes (9/11 Commission Report, 2004, p. 25 & 40-41).

04.02 – Risk and risk management

In regards to risk, risk management and the understanding of this, Quiggin (2007, p. 24-30) notes that one has to differentiate between the concepts of *threat* and *risk*, and at the same time see them in connection with each other. He defines threats and risks as follows:

> "*A threat is a potential for an individual or a group to exercise an action which exploits a vulnerability. It does not automatically imply the level of danger that exists.*" (ibid. p. 25)
>
> "*Risk can be defined as the probability of harmful consequences which arise from an action taken by a source to exploit a known vulnerability. A proper risk assessment can be meaningful to policy makers as it implies a course of action or reaction that can be taken.*" (ibid. p. 26).

Looking at the definitions above, it is clear that in order to use these concepts in contingency planning and general emergency preparedness, they must be seen in comparison to one-another. Take the following as an example: In Europe, 151 people were killed in terror attacks in 2015 (Europol, 2016, p. 10).[54] In comparison, there were nearly 155.000 deaths in the UK alone, due to cardiovascular diseases in 2014 (Townsend et.al., 2015, p. 8). Yet, despite the low *risk* of being the victim of a terror attack, the *perceived threat* (i.e. fear) of one are likely much higher. While it is difficult to measure or quantify perceived threat, one can safely say that the fear of terror versus the fear of a heart attack are not comparable in regards to the risks they actually pose in everyday life. In contingency planning, it is therefore important to see the *threat* and the *risk* in connection to one-another and in the context of what one are planning for, by making proper risk assessments.

DSB[55] (2014, p. 20), in writing their National Risk Analysis for 2014, chooses to define risk assessment as the *probability* of a specific incident and the *consequences* that incident will have. In other words combining *threat* and *risk* to make the outcome of the analysis actionable.

[54] While this number applies to EU member states, and does not cover the entire continent of Europe (nor the other parts of *the West*), it is still a valid number for demonstrating the, relatively speaking, few people that die in the West due to terror.

[55] Direktoratet for Samfunnssikkerhet og Beredskap.

Furthermore, they see risk assessment as a part of a larger system, *risk management*, and defines the concept as a whole as:

> "*(...) the entire process of defining in what areas and for what adverse events risk analysis should be conducted, conducting risk analyses, evaluating the risk results (whether the level of risk is justifiable or not) and implementing any risk-reduction measures.*" (ibid.)[56]

This is similar to the definition of risk management used by Aven; "*Risk management encompasses all measures and activities that are being taken in order to manage risk.*"[57] (2015, p. 13). Keeping in line with the theme of this thesis, the act of learning from other comparable events and, when needed, implementing these lessons, if they have a risk-reducing effect, can be seen as a central part of risk management. Likewise, this definition shows that risk management can be thought of as a *cyclic*, rather than simply a *linear* process, in which constant evaluation, implementation and re-evaluation are essential (not unlike the intelligence cycle as mentioned in chapter 03.03). This can further be seen in conjunction with Alberts (1996, p. 44) pointing out that C2-systems "*(...) are never complete and will be continuously undergoing transitions (...)*". This need for a cyclic approach with frequent re-evaluations becomes even more relevant when the threat one is trying to protect against is one that has the ability to adapt when faced with various counter-measures. A natural disaster or a major accident happens without a malicious intent or a will of its own. While many factors affect the progression and outcome of such an event, terror attacks differ in the vital points of *learning* and *adapting*.

As explained in chapter 01, terrorists learn and adapt with the goal of circumventing obstacles designed to avert or limit their actions. Once a vulnerability is discovered in one country's system, other countries with similar systems in place should take heed. While this may be most visible in ways to avoid detection by security services during planning and preparation, or circumventing target hardening-systems,[58] it is just as relevant when it comes to measures and tactics to obstruct the immediate response once an attack is initiated. The Mumbai attack in 2008,[59] with the use of multiple IEDs placed in various locations and the use of several small, but highly mobile teams of attackers to confuse the responding security services (Rabasa

[56] The translation is taken from the English version of the National Risk Assessment 2014 (DSB, 2014).

[57] Own translation. Original text in Norwegian: "*Med risikostyring forstås alle tiltak og aktiviteter som gjøres for å styre risiko.*"

[58] Such as the use of binary, liquid explosives in order to circumvent security screening, in the aforementioned 2006 "liquid bomb plot" in UK.

[59] See chap. 06.05.02.

et.al., 2009, p. 21), and the subsequent resurgence of this tactic in the 13th November 2015 attacks in Paris (Europol, 2016, p. 22) demonstrates this. Looking at counter-terrorism responses in other countries and trying to learn from them should therefore be an incorporated part in the management and evolution of any emergency preparedness system.

DSB (2014, p. 22) also notes that the most severe scenarios, of which terror attacks can be said to be part of, have an extra challenge in regards to risk assessments. Because such events are – relatively speaking – rare, there is often a lack of statistical data, which in turn increases the level of uncertainty in the risk assessments. They refer to Flage & Aven (2009) that puts forward three indicators used to assess the strength of the knowledge base in regards to risk assessment:

1) *Access to relevant data and experiences*
2) *Understanding of the incident / phenomenon*
3) *Consensus among those participating in the risk assessment.*

While it is worth noting that the article where DSB gets these indicators (ibid.) deals with *quantitative* risk assessment, and not *qualitative* risk assessment as this thesis, these indicators are none the less considered applicable here. And seeing as terror incidents are a rare occurrence in any given Western country, all relevant data, such as those from comparable countries, should be utilised in order to minimise the uncertainty of the risk assessments, thusly making the foundation for the risk management that much better.

04.03 – The importance of contingency plans in preparedness

Engen et.al. (2016, p. 283-287) sees contingency planning as a part of a larger emergency readiness system. Here, a contingency plan are the consequence of a risk analysis and an emergency preparedness analysis (abbreviated to “EPA”). The outcome of the risk analysis and the EPA lays the groundwork for creating a contingency plan, by looking at potential threats (and vulnerabilities, in conjunction with these threats), the risk they pose, available resources to either prevent, mitigate or respond to these threats, and how such a response should be organized and conducted. The aim here will always be to ensure a best possible response should any of the threats become a reality. Hammervoll (2014, p. 154) also notes that when command leadership fails, it is often attributed to problems with, or the lack of, contingency planning or poor coordination between different actors / systems. Due to the likely chaotic situation that is typical during the initial phase of a terror attack, such lack of plans will be nearly impossible to mend at that point in time. As such, it has to be planned for ahead of time. DSB (2004, p. 21) notes this in their review of lessons learned after the 2004 Madrid attacks: "*Others point out that it is important to have a continuous process in which plans are reviewed and updated according to systematic and dynamic risk assessment analyses.*"[60] This is not in and of itself any ground-breaking conclusion, but the fact that it is brought up as a central point in building resilient systems and functioning contingency plans, time and time again, underlines its importance. It is especially important to include C2 in these plans (also noted by DSB, ibid., p. 13, 24-25), as will be discussed in the sub-chapter below.

04.04 – The importance of command and control in contingency planning

As previously explained, C2-systems, while simple in its core structure, are vastly complex when they become operationalised, or "activated". It is therefore imperative that the structure and setup of a C2-system that is intended to be used during extraordinary events; i.e. terror attacks, mass-casualty events and natural disasters, are already planned and designed. Security services, such as the police force, will always be operational and thusly have a standing C2-system that is working. These systems are designed to operate in normal conditions and will have to be altered and / or reinforced in the event of extraordinary conditions. And as time is of the essence when such incidents occur, one will not have the opportunity to figure out how to reorganize in order to properly respond after the event is a fact. Therefore, it is of utmost importance to have a template for how to organize in the event of such incidents. Most of the time this will not lead to a brand new organizational structure – there is neither the time nor the place for such comprehensive changes – but rather this will lead to a strengthening of the functions that are deemed instrumental in responding to the event at hand. Moreover, because different events will call for different types of responses, this strengthening can differ depending on whether it is a terror attack, a major accident (such as a plane-crash or a larger maritime accident) or a natural disaster (Trnka & Woltjer, 2014, p. 84-85). These functions will therefore have to be identified in the planning-process, preferably as a part of the EPA.

Trnka & Woltjer (ibid.) also differentiates between *emergencies*, *disasters* and *catastrophes* in regards to different general states of an incident in order of increasing severity. In this regard, a terror attack alone will not reach the level of catastrophe. That would, as Trnka

[60] Author's translation. Original text in Norwegian reads: "*Andre mener det er viktig med å føre en kontinuerlig prosess med å oppdatere planverk basert på systematiske og dynamiske ROS-analyser.*" (DSB, 2004, p. 21)

& Woltjer (ibid.) sees it, require the attack make societal services and infrastructure unavailable or incapacitated for a prolonged time. As the attacks on 11th September 2001 undoubtedly are the single largest terror attack, by a non-state actor against a country in peacetime, did not reach this level, it is hard to imagine any other attack reaching that magnitude of impact. That level is thusly "reserved" for major natural disasters, like the 2004 tsunami, or a near full-scale military attack – none of which is relevant for this thesis. A terror attack will in this regard classify as either an emergency or a disaster. As Trnka & Woltjer further notes, one characteristic of these are the scarcity of both operational and C2-resources, and the need for cooperation and interdependence between different organizations. To be able to function effectively with scarcity of command-capacity, and the possibility for intermittent disruptions of these capacities, the need for C2 to be included in contingency planning becomes clear.

04.05 –Planning for "Black Swans"

A terror attack in a country not at war or plagued by heavy internal turmoil, will by its very nature always come as a surprise, more or less. On the one hand; if the attack were to not come as a surprise it would have to be expected with a high level of certainty, and as such it would most likely have been averted by police or security forces, or at least have led to a heightened state of alert and strengthening of response systems (as mentioned in chapter 01.04). On the other hand it is, statistically speaking, highly improbable to be killed in a terror attack in the West. Many terror attacks, especially those that utilise new tactics and / or attack previously untouched targets or countries, are low probability and high impact events, and are very – if not almost – impossible to predict; so-called "Black Swan events" (Taleb, Goldstein & Spitznagel, 2009, p. 78). Planning for such an event can therefore be a challenge. Building up an organizational structure to respond to a terror attack that might never happen is also a costly affair, both in regards to resources (people and money) and time. Not to mention when it comes to necessary equipment, training and readiness exercises.

Naturally, the planning will often focus on the known threats and risks: what we know to be dangerous and what we can realistically envision happening. This comes as a natural result of the prior risk-analysis, because it is difficult, if not impossible, to assess the risk of something completely unknown happening, the problem of so-called "ludic fallacy" (Nafday, 2009, p. 193), because "*No probabilistic model based on in-box thinking can deal with out-of-box type events.*" (ibid.). This is not in and of itself a new problem or bias. In intelligence (see chapter

03.03) and other similar systems (like risk management) this is also seen as a potential systemic problem (Quiggin, 2007, p. 56-58). In addition, the obvious dangers will naturally be the primary focus. Due to the potential cost of preparing against such unlikely or even unthinkable event, that can also be used as an excuse not to plan for it, even though, in a risk management perspective, this can hardly be said to be "good enough" (Aven, 2015, p. 164).

Nafday (2009, p. 194) uses the example of the Oklahoma City bomber:[61] "*One can not estimate probability of bombing for the Oklahoma City federal building, since the event is not a random process. These 'left field' outliers can vitiate all attempts at prediction since there is no historical precedence or data for prognostications.*" He further argues that because of this, there is a need for a shift away from solely traditional risk management, based on statistical probabilities, and focus on "*(...) strategies for dealing with the consequences of such unforeseen events.*" (ibid.). A series of strategies are suggested (ibid., p. 194-197), among them; prevention, risk-reduction, risk transfer, design-based, regulation based, control of consequence based and response based. Obviously, preventive strategies are the best ways to deal with terror attacks, by "simply" preventing them from happening. However, some of those preventive strategies such as barriers[62] can cause a would-be attacker to use a more powerful attack-strategy (such as a larger bomb, hence causing even more damage) or simply choosing another target (Bjørgo, 2013, p. 67-68), and while that might move the black swan event to another location, the attack will still happen.[63] Other strategies suggested by Nafday are system resilience trough, either or both, robustness and redundancy (ibid., p. 196-197). These will be further discussed in chapter 05.

[61] Referring to the attack in Oklahoma, USA, where Timothy McVeigh in 1995 used a massive VBIED to attack and destroy the Alfred P. Murrah federal building, killing 168 people and injuring over 680 (Bolz, Dudonis & Schulz 2012, p. 224).

[62] In this context *barriers* are both physical barriers and no-entry zones – see A2/AD and target-hardening.

[63] It is worth noting that Nafday adopts the *engineering* perspective, and thusly the width of potential black swan events are not limited to terror, but also accidents (meltdowns, blowout etc.) and natural disasters (earthquakes, tsunamis etc.).

05 – System resilience

As mentioned earlier, there are many things that can have an adverse effect on the C2-systems' ability to function properly during the response to a terror attack. It can be that the attack directly affects parts of the infrastructure that commanders and others on the strategic level rely on, like buildings, critical infrastructure and so on. However, the more probable is that the system will be affected by challenges such as absent personnel, outdated plans, problems with – and even loss of – communications etc. To ensure the system's ability to function, and to prevent loss of response-capability and capacity in the event of unexpected or adverse incidents, it is important to ensure the system has the necessary degree of *resilience*.

As described by Johansson & Pearce (2014, p. 79) there are several different perspectives in regards to defining a systems *agility*, and these are not necessarily consistent with one another in regards to their understanding of what actually constitutes agility in C2. Johansson & Pearce (ibid.) still notes that *resilience* is a recurring theme. Because the concept of *resilience* is a recurring theme in defining organizational agility and effectiveness in C2-systems, it can be said to hold a central part in C2, and thusly it has relevance in regards to assessing the system's performance.

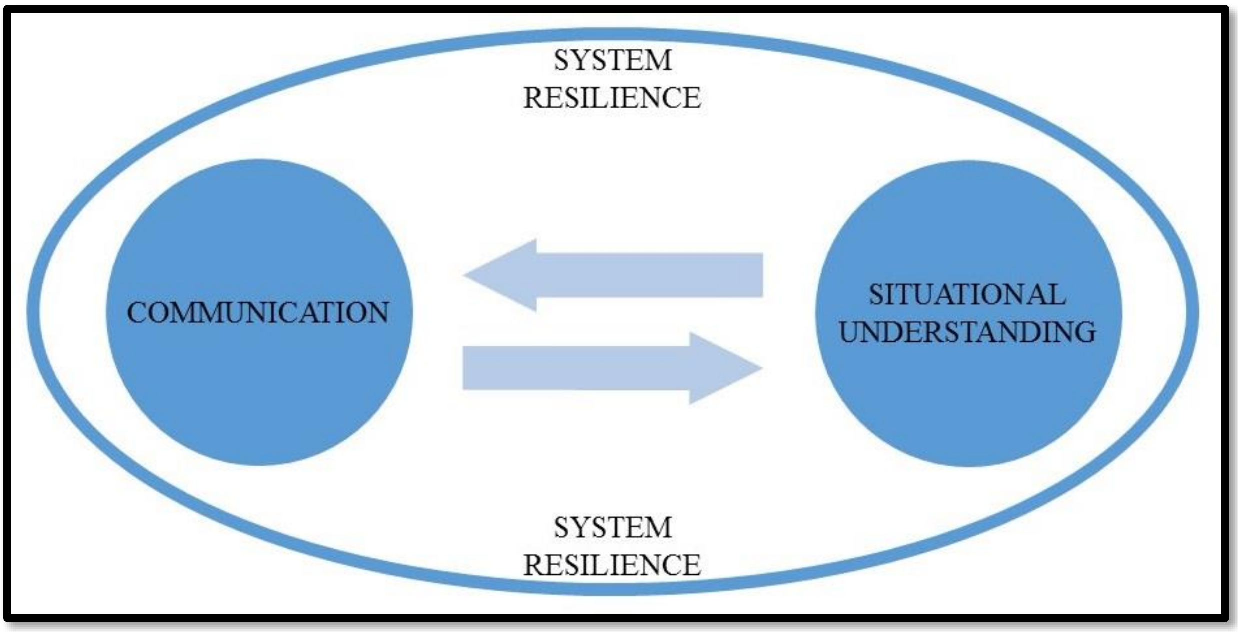
Among those mentioned by Johansson & Pearce (ibid.) are Alberts & Hayes. In describing their definition of *agility* in C2-systems, Alberts & Hayes (2006, p. 186-191), mentions *resilience* as one of the parts of this. They define resilience as "*The ability to rebound from damage or misfortune*" (ibid., p. 189). Others, like Boin & McConnell (2007, p. 54) adopts a similar view in that resilience is "*The ability to 'bounce back' after suffering a damaging blow*". Aven (2015, p. 45) similarly defines resilience as an organizations ability to identify, adapt and absorb changes, disturbances and surprises. He further notes that resilience goes further than robustness by not being based on a set event, but rather being more general in regards to what it allows the system to face (ibid.). Likewise, Hammervoll (2014, p. 214-215), notes that such flexibility in a system, although cost-increasing (in regards to spending and allocation of resources on a "just-in-case" basis), leads to an increased ability to handle uncertainty and events that are out of the area of control of the system, and ultimately increases the systems capability and capacity.

Nafday, which writes from an engineering standpoint, divides resilience into two strategies: *robustness* and *redundancy* (2009, p. 196-197). He defines these respectively as:

> "*A resilient system survives and carries on essential functions despite variations beyond the design envelope, by adapting itself to a new and safe equilibrium state (e.g., via load re-distribution, avoiding cascading failure etc.).*"
>
> "*System resilience can be achieved by providing redundant design and alternative load paths to ensure that the loss of a single component would not lead to overall structural collapse.*"

Obviously, and as already noted, these are definitions from an engineering point of view, but looking at them metaphorically, the same basic understanding of system resilience can thusly be said to be found in both structural safety and societal security.[64] Hence, these definitions can be said to be quite basic in the understanding of risk, vulnerability and the mitigation of these.

In regards to the topic of this thesis, the two concepts of communication and situational understanding, and their interdependency on each other, can be illustrated by the figure below:



Both parts can be seen as dependant on each other. If one experiences a drop in capacity or loses one or more core capabilities, it will also adversely affect the other part. System resilience can in this case be seen as something that encompasses the entire system:

[64] Engen et.al. (2016, p. 26) notes that in regards to the "safety" and "security", one should be cautious in reading too much into the difference of these words, even though it is advantageous to have a lingual differentiation, such as safety referring to accidents and security referring to malicious acts. The context of which the words are use should still be paramount in understanding their intended meaning.

communication, situational understanding *and* their interdependency on one another. Due to this interconnectivity, it will have limited effect to focus the build-up of resilience around the individual parts of the system, because the value of the system is greater than the sum of its individual parts. It is the system itself and not its individual parts that should be the focus for a build-up of systemic resilience capabilities and capacity.

Prudent crisis management dictates that one cannot rely completely on a system that is so fragile that a performance-drop in one of its parts will paralyze the entire system. While a drop in productivity and a general reduction of capacity may not be avoidable in such a situation, the important part is to ensure the continued function of system itself, as a whole. In debating why resilience is important, Alberts & Hayes (2006, p. 190) reasons that such resilience is important because:

> “*Resilience will be important because we cannot assume that adversaries will not be able to strike first or otherwise seize the initiative. Hence, we will suffer casualties and have our operations disrupted. This cannot be allowed to lead to failure.*”

While the militaristic style of the language, as noted earlier, becomes obvious in passages like this, its core message can be said to be preventing failure due to loss of initiative or other forms of disruptions. This will be the guiding definition and understanding of resilience in this thesis.

In regards to defining other forms of disruption, this can be said to be anything that will impair the system’s ability to properly function at the level it is expected to function at, within a reasonable margin of error. Elements such as loss of communications, inadequate plans, poor or simply wrong situational understanding are among many examples of what *other disruptions* entails. Communications and situational understanding itself will be further described in chapter 07 and 08.

06 – The attacks

In the following chapter there will be given a synopsis of each of the three attacks.[65] Each one is based upon the official account as presented by a parliamentary and / or investigatory committee. The synopsis is not meant to be a complete narrative of the attacks, but to focus on the theme of the thesis, and elements of the attacks and subsequent response that is relevant. A further in-depth view of the relevant incidents will be addressed separately in their corresponding chapters (7 and 8).

06.01 – USA – 11th September 2001

The 9/11 Commission Report (2004, chapter 1 and 9) recounts the attack as follows: On the morning of 11 September 2001, Mohammed Atta, and nine other hijackers passed, more or less without hindrance, through the security at Logan Airport in Boston. They soon after boarded the two flights known as American 11 and United 175. At about the same time in Dulles Airport in Virginia, five others passed through airport security and boarded flight American 77. Roughly simultaneously four other hijackers boarded Flight 93 out of Newark. All four flights were transcontinental, and thus heavy laden with fuel. At times between 08:15 and 09:30 that morning, all four planes were hijacked.

The hijackings all followed the same pattern and plan; some of the hijackers, sitting in seats in the front of the plane, rushed the cockpit, killing the pilots with small knives they had brought on-board. Then, while the pilot-hijacker[66], sitting a few seats further back, took control of the plane, one or more flight-attendant or passenger in the front of the plane would also be stabbed and killed to frighten and subdue the others passengers. Alternatively, pepper-spray or CS-gas[67] would be used. The passengers were to be led under the impression that it was a hijacking and the aim of the hijackers were to return to the airport and negotiate with the authorities. The pilot-hijacker would then alter the planes course and, critically, turn of the

[65] All dates and times given here are local, and given in the 24h-format.

[66] Each group of hijackers had one person that was their designated pilot, and that had received training in piloting aircrafts.

[67] CS-gas is more commonly known as “tear-gas”; a non-lethal gas that causes pain in mucous membranes and induces a choking-like sensation. It is, just like pepper-spray, commonly used as self-defence sprays and was at the time readily available over-the-counter in the US.

planes transponder. In doing so civilian air traffic control[68] would only get limited information from the plane via their ground-radar, as the plane itself stopped transmitting data from its instruments – such as course, speed, height and identity.

On the flight American 11, a flight attendant identified as Betty Ong was able to contact American Airlines operations centre via the planes phones-system at 08:19 and alert the company to the hijacking. Likewise, another flight attendant; Madeleine Sweeny, also managed to contact the operations centre, and they were both thusly able to relay information about the event to the ground. At the same time, the pilot had, in thinking he used the planes intercom, sent a radio-message saying that the plane was hijacked and that they were returning to the airport. At 08:46 American 11 hit the North Tower at the World Trade Center,[69] causing a massive explosion. At between 08:42 and 08:46 the hijackers on United 175 seized control of the plane and it struck the South Tower at the WTC at 09:03, causing an equally large explosion.

At some time between 08:51 and 08:54 American 77 was hijacked and altered its course. It would strike the Pentagon at high speed at 09:37, causing a large explosion. At 09:28 United 93 was also hijacked. The plane altered its course and headed towards Washington DC. Due to availability of in-flight phones and some cellular service, several passengers on United 93 learned that other planes had been hijacked and crashed into buildings, and at 09:57 they attacked the hijackers in what is thought to be an attempt at regaining control of the aircraft, or at the very least, to prevent the plane from reaching its target. At 10:03 the plane crashed in a field in Shanksville, Pennsylvania.

Almost immediately after American 11 had struck the North Tower both FDNY and NYPD[70] scrambled its personnel and responded to the scene, and started making their way up the building towards the crash-site to facilitate evacuation and to combat the fire. When the South Tower was struck, a similar operation was conducted there also. The South Tower collapsed on itself at 09:58, as a result of the damage from the impact and additional weakening of its core structure due to the fire caused by the crash and intensified by the large amount of fuel that had been in the plane. Almost immediately after, an evacuation-order was given to the personnel in the North Tower. That tower collapsed at 10:28. A similar fire- and police response

[68] Air traffic control is a generic term, and is in this thesis meant to cover all types of civilian air traffic control, such as Area Control Centres, Air Route Traffic Control Centres, Flight Information Regions etc.

[69] The WTC complex were made up of several buildings, the most notable ones being the "Twin Towers"; known as North Tower and South Tower of the WTC, alternatively One World Trade Center (north) and Two World Trade Center (south).

[70] New York Fire Department and New York Police Department.

occurred at the Pentagon, where a section of the impact zone collapsed on to itself at 09:57. In total, 2977 people were killed, and over 6000 injured, as a result of the attacks.[71]

06.02 – England – 7th July 2005

The ISC Report into the 7/7-attacks (2006, chapter 1) and the House of Commons report no. 1087 (2006, p. 2-6) recounts the attack as follows: On the morning of 7 July 2005, Mohammad Sidique Khan, and three other suicide-bombers, boarded a London-bound train from Luton station, just north of London. They arrived at King's Cross station in London and split up at around 08:30, where they subsequently split up. Three of them taking various subway-lines, and one walking outside, later taking a bus. At approximately 08:50 the three attackers in the subway detonated the PBIEDs they are were carrying in their backpacks. A little while later, at 09:19 the fourth attacker entered a crowded bus near King's Cross station. He detonated his PBIED aboard the bus at 09:47. In total, 52 people were killed, and nearly 800 injured, as a result of the attacks.[72]

06.03 – Norway – 22nd July 2011

The official report from the 22 July commission; NOU 2012:14 (2012, chapter 2) recounts the attacks as follows: Just before 15:00 on 22 July 2011, Anders Behring Breivik drove a van carrying a 950 kg fertilizer-based[73] VBIED from the western part of Oslo, and parked it outside the Government quarters[74] at 15:17. He lit the fuse to the VBIED and walked away from the scene in a uniform made to resemble that of a police officer. The VBIED detonated at 15:25, killing several people and causing massive structural damage to the surrounding buildings. Breivik got in a car he had parked nearby the previous day, and drove out of Oslo towards the island Utøya, located north-west of Oslo.

At just before 16:30 he arrived at the dock on the landside of Utøya. He identified himself as an officer from the Norwegian Police Security Service (PST), and said he was sent there to ensure the safety of the Labour Party summer youth camp that was on the island. A

[71] Figure not including the 19 hijackers, which all also died in the attacks.

[72] Figure not including the 4 bombers, which all also dies in the attacks.

[73] Commonly known as an ANFO-bomb (Ammonium-Nitrate Fuel Oil); a mixture of fuel-oil and fertilizer. (Bolz, Dudonis & Schulz 2012, p. 244) The same kind of bomb used by, among others, Thimothy McVeigh in the Oklahoma City bombing in 1995 (ibid. p. 224)

[74] NO: *Regjeringskvartalet*

short while later he was ferried across the lake to the island. He arrived on the island at 17:17, and at 17:21, near the islands main buildings,[75] he began a shooting-spree, firing indiscriminately at the people on the island. Due to the lack of boats on the island, and the distance from the island to land, many people were not able to evacuate themselves from the island.

At 18:27 the first unit from the polices' Emergency Response Unit "Delta"[76], disembarked on the island, not far from where Breivik had landed just over an hour before. A second team of Delta-officers also arrived a minute later. Working their way inwards on the island, they encountered Breivik near the southern part of the island at 18:34, and arrested him. He had continued his shooting-spree up until mere minutes before his arrest. In total, 77 people were killed, and over 300 injured, as a result of the attacks.

06.04 – Defining the golden hour

With reference to the definition of "the golden hour" in chapter 01.02.03, this sub-chapter will specify the definition of the golden hour in regards to the 11th September 2001, the 7th July 2005 and the 22nd July 2011 attacks, by setting a specific time for the end of the golden hour. The start of the golden hour will be at the time the attack itself begins. Even though all these attacks are multi-pronged, the start-time of the golden hour will still always be at the time of the first attack. The chances of two or more, unconnected terror attacks occurring within minutes of hours from one another are astronomical, so it is assumed that further attacks, after the first one has begun, are identified as and treated as a part of the already ongoing attack, by the police, FRM- and other relevant services.

In all the attacks the initial response from the first-responders (police- / security services and FRMs) begins almost immediately after the attack has begun. Although response-time is an obvious factor here, it is safe to assume that these resources will be scrambled as soon as the information of an attack reaches them. However, this is not seen as sufficient to qualify as a move to start the process of seizing the initiative of the situation, hence "ending" the golden hour. This is because the immediate dispatching of these forces are, basically, an automated response to any major incident, whether it is a terror attack or a large-scale accident. Therefore, the plan for these first-responders are not yet specific enough to effectively counter the attack,

[75] Known as Hovedhuset (EN: The *Main-house*) and Kaféhuset (EN: The *Coffee-house*).

[76] The national counter-terrorism / hostage rescue force in the Norwegian police.

simply because the access to information is not yet sufficient to formulate an adequate plan of action.

06.04.01 – 11th September 2001

While the attack started a few minutes earlier, with the actual hijacking of the planes, the call from flight attendants Betty Ong and Madeleine Sweeny aboard American 11 to American Airlines Operations Center at 08:19,[77] marks the point where the incident – at that time interpreted as a single-plane hijacking – became known to others on the ground, and the information forwarded to the government (9/11 Commission Report, 2004, p. 5). As time moved forward, similar reports came in from the other three planes: United 175, American 77 and United 93 (ibid., p. 7-13). The end of the golden hour is set to 10:15, at the time when the order to shoot down non-compliant hijacked aircrafts, so-called RENEGADE[78] was given (ibid., p. 40-41). In regards to this attack, the golden hour covers roughly two hours.

At approximately 08:38, NEADS[79] ordered two F-15 fighter planes on alert, and as the 9/11 Commission notes: "*The air defence of America began with this call.*" (ibid., p. 20). While this is a move towards mounting a response capable of regaining the initiative, this is not seen as the end of the golden hour, basically because the end-state of the attackers (crashing the planes into their target buildings), had not yet became apparent, as the first plane did not crash into the WTC until 08:46, so there was no plan of action to face such a threat, as it had not yet become apparent. While this order is a start, it would not in any way have prevented or disrupted the following attack, mainly because the confusion over what planes were hijacked, where they were, and where they were heading. In addition, the fighter planes would not have been able to effectively intercept and disrupt hijacked the plane(s), because the order shoot down RENEGADE planes had not yet been given, and their standing ROE[80] did not allow them to

[77] The call was re-routed from the American Airlines Southeastern Reservation Office to the Operations Centre.

[78] RENEGADE is the joint NATO / EU definition for a plane that is intended to be used by terrorists or other hostiles, as a weapon, primarily by using the plane itself as a missile, like seen on 11th September 2001. See Kölle, Markiarian & Tarter (2011, p. 97) and Zubrzycki (2013, p. 130-135). The concept was *not* in place during the 11th September attacks, but the term will be used here to describe such planes.

[79] Northeast Air Defence Sector. A part of the US Air Force, tasked with air-defence of the northeast part of the US mainland.

[80] Rules of Engagement – A set of rules that governs how and when a military unit can use (lethal) force, or otherwise engage hostiles.

engage civilian aircrafts. Likewise, it is worth noting that the RENEGADE concept, as it stands now, was not a part of the ROE at the time of the attack, but came as a result of the attacks.[81]

At 09:25 the FAA[82] Command Center, being aware of several hijackings and the two plane crashes at the WTC, ordered a so-called "nationwide ground stop", effectively closing the airspace over the entire US mainland (ibid., p. 25). As a result, as planes landed, potential RENEGADE planes would be easier to identify, and further actions, such as scrambling additional fighter planes to identify and intercept, could be done far more effectively and precise. However, as previously noted, since the shoot-down order had not yet been given, these fighter planes would have had a significantly limited ability to act. It is also worth noting that this decision to close the entire airspace was taken, somewhat unilaterally, by the manager at the FAA Command Centre in Herndon, while the measure itself was still being debated over at FAA headquarters.

The order to shoot down RENEGADE planes came approximately 10:15. This order was initially primarily directed towards two separately scrambled F-16 fighter planes that was originally tasked with intercepting American 11 (ibid., p. 34), now on combat air patrol[83] over Washington DC and redirected to intercept United 93 that was, erroneously,[84] feared to be flying towards Washington DC (ibid. p. 40-41). Even though this order was initially directed towards a "ghost-plane",[85] this order is seen here as the end of the golden hour. A lot was done in the time before this, but until this order came, the responding forces did not have any means to realistically be able to counter the terrorists.

While this can seem as a long golden hour it is worth noting that even though the attack technically started at approximately 08:15, it was not until 08:46 that the second plane crashed into the WTC that anybody realistically could have been able to fully comprehend that what was actually going on was more than a hijack- and hostage situation. Also, even though all four hijacked planes had crashed by 10:15, the government did not know this, and there was a high

[81] At the time the prevailing view was that an order to shoot down a civilian plane in US airspace would have to come from the so-called National Command Authority (NCA); meaning the president and / or the secretary of defence. While not implemented into the ROE, the possibility of a RENEGADE was still known by the late 1990s. (The 9/11 Commission Report, 2004, p. 17).

[82] Federal Aviation Administration.

[83] Combat air patrol (CAP) is a defensive mission for fighter planes, where they are tasked with intercepting and preventing other aircrafts from entering a specific area, be that an air defence sector, a specific target (such as an aircraft carrier) or a combat zone.

[84] United 93 had at that time already crashed in Shanksville, Pennsylvania, at 10:03, and the fear that it was closing in on Washington DC, was because the FAA was monitoring the plane's projected flight vector and not its actual radar signal, and reporting this to the Secret Service (9/11 Commission Report, 2004, p. 41).

[85] A plane erroneously believed still to be flying, when in fact it had already crashed.

and reasonable fear that several other RENEGADE planes or other forms of attack was still to come. Taking into account the scale, scope and complexity of the attack, and the information available at the time (10:15) this assessment of potential further attacks is seen as realistic and reasonable.

06.04.02 – 7th July 2005

While the attack began at approximately 08:50, with the near simultaneous detonation of three PBIEDs in the London Underground, the end of the golden hour is set to 10:55. This is because when the fourth PBIED was detonated on a bus almost an hour after the first attacks, at 09:47 (The ISC Report into the 7/7-attacks, 2006, chapter 1), the threat and possibility of further attacks are seen as highly probable. In the regards to this attack, the golden hour covers roughly two hours since the start of the attack.

A so-called "Code Amber" was issued at approximately 09:14. This calls for all Underground trains to stop at the next station and hold there until further notice (Coroner's Inquest, 2011, p. 41). The Underground network was evacuated by 09:40 (ibid.). On one hand, it can be argued that this evacuation marks the end of the golden hour, but when the fourth PBIED detonated on the No. 30 bus at 09:47 (when the evacuation still for all intents and purposes was ongoing, as people still was massed just outside the Underground stations), it became apparent that the threat was against the whole public transport sector in London. Also, before the fourth bombing occurred, the risks of such further attacks, considering the already clear similarities to the, then recent, attacks in Madrid,[86] are assumed to have been fairly obvious, and the fear of further attacks therefore justified. Because of this, a need to both clear people away from public transport hubs, and prevent more people from arriving, became apparent. As a result, at 10:55 the Home Secretary announced to the public that all public transport had been suspended (House of Commons report no. 1087, 2006, p. 7).

It is highly likely that this decision was taken sometime *before* this message was conveyed to the public, but due to the entire concept of public transport, this closing can hardly be seen as having taken full effect before the public are actually informed about it. If not, it is likely that people still would gather at public transport stations, and under the threat of a sustained attack against public transport, such gatherings of people can prove to be a high-yield target for any remaining terrorists. And in such a scenario, even though the city is virtually

[86] See chap. 06.05.01.

saturated with armed police and other responders, such potential high-yield targets needs to be either significantly hardened, or made less attractive as a target, such as by directing people away from it, thusly dispersing crowds – at least to some extent. While this will not necessarily prevent another attack, it will at least lower the potential damage of an attack, thus potentially making other attackers alter their plans or targets.

06.04.03 – 22nd July 2011

While the attack began with the VBIED detonating outside the Government quarters at 15:25, the end of the golden hour is set to 17:33. It was at that time that the first unit from "Delta" was redirected from the blast-site in Oslo to Utøya, where just before, reports of shooting had started coming in (NOU 2012:14, 2012, p. 27-28). This means that in regards to this attack, the golden hour covers roughly two hours since the start of the attack.

While police and FRMs responded rapidly to the blast-site, there were still a great deal of confusion regarding the person responsible for the bombing, and his whereabouts. Several sightings of the potential bomber and another vehicle said to be at his disposal were reported to the police, but – in part due to the lack of a functional national alarm system – this information was not sufficiently spread out among the various police forces (ibid., p. 17-22). Hence, it was known that the bomber was "on the loose", and the potential of secondary attacks was obviously present, but, besides from the occasional target-hardening, a joint plan or a joint effort to locate and neutralize this threat, was not effectively put in place. The main response was still, logically, centred in and around the blast-site at the Government quarters.

When the first Delta unit was dispatched to Utøya at 17:33, after the information about the attack occurring there, a detailed plan of action still was not formulated. However, the act of deploying the primary counter-terrorism capability of the police towards that site, signals the start of a set of actions to regain the initiative and control of the situation, as more or less random target-hardening was replaced by a direct effort to engage and neutralize the attacker.

06.04.04 – Notes to these golden hour definitions

In all the three attacks above, the golden hour have been set to roughly two hour from the start of the attack. This is not based on the time passed since the attack, but on when actions capable of regaining the initiative has been taken. It is worth noting that even though this seems to have taken roughly two hours in the all attacks that are looked at here, this – while albeit an interesting point – is not to be taken to mean that it generally takes two hour for a sufficient response to be mounted. The sample range here is far too small to make such a conclusion, and the basis here is an *interpretation* of when the response is sufficient to warrant an end to the golden hour, as to per its definition here.

06.05 – Similar attacks

While the three attacks mentioned above will be the focal point of this thesis, the attacks in Madrid in 2004, Mumbai in 2008 and Paris 2015 will be briefly mentioned here, as they also are topical to the theme addressed here.

In later years, several other attacks have also occurred, such as – including, but not limited to[87] – the attack against the magazine *Charlie Hebdo* in Paris 7 January 2015, the bombings in Brussels on 22 March 2016, the 14th July 2016 attacks in Nice, the 19th December 2016 attacks in Berlin and the 3rd June 2017 attacks in London. All of these could potentially have been topical to this thesis, but they will in all essences not be dealt with here. This is because they are relatively speaking “new” attacks, and as seen with the three main attacks to be studied here, it often takes time for all aspects of the attack, particularly the governments’ response to the attack, to be fully analysed.

06.05.01 – Spain - Madrid 2004

As described by Bolz, Dudonis & Schulz (2012, p. 347-348), on the morning of 11 March 2004, a minimum of 10 IEDs placed on four different commuter trains in Madrid, detonated nearly simultaneous (within a period of 10 minutes), killing 191 people and injuring more than 1800. Three more UXO/IEDs[88] were located and disarmed, showing the IEDs consisting of at least 10 kg high-powered mining-dynamite each. The attack were later linked to the GICM, a group closely tied to al-Qaeda (Wright-Neville 2010, p. 144). This was not a suicide attack, and the bombers remained at large for several weeks before a police raid against their hideout, where several of the terrorists were killed when they detonated additional explosive devices. Still, despite not being a suicide attack as 7th July 2005 was, Hoffman (2006,

[87] The attacks that are listed here are merely a selection of attacks committed in the West in later years, and as such this listing should in no way be seen as an exhaustive summary.
[88] Unexploded IED

p. 251-252) notes: "*The attacks on mass transit during the morning rush hour in London have inevitably been compared with the similar incident involving the bombing of four commuter trains in Madrid, Spain, on March 11, 2004, that killed 191 people.*"

06.05.02 – India - Mumbai 2008

As described by Bergen (2011, p. 265) and Rabasa et.al. (2009, p. 3-8, 23-24), on the evening of 26th November 2008, ten terrorists from the group Laskhar-e-Taiba, that had arrived in Mumbai a few days earlier, split into several groups and began a four-pronged attack against various soft targets in Mumbai. Armed with high-power assault rifles, grenades and pistols they attacked targets such as hotels, train-stations, hospitals and cafés. They had also placed five IEDs around the city.[89] During the evening / night, several of the terrorist barricaded themselves at the Taj Mahal Palace Hotel, the Hotel Oberoi and the Nariman House[90]. At 11:00 on 28th November Hotel Oberoi was stormed and cleared by government forces. Same with Nariman House at 19:45. Taj Mahal Palace Hotel was cleared on 29th November at 08:50, marking the end of the attacks. In total, 166 people were killed, and over 600 injured, as a result of the attack.[91]

With regards to this attack, it is worth mentioning that the 13th November 2015 attacks in Paris are by Europol (2016, p. 22) considered to be the first time a completed attack in Europe have used tactics so similar to the Mumbai 2008 attacks.[92] Whether or not the Paris-attackers and their handlers have taken lessons from the Mumbai 2008 attacks are difficult to say. However, the tactics here are similar to well-known guerrilla / insurgent and special forces tactics of using small, mobile teams in multi-pronged hit-and-run attacks to create chaos and disruption "behind enemy lines".[93] Without speculating further, it is just as probable that the ISIS-attack in Paris (ibid.) were inspired by combat tactics learned and honed in Syria and Iraq, rather than acquired by studying LeT-tactics. A tactic that works well one place are likely to be "discovered" separately several times, without any obvious inspiration from one-another. A

[89] These IEDs were made using the military-grade high-explosive RDX, and ball bearings to create shrapnel.

[90] The Nariman House is a Jewish outreach centre consisting of, among other things, a hostel, an educational centre and a synagogue.

[91] Figure not including the 9 attackers that were killed, and the 1 that was injured and subsequently arrested.

[92] Europol here uses the definition "EU Member State" when referring to Europe. Norway, Swiss and other non-member states are thusly not included there, but none of those countries have been subject to such attacks either, so the statement seems apt.

[93] Basically, asymmetrical warfare.

kind of *convergent evolution* with regards to terror tactics rather than biology,[94] or as Hoffman (2006, p. 250) puts it: "*An almost Darwinian principle of natural selection (...)*". The force multiplication effect of such asymmetric attacks can, among other things, be seen as Frattini et.al. (2016) notes that police forces have to use resources to secure FRM-services and to protect them against attacks. This both serves to limit the number of resources available to engage the attackers and creates the illusion of a larger group of attackers then might actually be, i.e. playing on the "fog of war" (see chapter 01.02.01).

06.05.03 – France - Paris 2015

On Friday 13 November 2015, several groups of terrorists from ISIS, armed with automatic weapons and PBIEDs, launched a multi-pronged attack against several soft targets in and around Paris (BBC, 2015). At 21:20 one suicide bomber detonated his PBIED right outside the Stad de France football stadium. 10 minutes later a second PBIED detonated outside another entrance to the stadium. At the same time, another group began shooting at civilians in a restaurant area a few kilometres away. Several restaurants in close proximity to one another was attacked. A short while later a third group attacked the concert venue at the Bataclan Theatre, killing several and taking additional hostages. Bataclan was later stormed by police forces just after midnight. Several more of the attackers also had PBIEDs and one additional detonated his outside the stadium, one in the restaurant area and two more in the Bataclan Theatre. In total, 130 people were killed and several hundred injured, as a result of the attack (ibid.).[95] As previously noted, the attack bore strong similarities to the tactic seen in the 2008 attack in Mumbai (the use of multiple independent teams of attackers, soft targets, hostage scenarios and the use of explosives and suicide tactics), as also noted by Europol (2016, p. 22).

[94] In evolutionary biology, convergent evolution are the *independent evolution of similar traits along different lineages without them inhabiting the same eco-system*. Traits that are of a general advantage will appear again and again in unconnected systems, such as eye-sight among animals or fruit among plants.

[95] Figure not including the 7 attackers that were also killed.

07 – Communications

Communication is a word with several meanings. In the case of this thesis, it can mean one of two things: communications equipment or the act of communicating. Both are central and interconnected elements of any emergency response, and unsatisfactory communication between different parts of an emergency response will negatively impact the response and the responders' capabilities as a whole (Enger et.al., 2016, p. 322-323).

07.01 – Defining communications

As noted above, in C2 and emergency preparedness *communications* can be divided into two main parts; communications as the *technical means* of transmitting information from one part of the system to another, and communications as the *act and ability* of communicating information from one part of the system to another (ibid., p. 323-326).

In regards to the technical means, the definition is pretty straight forward; the use of any technical device in order to transmit information, that follows the specifications needed for that purpose with regards to technical interoperability,[96] encryption and so on. Due to their increased technical complexity, and the general complexities of encryption (such as up-to-date encryption-keys and synchronised devices) the potential for technical failure are higher, than with their unencrypted counterparts. As encrypted communication-devices by their very nature, are designed to be used in scenarios where continuity of communication is vital, extra care to safeguard against technical failures are often taken, but still, one must expect a certain level of minor technical challenges due to the systems' complexity. Redundancy systems and back-up capabilities are to be expected from a system resilience view.

When it comes to the act and ability of communicating, the definition is more comprehensive. Here, elements other than the purely technical, which have an impact on the commander's ability to communicate intent,[97] are central, such as a proper command structure with which to communicate. If the commander does not know *who* to contact in order to either get information or issue commands, there is an obvious problem with communications – even

[96] Technical interoperability refers to a systems ability to communicate with another system that has different specifications; such as the ability of two different communications systems to communicate with eachother (van der Veer & Wiles, 2008, p. 5-6)

[97] See chap. 03.02

if all the technical systems are fully functional – basically; the chain of command. Likewise, having a C2 system that is capable of enabling effective communications both inside its own system, and outside (directed at other relevant cooperating systems) are key for the commander's ability to perform. Hammervoll (2014, p. 43-44) emphasises that this cooperation and exchange of information is a key capability in regards to emergency logistics, particularly when it comes to the containment of an incident, which incidentally is one of the primary objectives during the initial response to a terror attack. He further emphasises the importance of this information management by stating, in referring to both Perry and Maxwell & Watkins, that "*The faster the information becomes actionable, the more effective the containment-effort will be*."[98] (ibid., p. 48). While that is said in referring to humanitarian logistics and the evolving of emergency logistics from that point of view, it is still seen as applicable here.

Enger et.al. (2016, p. 324-331) also talks about communication as in crisis communication directed at communicating with the public. Shpiro et.al. (2011, p. 6-7) also states the importance of this kind of communication. While such communication obviously is important in regards to e.g. conveying important information to the public,[99] countering the terrorists' narrative or soliciting information from the public[100] (ibid., p. 20-21), this will not be central in the definition of communication in regards to this thesis.

Because of these two ways of looking at communication, this chapter is divided into two parts, one looking at the technical communications capabilities, and the other one looking at the non-technical part, i.e. the chain of command.

07.02 – Technical communications capabilities

In this sub-chapter, the technical means of communication and the capability thereof will be discussed. When it comes to the strategic level's ability to function in a crisis situation then its technical communication capabilities are important both to enable the different parts of the strategic levels to communicate, but also in its ability to communicate its intent to the operational level, as well as receiving information from that level, as shown in the figure in chapter 03.02.

[98] Author's translation. Original text in Norwegian: "*Jo raskere informasjon kan brukes, desto mer effektiv blir skadebegrensningen (...).*"
[99] See for instance chap. 06.04.02 with the closing of public transport in London as a result of the 7th July 2005 attacks.
[100] See chap. 03.02 and 03.03 in regards to sensors in information collection.

07.02.01 – 11th September 2001

While there were reports of some technical difficulties, mainly with the so-called secure telephones[101] and other means of encrypted communication, it does not seem to have had a significant adverse effect to the abilities of the strategic levels' abilities that day. The few problems that arose can partly be ascribed to the inherent challenges with encrypted communications, as described in chapter 07.01, such as the difficulties Pentagon operators had in including FAA into their teleconference, the so-called "Air Threat Conference". NORAD, at around 10:00, repeatedly asked whether the FAA was connected to the conference, but they did not manage to connect until 10:17, partly due to technical difficulties (9/11 Commission Report, 2004, p. 37). Likewise, it was reported that the President, on Air Force One, had communications problems in connecting with the Vice-President at the White House bunker and the Secretary of Defence, and that the calls kept cutting off. He described these communication-problems as frustrating (ibid., p. 40). As will be discussed in chapter 07.03.01 and 07.03.02, these – somewhat minor – technical difficulties is not seen to have been decisive in affecting the strategic levels' capabilities, as the challenges with communication along the chains of command probably would have been just as prevalent had there been no technical difficulties at all.

07.02.02 – 7th July 2005

After the initial three, near-simultaneous, explosions occurred, the control centres of the emergency services and the London Underground's Network Control Centre (NCC) became flooded with calls and radio-traffic, initially overwhelming the radio operators (Coroner's Inquest, 2011, p. 28). In and of itself this is to be expected during such an event, and initial chaos caused by a sudden influx of communications can in such cases not be classified as a "failure". However, the system used to record and coordinate the flow of information received was at the time of the incident still reliant on hand-written logs. Regarding the situation at the NCC, the Coroner's Inquest notes (ibid.): "*This meant the operators were distracted from answering calls and, therefore, were not kept updated with relevant information. The information they did receive was not communicated to others in a timely and effective fashion.*"

[101] A euphemism for encrypted telephones.

While the police Gold Command[102] was already operational due to the G8-summit taking place (House of Commons report no. 1087, 2006, p. 7) (Coroner's Inquest, 2006, p. 33), it was still reliant on the operational level to receive, filter and forward information gathered from the City of London Police (COLP), the Metropolitan Police Service (MPS) and the British Transport Police (BTP). Much like at the NCC (and at other FRM control centres) the various police control centres became overwhelmed by the sheer amount of radio- and telephone communication (ibid., p. 32). That both the COLP and the BTP after the attack revised both their technical systems and their minimum staffing levels, can indicate that the technical communication systems in place at the time, was not capable of handling a high volume of incoming data. Likewise, much of the communications equipment used by these various control centres to communicate with their personnel, did not function in the tunnels where the initial bombings had occurred (ibid., p. 35).

It is important to note that these examples regarding technical factors mentioned here are all primarily at the operational level (and to some extent the tactical level), and not the strategic. They serve to show the interdependency of the different levels, as the strategic level are not collecting information on its own, but rather via the operational level, and the vulnerability this presents for the strategic level. This link between these two levels are, however, not a central topic of this thesis. And while the medical Gold Command had problems with their own communications equipment (ibid., p. 31-32), this does not seem to have been the case with the police Gold Command. Whether the preparations and systems already in place due to the G8-summit were a contributing factor to this, or whether this particular Gold command were simply sufficiently set up in regards to communications technology, are difficult to say, but the Coroner's Inquest (ibid., p. 33) notes that the G8-summit had a significant impact on the preparedness of the police.

07.02.03 – 22nd July 2011

During the initial phase of the attack, there were several problems regarding the technical communications equipment used by the police. An extremely high volume of traffic both on the regular phone lines as well as on the communication equipment caused a situation at the Oslo police department's operations centre in which information easily could be lost in the confusion and sheer amount of traffic. The systems for handling the information were also

[102] "Gold" referring to the strategic level, ref. chap. 01.02.04

not designed to effectively process such amounts of information (NOU 2012:14, 2012, p. 88-94). As noted by the 22nd July Commission, this gave the leadership of the operational level poor premises on which to lead on.

Likewise, the combination of new and old technology in different units' communications equipment, and the lack of effective system interoperability, meant that several units could not use their digital equipment, because many supporting units only had analogue equipment, and the expansion of the digital network had not yet reached the area surrounding Utøya. For many units, this lead to the reliance on mobile phones to ensure communication and coordination between different units (ibid., p. 305-307).[103]

Both of these situations described above does not apply directly to the strategic level, as the tactical and – mainly – the operational level bore the brunt of these problems. These technical challenges are worth keeping in mind, as they potentially affected the operational levels' ability to both obtain information from, and effectively lead, the tactical level, to a certain extent. This, in turn, it is fair to assume that affected the ability of the strategic level to both effectively transform their intents into directions for their forces and to fully form a correct assessment of the situation. However, while an inconvenience, these does not appear to have affected the strategic level to such an extent that it can be said to be detrimental in regards to the scope of this thesis, i.e. the strategic levels' initial actions. Likewise, as mentioned in chapter 07.02.02, this cross-level communication, while important, is not the main focus of this thesis.

In regards to a national alert system for the police, there was no reliable technical system for that available at the time. As described by the 22nd July Commission (ibid., p. 147-149) the system was based on sending an e-mail to predetermined e-mail addresses in operations centres and different commands in the police. As had been discovered following a major robbery in Stavanger in 2004[104] the police needed a reliable system to send out nationwide alerts. As noted by the 22nd July Commission, this was not followed up on, and on 22 July a satisfactory system was not implemented, leaving the e-mail as the only option. A test of the e-mail system on 9 June 2011 showed a system that basically did not work. The last district's acknowledgement of receiving the test-alert came after three months (ibid.)

[103] It is worth noting that the 22nd July Commission bases the assessment that the new digital communications system, "Nødnett" (EN: *Emergency network*), all in all performed according to specifications upon the assessment given to them by the directorate responsible for the network itself; the DNK (Direktoratet for nødkommunikasjon, EN: *Directorate for emergency communications*). The challenges with the system's technical interoperability in regards to older, analogue systems, are briefly mentioned by the commission. (NOU 2012:14, 2012, p. 305-307).

[104] The so-called Nokas-robbery in Stavanger 2004.

It was via this system that the first national alert, which contained a partial description of a vehicle of high interest regarding the bombing,[105] was distributed after the Oslo police contacted the polices' national contact point at Kripos.[106] Out of the 32 commands that received this alert, only four discovered the message during 22 July.[107] The message itself was sent 1 hour and 18 minutes after the VBIED explosion in Oslo (ibid., 149-154). While this also are not directly linked to the strategic level, it shows that the due to the lack of a capable system, the polices' strategic levels', whether that be the leadership of the individual district or the national command, did not have any capabilities to rapidly inform the different operational levels (or other strategic levels) of vital, "flash-information",[108] should the need arise.

07.03 – Chain of command

In this sub-chapter, the so-called "non-technical" capabilities of communication will be discussed. As mentioned in chapter 07.01, this part of communications is based on the ability to reach those that one are trying to reach, i.e. that there is a chain of command that is capable of relaying the communications between the different parts of the strategic level and from the strategic level to the operational level. Unlike the two other attacks, the 11th September attack will be debated in two separate chapters, instead of one. This is because the higher degree of complexity of that attack compared to the two others, means that both the "typical" strategic commands as well as the top-level political leadership became involved in the effort. As they, to a certain degree differs, this is seen as the most easy-to-follow way to present this.

07.03.01 – 11th September 2011: Military and civilian strategic commands

During the 11th September attacks primarily two events in regards to the chain of command are seen. These are the challenges with the communication between the civilian and the military strategical commands (FAA Headquarters and the NMCC)[109] and the challenges of communication between different parts of the strategic leadership of the government.

As the primary handlers of the civilian traffic in US airspace, the FAA were the obvious first point of contact in regards to the information about the hijackings. In the event of a

[105] This was later found to be the description of the car the terrorist used to relocate from Oslo to Utøya.
[106] The Desk at Kripos is the national contact point for domestic and international police contact and cooperation.
[107] Several other messages were sent later that day, but none during the initial phase of the attack (ibid., p. 152).
[108] Vital and extremely time-critical information.
[109] National Military Command Center. The command and control centre for the NCA, located at the Pentagon.

hijacking, a set of protocols was put in place to define the cooperation between the civilian authorities; the FAA Command Center, and the military authorities; NORAD. Among other things, the protocols governed the FAA's ability to request assistance from military assets via NORAD. As noted by the 9/11 Commission Report (2004, p. 17-18), the standard request for military assistance, typically fighter planes to observe and escort a hijacked aircraft, would need to pass through several levels of command before being authorized (or denied) at the top level of the government.[110]

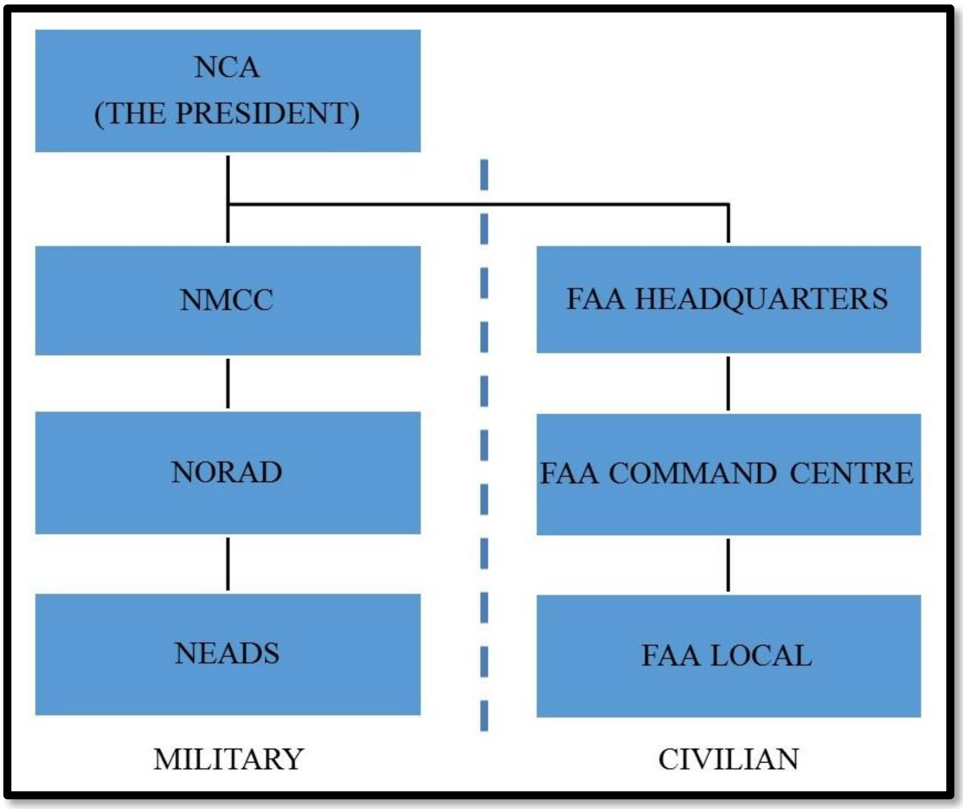
The protocol for such requests and coordination between the civilian and the military units was that the hijack coordinator at the FAA Headquarters would alert Pentagon's NMCC. They would in turn get clearance from the Office of the Secretary of Defence (a part of the NCA[111]) and those orders would follow the chain of command to NORAD. Continuous communication between FAA Headquarters and the NMCC, and the FAA Command Center and NORAD, would allow those involved to track the plane, monitor the situation surrounding the plane and the military's response. In addition, since the FAA were the responsible agency in regards to the control of the civil airspace over the US, they would have the best basis for tracking such a plane, as NORAD, naturally, had their main focus directed outwards against international and foreign airspace, as they saw that as the primary area for threats against the US (ibid., p. 16-17, 352, 427-428). The radars FAA relied on was directed toward domestic airspace and calibrated towards civilian aviation, as were the personnel monitoring the radars.

Because a hijacked plane triggers several responses from many parts of the government besides scrambling fighter planes, such chain-of-command reporting rules also serves a purpose allowing involved departments to move this information along their own internal chains of command, thus ensuring that all the essential parts of strategic command gets the notice. A simplified setup of these chains of command, both civilian and military, are shown below:[112]

[110] This need for political clearance for deployment of military assets in domestic situations are normal in most Western countries. See also chap. 04.01.

[111] National Command Authority. The designation for the top-level of command for the US military: the President of the United States and the Secretary of Defence (and their deputies; Vice-President and Deputy Secretary of Defence).

[112] It is important to note that the schematic setup shown here are very simplified and a full, detailed view of the chain of command would be vastly more complex. It is shown like this to give a simple schematic overview of the chain of command.



It can be argued that the linchpin of this protocol is the strategic levels' (FAA Headquarters and the NMCC) ability to actually get the information they need to act upon. Neither of them are primary sensors, as they are the strategic levels of their chains of command. What is seen happening on 11 September 2001 is the failure of those chains of command to actually deliver the timely information to the strategic level, and the strategic levels' failure in realizing this and taking steps to correct it. Because of these challenges within the chains of command, they did not have a proper situational understanding, which will be further addressed in chapter 08.02.01.

This need for the FAA in providing the military agencies with flight data is exemplified by the cases of Delta 1989. For a long time NEADS tracked a civilian plane designated "Delta 1989" because they suspected it to be hijacked (which it later turned out it was not), but at the same time they failed to identify United 93 on its path towards Washington DC (ibid., p. 27-28). They also had problems locating American 11, because it had turned off its transponder system, and they had to identify its radar return to be able to track it (ibid.).[113] Granted, the FAA also had to identify the planes radar return due to the lack of a transponder, but because they

[113] The primary radar signal, i.e. the "blip" on the radar screen.

had the primary responsibility of watching the national airspace, they were in a position to easier identify it, as they was already following it when the transponder signal disappeared.

When American 11 was identified as the first hijacked plane, FAA Boston alerted the FAA chain of command to the situation. Near simultaneously, the FAA Command Center likewise contacted FAA Boston because they had received a hijack-warning from American Airlines Operations Center, due to the calls from flight attendants Betty Ong and Madeline Sweeny (se chapter. 06.01) (ibid., p. 5-6). However, in breaking with protocol, FAA Boston contacted NEADS directly with the request for military assistance (ibid., p. 18-21). The reason for this is unknown. As it turns out, the FAA Command Center was already aware of the hijack, but there is no record as per the 9/11 Commission Report that they sent the request for military assistance up the chain of command, as the protocols in place at the time dictated. Because FAA Boston is below FAA Headquarters in the civilian chain of command, and NEADS being below NORAD in the military chain of command, this resulted in a decision to activate military assets taken below the designated strategic level. NEADS scrambled fighter planes and then informed NORAD of the situation and retroactively asked for permission to do so. As commander of NORAD's Continental Region (of which NEADS was part) Major General Larry Arnold was quoted saying to NEADS Battle Commander, Colonel Robert Marr (who had already ordered fighter planes to battle stations)[114], when giving Marr the go-ahead to scramble the fighters; "*Go ahead and scramble them, and we'll get authorities* [sic.] *later.*" (ibid., p. 20). Gen. Arnold then contacted NORAD to inform them.

When FAA New York identified United 175 as a hijack, they were already aware of the hijacking of American 11 – although not that it had already crashed into the WTC (ibid., p. 21). In addition to informing their own chain of command about the hijacking of United 175, FAA New York also contacted NEADS and alerted them to the second hijacking. In regards to American 77 and United 93 (ibid., p. 24-31), the FAA reported the incidents up their own chain of command, but in both these situations also, NORAD was not the primary contact, but rather NEADS. It is however debatable whether NEADS was ever alerted to the hijacking of United 93, as there was widespread confusion in regards the identities of several of the planes. What is clear, however, is that NORAD was never notified about this until after the plane had crashed into the WTC. Because the transponders on the hijacked planes was turned off, FAA controllers was unable to properly identify all the planes and the confusion resulted in misidentification of

[114] A heightened state of readiness, in which the forces at "battle stations" is ready to be scrambled at a moments notice.

the planes, and miscommunications between FAA and NEADS. The 9/11 Commission Report notes that training and protocols were not followed that day in regards to the defence of US airspace. The further (unintentional) incorrect information in regards to the warning and response scheme from NORAD before the 9/11 Commission itself, further exemplifies the prevalence of the confusion on that day (ibid., p. 31-34).

It seems like the system that was in place to ensure smooth communications between the civilian sector (mainly the FAA) and the military (NORAD) was specifically designed to deal with so-called "regular" hijackings (in which the hijackers' intent were to land the plane somewhere and use it in further negotiations) and therefore communication between them would be able to follow their normal chain of command. While such a situation is time-critical in and of itself, the window of opportunity to act is in those cases are far greater than when the plane is being used as a weapon in a suicide attack.[115] This, in conjunction with the fact that their routines did not take into account hijacked planes deliberately trying to disappear from radar and / or being used as a suicide weapon, meant that the system was not prepared to deal with such a fluid and extremely time-critical situation as the one that occurred on 11 September. The 9/11 Commission Report (ibid.) states "*On the morning of 9/11, the existing protocol was unsuited in every respect for what was about to happen.*" While this statement refers to the entire protocol for cooperation between civilian and military assets and their respective responses, it also points to the difficulties that were seen in the communication between them. This lack of situational understanding (see chapter 08.02.01) can be argued to have attributed to the fact that the top parts of the strategic levels; the NMCC and the FAA Headquarters did not press the need for information down their respective chains of command, simply because they did not understand the situation, partly because they – in a self-reinforcing loop – did not get enough information to understand that their chains of command had failed in relaying information.

Before 10:00 there were several teleconferences set up by parts of the FAA and the DOD[116] and the White House. The 9/11 Commission Report notes that "*Because none of these teleconferences – at least before 10:00 – included the right officials from both the FAA and Defense Department, none succeeded in meaningfully coordinating the military and FAA response to the hijackings.*" (ibid., p 36). This lack of the correct personnel available at these

[115] Thus demonstrating the need for a set of protocols for the RENEGADE scenario.

[116] The Department of Defense. The US Department in charge of the military. The head of this department; the Secretary of Defence, is a part of the NCA.

information-exchange and decision-making scenes is prevalent throughout the spectre of military and civilian strategic levels, and as quoted above, this may have had a significant effect on both the capability to mount an effective response and a the situational awareness at the top-level strategic command; the NCA. This last part will be further discussed in chapter 08.02.01.

In regards to the teleconferences, they seem to have become partial communication dead-ends without anyone realizing it at the time. In situations like this, there is naturally a high level of activity on each of the participant's sides, and coordinating that activity and at the same time attempting to keep track of who is on the conference at any given time cannot automatically be expected of any one participant. In addition, as both military and civilian authorities was participating, it is fair to assume that detecting gaps in the chain of command of a completely different department (military vs. civilian) would be more difficult, given the differences between military and civilian organizations. A lack of leadership regarding the coordination is self, is assumed to have played a substantial part here.

Furthermore, in several of the teleconferences many supposed participants simply was not present. The FAA's teleconference, which according to the protocol should be the primary information exchange between the civilian and military sector, only featured the NMCC sporadically before the Pentagon was hit. Both participants here acknowledges that this teleconference played no role in coordinating the response, which is in direct contradiction to the governing protocols at the time. Likewise, the White House's teleconference also included the FAA and not the NMCC, but the DOD. Furthermore, none of the information from the initial part of this teleconference was relayed to the NMCC. These parallel, but unconnected, lines of communication caused what the 9/11 Commission quotes one of the involved saying: "*[It] was almost like there were parallel decisionmaking processes going on; one was a voice conference orchestrated by the NMCC… and then there was the [White House video teleconference]… [I]n my mind they were competing venues for command and control and decisionmaking.* " (ibid.) It is also worth noting that the White House teleconference was not connected to the part of the NMCC that was in charge of crisis-management and coordinating the response with NORAD (ibid., p. 463), effectively hindering the link between the two central parts of the strategic levels in the military's response, and slowing down the relaying of vital information to the NCA in a very fluid and rapidly changing part of the attack.

In the case of United 93 the FAA Headquarters was fully aware that it was hijacked, and that the FAA Command Center was pressing for military support in the form of fighter planes. This was even discussed among FAA Headquarters' most senior leadership, but this information was at no point in time relayed to the NMCC. The feedback from FAA Headquarters down to FAA Command Center and finally down to FAA Cleveland was that they were aware of it and was discussing requesting military support. As a result the direct communication between lower levels of the FAA and NEADS, that was seen in regards to the other planes, did not happen here as soon as it had happened in the other hijack-situations (ibid., p. 28-31). As the 9/11 Commission Report notes: "*Cleveland even told the Command Center it was prepared to contact a nearby military base to make the request. The Command Center told Cleveland that FAA personnel well above them in the chain of command had to make the decision to seek military assistance and were working on the issue*" (ibid., p. 28-29). Thus, effectively hindering any flow of information between the lower levels of the civilian and military chains of command. As a result, NEADS was not made aware of United 93 before five minutes after it had crashed. United 93 had then been hijacked and airborne, with a course towards Washington DC, for approximately 37 minutes without the military, and crucially the NCA, and by extension the government's entire top strategic leadership, being aware of it and the extreme threat it posed.

As the 9/11 Commission Report describes it: "*Jarrah's objective was to crash his airliner into symbols of the American Republic, the Capitol or the White House. He was defeated by the alerted, unarmed passengers of United 93.*"[117] (ibid., p. 14). Whether or not the later shoot-down order would have stopped United 93 from reaching its intended destination, had it not been forced to the ground by the passengers, is pure speculation. The order was given at approximately 10:15, and fighter planes was at that time on CAP over Washington DC, but it is worth noting in this respect that the due to massive confusion in NEADS, the order might not have reached the pilots in time to intercept the plane (ibid., p. 43-44). There is no information about the NCA being aware of this delay in operationalising the order, rather to the contrary, they were under the impression that the order had not just been operationalised but also acted upon (ibid., p. 43). The 9/11 Commission Report doubts that the military would have been able to intercept United 93, and prevent it from reaching its destination, had the passengers not acted, unless a lower level military commander had taken that decision unilaterally (ibid., p. 44-45).

It is further worth noting that at around 10:38 a different set of fighter planes had been scrambled to CAP over Washington DC, from outside of the entire military chain of command,

[117] "Jarrah" being Ziad Jarrah, the pilot-hijacker aboard United 93.

via the Secret Service, and these fighter planes were so-called “weapons free” in regards to engaging hijacked planes.[118] Neither NORAD or the NMCC was aware that there were two sets of ROE’s in play over Washington DC at the same time, as this information, in addition to the fact that these planes had been scrambled had not reached the NMCC (ibid., p. 44).

While the strategic level is not solely responsible for that all information follows the proper chain of command, it is that levels responsibility to ensure that the chain of command is functioning, and to take immediate steps to attempt to correct it if it is seen faltering during a crisis. Whether or not they were aware of these shortcomings during the attack or not, is not known, but at around 09:00 the NMCC was aware of both the fact that United 11 had crashed into the WTC and that it had been hijacked before the crash. Still it did not question the lack of requests for assistance when it was in contact with the FAA (ibid., p. 35). As more reports of the other planes started to come in, it the NMCC still did not question the lack of communication coming from the FAA. While there is no basis to claim that the NMCC should have understood the scope of what was happening, it can be argued that the NMCC should have been able to identify that there was a potential problem with the chains of command in regards to the flow of information. As a result, the 9/11 Commission Report notes that NEADS had a total of nine minutes to respond to the hijacking of the first plane (American 11) before it crashed into the WTC, and no advance warning of the other three planes (ibid., p. 31). And as noted before, only an NCA-level authority had the power to order the military to shoot down any of the planes, so NEADS had no realistic course of action to take against the one flight they were aware of, and none, had they been aware of the other planes. This is exemplified by the following excerpt from the 9/11 Commission Reports summary of the military’s response in regarding to United 93, (which at the following time already had crashed in Shanksville, Pennsylvania):

> “*At the same time, the NEADS mission crew commander was dealing with the arrival of the Langley fighters over Washington D.C., sorting out what their orders were with respect to potential targets. Shortly after 10:10, and having no knowledge either that United 93 had been heading toward Washington or that it had crashed, he explicitly instructed the Langley fighters: ‘negative – negative clearance to shoot’ aircraft over the nation’s capital*” (ibid.)

[118] “*Weapons free*” means that the authority to decide when and if to engage are given to the pilot, and the ROE permits engaging any target *not* identified as friendly. This being the most permissive of these ROE’s (as opposed to “*weapons tight*” and “*weapons hold*” which are much more restrictive).

The fact that the main bulk of communication between the military and civilian sector, that for all intents and purposes guided the initial (military) response of the US government, went outside of the strategic levels of command and instead was a direct communication between the lower levels (such as FAA Command Centre and NEADS) left the strategic level out of the loop, and unable to follow a very fluid and rapidly changing situation. It can seem like the system in place at the time was not capable of effectively facilitating communication and flow of information, leading to what ‘t Hart et.al. (quoted in Engen et.al., 2016, p. 304) describes as an *informal decentralisation* of the chain of command. This, in turn, led to a situational understanding that in many parts differed greatly from the actual situation, as seen in the prevalent confusion at NORAD as to the events that day (the 9/11 Commission Report, 2004, p. 31-34). One other problem that arose from this was that because of the fact that much of the information did not reach NORAD, and less reached the NMCC, even less reached the top level of the strategic decision-making, namely the NCA. This, combined with the difficulties of internal communication between different parts of the NCA led to a series of compounded errors that directly affected the NCA’s ability to both gain an adequate situational understanding and take control over the response and communicate its intent down through the chain of command, as will be addressed below.

07.03.02 – 11th September 2001: Top-level strategic command

Due to several circumstances at the time of the attack, the top level of the US strategic decision makers were all on different places during the attack, and found themselves to be in sub-optimal situations in regards to effective and coherent crisis management. For the first part, the President was out of the capitol on a trip to Florida. A short time after the attack had been identified as just that, and not simply a terrible accident, the Secret Service[119] moved the President on-board Air Force One (ibid., p. 38-40). While the Presidents original plan was to return to Washington D.C. and lead the nation’s response from there, the Secret Service convinced him that the security situation in the capitol was to uncertain, and he stayed aboard Air Force One, which flew without a final destination, as that was deemed the safest course of action at the time. At the same time, because of the attack against the Pentagon, it became an additional challenge for the Secretary of Defence to lead the response from the NMCC. So the nations top-level strategic command was that day split into three; the President airborne aboard

[119] The agency in charge of safeguarding the President and other officials in the US.

Air Force One, the Vice-President and other parts of the national security staff in the bunker under the White House and the Secretary of Defence in a partially crippled Pentagon.

The central part of the communication between the different parts of the NCA regarded the ROE to fighter planes on CAP in case they came across planes considered to be RENEGADE. Due to the technical difficulties described in chapter 07.03.01, there was not a constant open line of communication between Air Force One (the President) and the White House (the Vice-President). In a call just before 10:00 that morning, between the President and the Vice-President, the President authorized the use of force for fighter planes on CAP. When a short time – a few minutes – later the Vice-President was alerted to the plane approaching Washington D.C. (this being United 93) he rapidly authorized the use of force against the plane. When asked again a short time later he again gave the authorization. Due to the lack of an open line of communication between the President and the Vice-President, others in the room requested that the President be contacted again to confirm that the shoot-down order was correct (ibid., p. 40-42). The other parts of the NCA and the staff at the White House were apparently not fully aware of the earlier conversation between the President and the Vice-President, where such an authorization had been given.

As explained in chapter 06.04.01, the key action poised to be able to regain the initiative of the situation came when this order to shoot down RENEGADEs was given. As also explained, at the time, this was an order that only the highest levels of the government, namely the NCA, could give, as it would result in the use of military force against civilian targets in domestic territory. At the time, it was understood that only the President had the authority to give the military such an order. The Secretary of Defence had the power to authorize the use of military forces to observe and escort hijacked planes, but not to take action against them. Seeing as such an order would constitute using the military against civilians over US airspace in peace-time, this was not an order the military took lightly, as can be seen in their reluctance to immediately operationalise the order (ibid., p. 43). The order was received at NEADS from the Vice-President via NORAD’s Continental Region Command. As the 9/11 Commission Report further notes, the normal chain of command for use of force goes from the President, via the Secretary of Defence and to the relevant combat commander. Whether or not the reluctance the military had in operationalising that order was influenced by the fact that the order came outside of the normal (expected) chain of command is not known, but it is clear that the personnel charged with relaying this order to the planes was aware of that the order had come from the Vice-President (ibid., p. 42-44). Possibly adding to the confusion was the fact that the Secretary of Defence, which normally would transmit that order from the President to the NMCC (ibid., p. 43), was not at the NMCC at the time of the order. He was outside of the Pentagon building and later at his office inside, participating in the teleconference with the White House, before relocating to the NMCC at around 10:30, roughly 15-20 minutes after the order was first given. As the NMCC was not a part of the White House teleconference, and their primary link to the NCA (the Secretary of Defence) was not present at the time, the NMCC – during that time – did not have a direct line of communication to the NCA. It is in this case worth noting, once again, that the mission of the NMCC is to coordinate communication and orders between the NCA and the military unit(s) in question.

It is in this instance also worth noting that while the separation of the members of the NCA posed challenges in regards to the quick and efficient exchange of information and ability to debate possible courses of action, the NCA system is by design not supposed to have problems because of this. Designed during the Cold War, with a cataclysmic thermonuclear attack from the Soviet Union in mind, the system is largely built around the concept of "continuity of government" (more recently known as; "continuity of operations") (Petersen, 2004, p. 1-4) (Petersen & Seifert, 2005, p. 3-4) in which the government will be able to mount a response to an attack even if it is partly destroyed. While their chains of communication were weakened because of the attack against the Pentagon, there is no evidence to suggest that that itself was a reason for choosing to attack the Pentagon, and likewise this should not have a detrimental effect.[120] All targets that day were highly symbolic in regards to America's power on the world stage; the WTC as a symbol of their economic power, the Pentagon as a symbol of their military power, and the attempt against either the Capitol building or the White House as a symbol of their political power.

07.03.03 – 7th July 2005

According to the House of Commons report no. 1087 (2006, p. 7) the police's Gold Command, already being operational due to the G8-summit, took command over the response relatively quickly. The Coroner's Inquest (2011, p. 35) somewhat contradicts this, in saying: "*To manage such incidents members of each of the emergency services are assigned 'Gold', 'Silver' and 'Bronze' (...) On 7/7 such command structures were effectively not in place until*

[120] On the other hand it can be suggested that as the system was designed to work in case of a large-scale (conventional or nuclear) attack from another country, it simply was not prepared to respond to a smaller, highly fluid scenario as was the case on 11th September 2001.

close to, or after, the 'golden hour' (the initial response stage) had passed." It is not specified here what parts that was lacking, and at what time the golden hour (according to the Coroner) ended.

The London Assembly (2006, p. 42) notes that the Gold Coordinating Group (GCG) had their first meeting at 10:30. The purpose of this group is to coordinate the activities of all the relevant strategic commands and other involved authorities. Normally the GCG would meet at the MPS' headquarters in New Scotland Yard, where it had the facilities it needed. However, this meeting was relocated to Hendon, a London suburb. The reason for this is somewhat unclear, but it resulted in a severance between the different strategic commanders and their own operational centres, as traveling between those and the GCG became more difficult due to the distance. This was compounded by the fact that subway's services was suspended and there was heavy traffic on the roads as a result.

As the senior strategic coordinating body, the GCG are dependent on the other various strategic commands. If it are to have any relevant effect, all involved strategic commands and other relevant authorities must be present or otherwise represented to ensure the sharing of information and to channel decisions taken by the GCG back down in their own chains of command. As seen with the later implementation of the so-called ACCOLC-system,[121] this did not function properly during the initial phase of the attack. At the GCG's first meeting, the activation of ACCOLC was discussed, and: "*It was decided that ACCOLC should not be activated, because of the risk of public panic and because it was not clear that the right personnel would be carrying ACCOLC-enabled telephones. If they were not carrying this equipment, ACCOLC could have made matters worse.*" (ibid., p. 44) Because the potential effects of activating such a system, and its potential impact on the various police and FRM-services, the authority to activate ACCOLC lies with the GCG (ibid., p. 44-46). Despite of this, COLP went outside the normal chain of command and ordered the activation of ACCOLC on their own at 12:00. This was not done against the quite specific decision of the GCG to the contrary, because the senior leadership of the COLP was not aware of the GCG's decision. This means that this decision, taken at the GCG-meeting at 10:30 had not reached the strategic command of one of the primary responding forces, the COLP by 12:00. It is likewise fair to

[121] Access overload control. A system that gives pre-determined numbers prioritised access to GSM-networks, thus preserving the emergency services' ability to communicate via GSM during situations of extremely high network traffic (overload scenarios), such as was the case on 7 July 2005.

assume that the decision to activate the system also did not reach the GCG for quite some time, as the system was active for nearly 5 hours before being shut down (ibid.).

Furthermore, according to the Coroner's Inquest there was no representative from the London Underground at this first GCG-meeting. They wright: "*This is surprising given that three of the atrocities had occurred on the network for which it was responsible.*" (2011, p. 29). This was not because they were not welcome there, they were simply not aware of the meeting. Given these lacks in the GCG's ability to fully insert itself into the chain of command, and their somewhat late convening (nearly 2 hours after the initial attack), it is doubtful that the GCG had the ability to affect the initial strategic response to the attacks. This is, however, not to diminish the capability it later had, as the response moved into the *late-response* / *early-recovery* phase (see chapter 01.02.02).

As a primary "owner" of the affected area, the London Underground's NCC played a central part, both as a sensor for the various police and FRM-forces, but also as a necessary link to enact a shutdown of the subway network. London Underground is a subsidiary of Transport for London, of which London Buses Services Limited is also a part. Due to its day-to-day responsibilities, it is possible that the NCC may have had more experience working the fire and ambulatory services, as accidents, malfunctions and other incidents that are most likely to occur, would need primarily need their assistance and not the polices', and also on a more operational rather than strategic level. As noted by the Coroner's Inquest (ibid., p. 28-29 & 40) the NCC were very reliant on the BTP to liaise with the other services. For the various police and FRM-forces, it quickly became apparent that the events was in fact most likely caused by bombs. This information travelled up the chains of command in both the COLP, the BTP as well as the fire brigade. As the NCC expected such information, if there was any, to come to them via the BTP, active steps to collect such information was not immediately taken. As the Coroner notes, the information that the COLP and the BTP had would have enabled the London Underground, via the NCC, to identify the causes of the incidents. When this information reached Transport for London (as the top-level of the transport sector) is uncertain, but it is clear that the control centre for the London bus-network was not made aware that the situations at the subway was actually a terror attack, until after 09:53, when the fourth bomber detonated his PBIED aboard Bus no. 30. Likewise, the Coroner points to problems with the NCCs ability to alert the emergency services of actions taken by the NCC in regards to evacuation orders[122] and the Transport for London and its subsidiaries (subway and busses) was not "*in the loop*" regarding being alerted if one of the emergency services were to declare a major incident (ibid., p. 41).

Another part of the strategic command relevant at the time is the government's Cabinet Office Briefing Rooms (COBR).[123] According to the House of Commons report no. 1087 (2006, p. 7) COBR was activated at appx. 09:30, already being operational due to the G8-summit. The report also notes that, in regards to the incidents, they assessed that: "*Seems increasingly likely that this is a terrorist incident*" (ibid.). It is unclear at what time, and on the basis of what information that lead them to this. While it is noted by reporters, such as Johnson (2015) that counter-terrorism officials from the MPS and the MI5 came and briefed them, the time for this is not given. The activities of COBR is also not mentioned in the Coroner's Inquest (2011), only very briefly in the London Assembly report (2006, p. 89) and also briefly in the ISC-report in to the attacks (2006, p. 2), but not in connection to the effort on 7 July. As mentioned in chapter 06.04.02, the Home Secretary announced at 10:55, after a meeting with COBR, that public transport had been suspended following the attacks. The lack of information in the various reports regarding COBR's potential involvement in this decision, and their role during the golden hour makes it difficult to assess their part in the initial response. The lack of them being mentioned to any meaningful extent, and the difficulties GCG (the strategic level below COBR) had in reaching their own chain of command, can indicate that there was not a fully functioning line of contact between COBR and the GCG during the initial phase of the attack, effectively putting them outside the chain of command.

07.03.04 – 22nd July 2011

During the initial phase of the attack on 22 July 2011 there are primarily two levels of strategic command that are relevant for the scope of this thesis; the strategic level in the Oslo police district and the national strategic level of the POD (the National Police Directorate).[124] Each districts' strategic level are responsible for their own geographically area, while POD are

[122] Which, as the Coroner's Inquest (2011, p. 41) notes, leads to 250.000 passengers being moved from the subway to the streets of London, with all the challenges that comes with such a sudden influx of people, including increasing the potential target-yield in the case of an ongoing attack.

[123] Sometimes also known as COBRA, the A referring to briefing room A.

[124] Nordre Buskerud police district, which was the site of the secondary attack at Utøya, will not be debated here as the "golden hour" ends with the re-deployment of the Delta unit at 17:33 (ref. chap. 06.04.03). Since the first report of that attack at Utøya came at 17:24 (NOU 2012:14, 2012, p. 27), Nordre Buskerud police district did not have a realistic time-frame in which to activate their strategic leadership before the golden hour – as defined in this thesis – ended.

their superiors and are responsible for coordination on the national level, and further up towards the political leadership. The levels above there again, the Government Crisis Council (NO: *Regjeringens Kriseråd, RKR*) and the Crisis Support Unit (NO: *Krisestøtteenheten, KSE*) (NOU 2012:14, 2012, p. 210-211) were for all intents and purposes neutralised during the start of the attack, as they were housed in the Government quarters (Høyblokken) which was the main target of the VBIED. The later actions of the Crisis Council will not be further debated here, as they were not operational until they convened for their first meeting at 18:30 (ibid., p. 220).

When the attack commences, and the VBIED detonated, one leader of district's staff was still at work, and was able to start work according to her area of responsibility as P2[125] (intelligence and investigation) almost right away. The leader of the P3 function (plans and operations) was on holiday and his deputy was a tactical commander (NO: *innsatsleder*), already working at the bombsite. This function was therefore filled by an officer with long experience in tactical command, but without experience from the staff function. The presence of plans for the P3 function was unbeknown to him (ibid., p. 95-96). However, he was aware of the risks of a secondary attack, and initiated measures to prevent an attack against the building housing the staff and the operations centre (ibid.). P3 arrived at the staff room at approximately 15:40, about the same time as the Deputy Police Chief, who in the absence of the police chief, became acting leader of the strategic level.

At about 16:45 the chief of staff also arrived, and 10 minutes later the first meeting at the strategic level was held. Neither the Deputy Police Chief or his chief of staff received information from the operations centre that they had information regarding a potential vehicle linked to the bombing (as described in chapter 07.02.03) when they arrived, and there is no logs of any communication of a situation update between the strategic and the operational level in this meeting (ibid., p. 96-97). Since the strategic level in Oslo reports to the strategic level in POD, this information also did not reach the national strategic leadership of the police. As shown in figure 8.3 in Meld. St. 21 (2013, p. 76) the strategic leadership of a given police district can be seen to have a dual role; as both the top-level in its own, local chain of command, and at the same time the bottom-level part of the national strategic chain of command. As such, the leadership of a police district serves as an important sensor for the national strategic leadership as well as the primary communications link between national and local levels. Due

[125] The Norwegian police are have organized their staff functions in the same way as the military (which follows the NATO organization) of the functions 1, 2, 3, 4, 5, 6 and 7. They are denoted as P1, P2, P3 etc., the "P" as in "police" (Politidirektoratet, 2011, p. 124-128).

to of this breakdown of the flow of information up the chain of command, the 22nd July Commission notes:

> "*The commission can as a result of this establish that critical information did not reach the staff members as they arrived, or the staff when it became operational. Without this information, and information regarding the operation at hand, the staff would at this time be severely limited in their ability to exercise knowledge-based command and control over the ongoing police operation.*"[126] (ibid., p. 96).

As an example of this, it is uncertain at what time POD first was alerted to the secondary attack at Utøya. The staff in Oslo got the first messages regarding this at 17:29 when one of the children to a staff member called *from* Utøya and reported the situation. This was relayed directly to the liaison from Delta that was in the staff, and this was the direct reason for the first re-deployment of Delta resources towards Utøya (ibid, p. 114-116).

At POD, the staff was formally operational at 17:55, but informal and rudimentary staff functions began working almost immediately after the explosion in Oslo (ibid., p. 156-157). The 22nd July Commission describes that while those there did what they could with what they had available, the capabilities of the staff in the initial phase of the attack was severely limited, at best. It is being further described that contact lists for both its own personnel and for external partners was not up-to-date, instructions and standing orders had not been updated for several years, many staffers was not trained in their functions and many in the staff was not able to log into neither the open or classified networks. This greatly reduced their capability to communicate and insert themselves into the chain of command. There was also some confusion as to who was actually in charge. The Assistant National Commissioner arrived at the staff at appx. 16:00, taking command. Sometime after this, the National Police Commissioner (the highest-ranking officer within the police) arrived and took over the command. When this happened are uncertain, as it is not registered. This confusion as to who was in charge can among other things be seen in the fact that at the first meeting with the RKR at 18:30, the Assistant National Commissioner who attended, was by several members thought to be the acting commissioner, even though the National Police Commissioner had taken command a

[126] Author's translation. The original text in Norwegian reads: "*Kommisjonen kan etter dette slå fast at kritisk styringsinformasjon ikke nådde fram til staben verken etter hvert som stabsmedlemmene ankom, eller etter at stab var satt. Uten disse opplysningene, og uten kjennskap til operasjonsleders tiltak så langt, kan staben på dette tidspunkt vanskelig ha vært i stand til å utøve kunnskapsbasert ledelse og kontroll av politiets operasjon.*" (NOU 2012:14, 2012, p. 96).

while ago, and had sent the Assistant National Commissioner to this meeting in his stead, as he was busy with his own command. The Minister of Justice also thought this was the case for much of 22 July (ibid., p. 154). This demonstrates confusion among much of the different parts of the strategic leadership as to the chain of command that day.

In evaluating their own performance, POD writes: "*All things considered, the staff at POD performed to a satisfactory level.*"[127] (ibid., p. 157) This refers to the work of the staff during the entire attack and in the days following. And while the staff at POD became much more efficient once it became fully staffed and operationalised (happening after the end of the golden hour) its capabilities in regards to communication, both technical and non-technical, severely limited their ability to function during this initial phase. The activation, or lack thereof, of the so-called terror plans will be debated in chapter 08.02.03, as this primarily concerns the situational understanding. Though it is considered likely that the difficulties the staff had during the initial phase probably affected their situational understanding and vice versa.

In regards to one of the most time-critical functions of POD during the initial phase of a terror attack is to process and relay requests from the leadership of affected districts concerning the need for resources that needs requires clearance to obtain. In cases like this, this is typically assistance from military forces. Just like in most other Western countries there are safeguards put in place to prevent the military from being deployed against citizens in domestic territory, and any such assistance will normally be under the command of either the police or the political leadership.[128] The need for helicopters, in a logistical capacity, on 22 July have, in hindsight, been very apparent, and the 22nd July Commission have dedicated an entire chapter of their report to this topic (ibid., p. 289-304).

Due to vacations for personnel and technical factors with the equipment itself, the police's one helicopter was not in an operational state during the golden hour on 22 July. It did however become airborne later that night (at 21:06). Regardless, the helicopter did not possess the capability to transport personnel, such as Delta, in any significant number. For that, either primarily the military's Bell helicopters or alternatively the SAR[129] Sea King helicopters would have to be used. In order to use the Bell helicopters a clearance from the political level was needed. This is obtained by the local Police Chief sending the request to POD, which in turn

[127] Author's translation. The original text in Norwegian reads: "*Alt i alt ser de tut til at staben i POD i hovedsak løste sine oppgaver på en tilfredsstillende måte.*" (NOU 2012:14, 2012, p. 157).
[128] See chap. 04.01 regarding the debate around this delegation of power.
[129] Search and rescue.

would send the request further up the chain of command to the leadership of the Justice department and the operational command in the military; FOH. (ibid., p. 296).

Roughly an hour after the attack had started, the 720 Squadron, for which the Bell helicopters are a part, on their own initiative started preparing their helicopters, so they could be ready in case their assistance was requested. Not long after, at 16:55, the permanent liaison from the military arrived at the staff in POD. He had already been orally instructed by POD to request clearance for helicopter support from the Minister of Justice. He relayed the request to FOH and, possibly due to the fact that the Bell helicopters were not ready yet, this request was further relayed to HRS (the rescue coordination centre), which had operational command over the two SAR Sea King helicopters designated Saver 40 and Saver 60.[130] This initial request was later denied by the HRS, because they were not to be used in counter-terrorism operations. This denial was appealed to the Ministry of Justice, but the appeal was overruled.

At roughly the same time as the military's liaison arrived at POD, HRS tried to establish contact with somebody from the Ministry of Justice. At this point, Saver 60 was airborne over Oslo.[131] The reasons why they were not able to reach anybody from the Ministry of Justice are not clear, but as there had not been reported noticeable technical difficulties with relevant communications equipment, it is reasonable to believe that the problem was related to availability of contact-points, i.e. problems with the chain of command.

It is further worth noting that relevant military units, possessing capabilities that could be requested by the police,[132] were rather rapidly informed of the ongoing situation via the military's own chain of command (ibid., p. 216-217). Moreover, while the system the military used to alert and mobilise personnel and key capabilities, was not the most efficient one, the 22nd July Commission still notes that:

> "*All in all, the military seems to have handled the initial phase of the crisis in a good way. Despite this being during the holiday period, the process of alerting and mobilising personnel was initiated quickly. The military's*

[130] Saver 40 was transporting the military's EOD unit to Oslo, while Saver 60 was running SAR-missions in Oslo.
[131] From 17:10 until 18:27 Saver 60 was idling on the ground at Voldsløkka in Oslo.
[132] Such as the Home Guard in Oslo (HV-02), the Special Operations Command (FSK), the military's EOD school (FAES) and the helicopter squadron (137th Airwing / 720 Squadron).

> *strategic and operational commands was, with few exceptions, alerted during the first 20-25 minutes after the incident.*"[133] (ibid., 217).

07.04 - Summary

As the chapter is split into technical and non-technical factors in communication, as explained in the beginning of chapter 07.03, the summary of this chapter will be similarly split.

07.04.01 - Technical factors

Regarding the technical aspect, it does not appear that communications equipment are a major factor towards the strategic levels' ability to perform their functions. Because the operational level are the ones responsible for operationalising the commands intent and relaying information back up to the strategic level, the problems mainly manifests itself there instead. The communicative links between the strategic and operational levels are usually not reliant on communications technology to same extent as the levels below. This because the strategic level normally do not have the need for "fast-paces" and rapid communication, as they convey "*intent*" and not "*operationalised commands*" (see chapter 03.02). However, the 11th September 2001 attacks are different in this aspect. Due to the need for top-level authorisation to intercept and ultimately shoot down the planes, this need for rapid communication also encompassed the strategic level. It can be argued that this became less problematic then it potentially could have been, due to the fact that the lines of communication used here, basically are the same as if the US military were to respond to a nuclear attack (see chapter 07.03.02 regarding continuity). It is therefore reasonable to assume that the people involved are trained in the use of this equipment and that the equipment itself are reliable and that back-ups exist. This does show the potential need for such a technical capacity at the strategic level, as potential black swan scenarios can occur, that will require the strategic level to rapidly respond to the operational and tactical levels' need for various authorisations. Typically, this can be attacks that would require the authorisation of the use of military force on domestic territory (other than the need for force transport capabilities that the military possess).

[133] Author's translation. The original text in Norwegian reads: "*I sum ser Forsvaret ut til å ha håndtert den innledende fasen av krisen på en god måte. Ferie-avviklingen til tross kom man raskt i gang med varsling og innkalling av personell. Forsvarets strategiske ledelse og FOHs kommandogruppe var med få unntak varslet i løpet av de første 20-25 minutter.*" (NOU 2012:14, 2012, p. 217).

When taking into consideration the technical difficulties the operational and tactical levels had, it is fair to assume that the strategic level, which normally does not have the same direct dependency on these systems, would risk experiencing similar problems, possibly even amplified do to the lack of experience with the day-to-day use of such systems in comparison to the other levels. Further incorporation of communications technology usually used for communication between strategic parts of a country's military and civilian command into general contingency plans, use of ACCOLC-systems or similar technology (Civil Contingencies Secretariat, 2011, p. 1-7), are seen as potential mitigating factors here, as also suggested by DSB (2012, p. 47-50).

However, as the London Assembly (2006, p. 42-47) notes, the reliance on and activation of such systems as ACCOLC may also result in the loss of communicative ability for personnel with equipment not covered by the technical solution. It can also put a further strain on the strategic level, as it has to know whom on what sites ACCOLC or similar systems are being implemented in, has telephones that are ACCOLC-enabled. The quite rational concern that one might impede communication rather than enable it can for instance be seen in the decision by the GCG in London during the 7 July 2005 attacks not to enable ACCOLC at one of the attack-sites for this very reason.[134] In other words: it needs to be worked into the contingency plans and continuously updated if it is to have any significant worth.

07.04.02 - Non-technical factors

The non-technical parts of communication (the chain of command), appears to be where system failures are more likely to occur, at least in a manner that affects the strategic level. An initial level of confusion are to be expected during an attack, but the more complex or multi-pronged an attack are, the more important it is that the strategic level comes into play as soon as possible. The operational level will be overwhelmed during this initial phase, and their capacity will mostly be limited to reacting to events as they unfold. The strategic level has the advantage of being "*above the fray*" and therefore has the capacity to seek out counter-measures against the ongoing attack and ways to regain the initiative. Especially in hierarchical structures, such as police and security forces, the strategic level also has the authority to initiate certain actions that the operational level does not have, such as requisitioning support from military units, shutting down physical and technical infrastructure and the likes.

[134] Aldgate station; one of the subway stations targeted in the first attack.

However, the strategic level sits atop a large and complex chain of command system. Because of this, it falls to reason that the higher up the chain of command the relevant strategic level are, the more complex the system are. All this leads back to the importance of available plans and (non-technical) lines of communication. As is seen with all three attacks, the convening of the entire strategic leadership takes time. This means the responsibility of handling the initial part of the strategic commands responsibilities falls to whomever of the strategic level that gets there first. This often leads to a few people having to fill several roles. Regardless of how well trained these people are, they will still need to rely on contingency plans that, among other things, lays out the chain of command and relevant courses of action depending on the situation at hand.

It is in this initial phase important that the strategic level shows itself active for the rest of the chain of command. As seen on 11th September 2001 when the FAA Boston contacted NEADS directly or on 7th July 2005 when COLP activated ACCOLC on their own accord, the rest of the system will act on its own if either the chains of command are unclear or if they are seen as not sufficiently effective or simply too slow. In situations like this the strategic level can quickly find itself out of the loop, compounding its difficulties in getting information about the situation from the chain of command, as other parts of it has taken matters into their own hands. Likewise, on 22 July 2011 POD was not able to properly insert itself into the chain of command in a timely fashion, leaving the strategic leadership in the Oslo police district’s staff to usurp its functions in the beginning. While in the example here, this might not have had major consequences, it still leaves the Oslo staff at a disadvantage, because they are, naturally, preoccupied with the situation in their own AO and neither have the sensors to effectively pick up other potential scenarios outside their AO. In addition, they are still dependant on the function of POD to requisition support from the military and be the link towards the national strategic leadership, and other relevant partners. Not intended for such a function, their contingency plans does not meet these unforeseen requirements. Still, being the biggest district in Norway, it was the one with the best premise to take this role.

Likewise, confusion over who are in charge and what parts of the strategic level that are operational at any given time is seen to have an adverse effect on the chain of command as a whole and especially for the strategic levels’ ability to lead. For instance, on 11 September 2001 there was confusion over who had the authority to order both military support and interception of planes, as seen by lower levels of FAA requisitioning military fighter planes, the Secret Service scrambling fighter planes from completely outside the normal chain of command, to the uncertainty whether the Vice-President had the authority to give the shoot-down order.[135] On 7 July 2005, such confusion lead to, among other things, the exclusion of the London Underground (in which the NCC are a part) from the GCG-meeting, because they were not aware of the meeting, and presumably, because they were not thought of by the other strategic commands. On 22 July 2011 it was long uncertain if the National Police Commissioner or the Assistant Police Commissioner was in charge. On the other side, such confusion regarding the chain of command can lead to assumptions that things are being done when they are not, because "it is being taken care of on a level way above ours", as was seen with the FAA Headquarters debating, but not acting on requesting military support, leaving other parts of the FAA content in the, false, belief that this was being taken care of.

To summarize, what is seen in all the three attacks are a partial breakdown of the strategic level in the chains of command, and the strategic levels' ability to insert themselves into the already established chain of command. In all scenarios, those at the strategic level did what they could with what they had, but they are dependent on contingency plans, which among other things includes an "order of battle"[136] to actually be able to perform their function. Due to the complexity and fluidity of such situations, the additional task of having to identify whom to contact and making sure they know that there are at least some form of strategic leadership present, in addition to performing their leadership-functions, uses up already sparse resources, both in the form of personnel and their capacity.

[135] It turns out he was conveying the orders from the President, but the uncertainty regarding this lead military commanders to delay the relaying of the order to the scrambled fighter planes and those already on CAP over Washington DC.

[136] Order of battle (OOB) is a military term that simplified can be said to refer to the overview of command structure, personnel, capabilities and hierarchical build-up of a predetermined force.

08 – Situational understanding

A key part in being able to lead and direct forces, both on the strategic, operational and tactical level, is having an understanding of the situation “on the ground”. Who, what, where – and to some extent why – are essential questions a commander must either know or strive to find the answer to. As mentioned in chapter 03.02, situational understanding is paramount for the command’s / strategic leadership’s ability to formulate a set of commander’s intent’s, by which they can direct their actions according to. The key here is *understanding* what is happening, and not just *knowing* it, i.e. adding knowledge to information so it becomes actionable information.

08.01 – Defining situational understanding

Alberts & Hayes (2006, p. 63-66) talks about “*sensemaking*” in regards to gaining the ability to use the knowledge of what is happening, in combination with more tacit knowledge, as a key part in the C2 process. They define situational awareness (i.e. situational understanding) as “*(…) the capability to extract meaningful activities and patterns from the battlespace picture (…)*” (ibid., p. 64). Likewise, Alberts, Garstka & Stein (2000, p. 69) identifies that C2 is basically a decision-making progress that are, among other things, dependent on feedback from the tactical end, thus underlining the importance of this awareness and understanding.

While information regarding the unfolding of events “on the ground” is one important factor, it alone will only let the commander see *what is happening* at any given time, instead of *what is likely to happen*. This alone will lead to a reactive response, as the commander is forced to respond according to the awareness of what is happening, as the lack of *understanding* hinders the ability to anticipate and pre-emptively make moves that can help in regaining the initiative of the situation. This understanding is also dependant on knowledge regarding the threat (who they are, what they want and so on), expertise in the relevant field and the ability to turn this knowledge into “actionable knowledge”; an adequate *understanding* of the situation (i.e. the patterns described by Alberts & Hayes above) on which one can act upon. Likewise, as stated by Builder, Bankes & Nordin (1999, p. 123), in their study of command and control in regards to several historical battles:

> “*1. Command concepts that turn out to correctly anticipate development on the battlefield will place less of a burden on the C2 system (enhancing its responsiveness, among other things).*
>
> *2. If development, articulation, and execution of command concepts are the essential elements of the C2 process, then C2 systems should, at a minimum, be designed to ensure that they support that process.”*

As mentioned in chapter 03.02, demonstrated by the C2-figure there, the information necessary for command to be able to obtain information for an adequate situational understanding are dependent on, among other things, the flow of information from the operational and tactical parts of the system. In addition, they in turn are dependent on the commander’s intent and the command’s known need for information (ref. the intelligence cycle in chapter 03.03) in order to be able to collect, analyse and convey the information that command needs. Hence, the command’s ability to collect sufficient information to use as a base on which to build their situational understanding also depends on their ability to communicate their needs and intents down the chain of command. This part regarding communication is addressed separately in chapter 07.

08.02 – Situational understanding

While relatively easy to draw up models of, the practical nature of situational understanding during a crisis, especially one as fluid as an ongoing terror attack is not easy. The sheer amount of information that needs to be collected, analysed and disseminated can be enormous, and the risk of information overload (Buckley, 2014, p. 198-199) is ever-present. Equally challenging is the process of taking all that information and use it to create an understanding of the situation. An important part of this is as Buckley (ibid.) explains; the "weeding out" of information considered useless or not pertinent to the mission and situation at hand. Following the C2 model in chapter 03.02, this will typically be the responsibility of the control level. This requires both a certain situational understanding, in order to be able to differentiate between vital and non-vital information, and a knowledge of what kind of information the command needs. The responsibility for conveying these needs for information down the chain of command lies exclusively with the commander. Buckley (ibid.) notes “*Ultimately, the criteria for inclusion* [of intelligence] *in the repository will be decided by the agency’s senior intelligence manager and laid down in procedures.*” While he primarily are describing the prevention of information overload in a day-to-day intelligence system in a law-enforcement agency, this “gatekeeper” function can be seen as to equally apply to the control level using the commander’s intent as a selection criteria to help avoid information overload, and further evolve the situational understanding.[137]

As put forward by Alberts et.al. (2001, p. 212-215) the ability to synchronize ones capabilities and their capacities (ibid., p. 57-60), a central part in any military, police or security-operation, are becoming ever more challenging because of the complexity of the situation, the heterogeneity of the responders and the fast pace of events. As a shared situational understanding is key to this process (ibid.) the quality and correctness of such an understanding is paramount. It is likewise also important for all parties to be aware of the limitations of this shared understanding; that it is created based on the best information *available* at the time and may not reflect the reality with complete accuracy. For a strategic commander, to keep this in mind, and make sure that this understanding are shared by the other elements of the chain of command, is an important task. It opens the possibility for greater potential autonomy for the forces on the ground, and it can be argued to stimulate the understanding of the importance of collecting and disseminating information up and down the chain of command; sort of a “The better information I'm able to collect and pass on, the better information I will get in return and the better I will be able to do my job”.

08.02.01 – 11th September 2001

As shown, in chapters 07.03.01 and 07.03.02, the problems with the chains of command on 11 September 2001 affected the strategic levels’ ability to effectively communicate. Likewise, these communication difficulties also affected the NCA’s ability to receive timely information pertinent to the situation at hand, in order to gain an adequate understanding of the situation. As with the assessment of communications, the situational understanding in this case consists of two main parts: the situational understanding in regards to the specifics of the situation at hand (i.e. what planes are hijacked and where are they) and the situational understanding in regards to understanding what is actually happening. In the case of a situation such as on 11 September 2001, both of these understandings are pivotal in order to be able to

[137] It is worth noting that despite Buckley’s quite apt “fruit analogy” (2014, p. 7-12), the generalisation in this example makes the comparison between military, intelligence and law enforcement organizations and their intelligence management valid. As Buckley also notes (ibid., p. 10) “*They are all fruits.* (…) *Intelligence management in all three disciplines is fundamentally similar.*”

respond properly. There is an obvious need to know what planes are hijacked and where they are, and it is equally important to understand what is actually happening in order to mount a response against any further parts of the attack (in this case, the RENEGADE scenario).

The first part of knowing what planes are hijacked and where they are heading is a level of detail that normally would rest primarily with the operational level and not the strategic one. However, because to the circumstances of this attack, such information becomes directly relevant to the strategic level, due to the need to authorise or deny the use of military force against civilians on domestic territory (i.e. shooting down hijacked planes). Because of the consequences of such a decision, is has to be taken by the strategic level, and therefore they need a high level of specific information regarding the more "operational" situation in order to be able to make an informed decision on such a matter. It is not so much the details in regards to the planes' location that are paramount here (that information is almost of no value to the strategic level). What is important here is what their position *means*, i.e.;

- Are there nearby assets capable of intercepting the planes?
    - Determines what response-options that is realistically available.
- What are the planes' destination / target and are they close?
    - Determines the time-frame available to make a decision and outlines the risk the planes pose (in regards to their assumed targets).
- Where are the planes now and where will they be at the moment of interception?
    - Determines the potential collateral damage of shooting down the plane (such as the fallout of the debris and its potential to cause additional damage).[138]

As previously explained, and as noted in The 9/11 Commission Report (2004, p. 31-34), NEADS had just 9 minutes of forewarning regarding American 11 before it crashed into the WTC and no warning in regards to the other planes. Likewise, NORAD was not aware of the planes before they crashed. In hindsight, it is clear that no realistic response would have been able to intercept the planes in time, but, as is the point in this thesis, there was no possible way to know that *during* the attack itself. When three or four planes have been hijacked, the potential of several more hijacked planes becomes a highly likely scenario.

[138] The damage-potential of the debris fallout was made frighteningly clear by the bombing of Pan Am 103, also known as the Lockerbie-bombing, where the debris crashed into the town of Lockerbie in Scotland, causing additional casualties. Similar fallout over a large city-centre would potentially be catastrophic.

On 11 September there were several lapses of the situational understanding in both the military and the civilian strategic command as well as within the top-level strategic command. It is in this case worth noting that since both the military and civilian strategic commands, as shown in the figure in chapter 07.03.01, are primary sources of both information and advice on further courses of action to the top-level strategic command, any problems with their situational understanding carries with it a high risk in propagating to the top-level. Normally it can be a mitigating factor that the civilian and military chains of command are separated and are communicating upwards independently of one another. In addition to getting two viewpoints on a situation, this duality can also function as a fail-safe against flawed situational understanding within one of the chains of command. However, in this case, and as shown in chapters 07.02.01, 07.03.01 and 07.03.02, this attack led to a high level of coordination and exchange of information between the chains of command. Moreover, when this also occurred not exclusively along the pre-determined lines, the systems that could have picked up on this, did not appear to function.

Amplifying this was the fact that the attack-concept of using planes as virtual guided missiles was not a threat that had been realistically planned for. While this idea was not new or completely unheard of, it was apparently not considered to be a probable scenario at the time. The so-called "Gore Commission" (named after former Vice-President Al Gore) finalised in 1997 a report regarding aviation safety and security.[139] In it, the new danger against civilian planes was considered to be surface-to-air missiles used to shoot down planes. The concept of suicide-hijackings (RENEGADES) was not discussed in the report. There was furthermore nothing in the manuals or policies of the FAA that considered such events to be likely to occur. On the contrary, the prevailing assessment was that potential hijackers would act as they always had; force the plane to land for further negotiations or attempt to get the plane to fly to a safe airport (ibid., p. 82-86). As The 9/11 Commission Report (ibid., p. 85) notes:

> "*According to the FAA, the record had shown that the longer a hijacking persisted, the more likely it was to end peacefully. The strategy operated on the fundamental assumption that hijackers issue negotiable demands (most often for asylum or release of prisoners) and that, as one FAA official put it, 'suicide wasn't in the game plan' of hijackers.*"

[139] The full name of the report are "Final Report of the White House Commission on Aviation Safety and Security".

And while there was, in the months leading up to the attack, several reports circulating among the top levels of government and security in the US, and a general level of worry for fear of an impending terror attack, also possibly involving planes (ibid., p. 256-265), the concept of suicide-hijacking was still not seen as a threat. This becomes clear in, among other things, the 6th August 2001 Presidential Daily Brief titled "Bin Ladin Determined To Strike US" where terror against planes are mentioned, but in the traditional hijack-for-release manner. Likewise, material given by the FAA to civilian airlines did mentioned the concept of suicide hijacking, but said "*(...) fortunately, we have no indication that any group is currently thinking in that direction.*" (ibid., p. 264). As such, the attack-concept that would later became known as RENEGADE, was not considered probable or likely by neither the civilian or military departments in charge on the day of the attack. How much this affected the ability to identify what was happening is not certain, but it is more likely than not that the lack of consideration for such a black swan event contributed to the chaos among decision makers and advisors that day.

The fact that the modus operandi of the attack took the entire system by surprise, there was a need for a high level of improvisation. It is possible that because of this, and the fact that existing plans did not take into account unknown scenarios, people were unable to identify that the existing lines of communication did not work, and that people that should have been inserted into the chains of command, was not. This lack of understanding what the situation required led to people falling back on known methods of contact, without being able to realise that they did not work, as was the case with the many teleconferences that occurred that day (as mentioned in chapter 07.03.01 and 07.03.02).

08.02.02 – 7th July 2005

After the bombs had detonated in the Underground, it was unclear whether it was an accident or if it was an attack. However, at appx. 10 minutes after the explosions, the fire brigade at Aldgate station reported that it suspected that it had been a bomb that had caused the damage. Just minutes after, the COLP and the BTP, independent of one-another, reported up their chains of command that there had been bomb attacks. When three explosions occur on different, unconnected subway trains within minutes of one another, terror rapidly becomes a highly probable theory. With additional information coming in that the first responders suspects bomb-damage, terror becomes the most likely scenario, and responding as such is seen as prudent. The Coroner's Inquest (2011, p. 39) and the London Assembly (2006, p. 38) notes that according to the LESLP manual in place at the time, when one emergency service declares that a major incident had happened – thus setting in motion a range of actions including the activation of the different coordinating groups, of which the GCG is one – this is applies to all the services. However, as noted by the London Assembly: "*On 7 July, each of the emergency services arriving at the scene of the explosions separately declared major incident within their own service. It is not clear to us why each of the emergency services found it necessary separately to declare major incidents.*" (ibid., p. 38). As the initial response covered three different bomb-sites, this intra-agency communication in a place where it was meant to be *inter*-agency, caused a fragmentation of information within each of the services. As an example, during the first conference call between the emergency and transport services, the so called "first alert call"[140] at 09:25, a major incident had not yet been declared at Edgware Road station[141] and the MPS had just 6 minutes before been officially called out to Aldgate station, even though the explosion occurred there at 08:51, and BTP had been on-site at 08:55 (ibid., p. 24 & 38).

While the operational level of MPS were most likely aware of the incident at Aldgate before 09:19, it is unclear why the BTP did not contact the MPS sooner, because the operational level's awareness of a situation does not equate to the strategic level's awareness. Also, since the MPS has a lead-role in coordinating the polices' effort, and the BTP are a liaison between the NCC and the other emergency services, there is here a chain of information between the police and the transport sector that can benefit both. As an example: the London Underground decided to issue a so-called "Code AMBER" at appx. 09:14, which halts the operations of the Underground (Coroner's Inquest, 2011, p. 41). At roughly the same time, the decision to evacuate the entire Underground was taken (London Assembly, 2006, p. 80). This lead to a massive influx of people in the streets, as mentioned in chapter 07.03.03. If the other emergency services are not aware of this, the sheer confusion of a mass-evacuation of the Underground can easily be misinterpreted. In addition, as terror was the primary scenario at 09:40 when the Underground was evacuated, this also presents the various police forces with the challenge of clearing out the masses of people, to prevent further high-yield targets risking attack. Because the London Underground did not have predetermined areas for people evacuated from its stations (ibid., p. 71) crowds were, naturally, gathered outside the stations. While it at this time had not occurred another attack, with the Madrid attacks fresh in mind, not considering further

[140] When a major incident takes place, the various control centres are alerted by a first alert call – a teleconference.
[141] One of the bombsites.

follow-up attacks would show a lack in understanding the potential risks at hand. Whether this factor was considered by the strategic level when the order to evacuate was given are not known. When the No. 30 bus exploded just 7 minutes after the evacuation had commenced, this scenario would be even more obvious.

The importance of this information reaching the other emergency services are underscored by the Coroner, noting that "*The fact that the Underground is being either suspended or evacuated, and that very large numbers of passengers (over 250,000 at any one time during the rush hour) are about to be disgorged suddenly onto the streets of London, are matters that London's emergency and transport agencies need to be informed about and there is a risk to life it they are not.*" (ibid., p. 71) The London Underground had given this information to an officer from the BTP and had the understanding that the BTP would disseminate this information to the other services. It is unclear as to what extent this was done. It is also unclear as to what extent this was relayed to the Bus Services, but as they had not been made aware of the explosions in the Underground until after the explosion on the No. 30 bus, this is probably unlikely (ibid., p. 29). With so much happening at once, it is unclear as to why the strategic levels of the police forces did not seek to link up with their counterparts in the London Underground, or Traffic for London, for that matter. A basic understanding of the situation, and keeping the Madrid-attacks fresh in mind, would show the importance of close cooperation with them, both to better facilitate the police and FRM-response in an environment somewhat unknown to them (but very well known to the London Underground), and as a sensor for information as situational updates.

As mentioned in chapter 07.03.03, as to what extent COBR was involved during the initial phase of the attack is uncertain. However, the House of Commons report no. 1087 (2006, p. 7) writes that COBR early became aware of the strong possibility of this being a terror attack. The timing of this awareness are not specified further, and it stands to reason that this was a realisation that evolved similarly to the one in the police and GCG. However, due to initial confusion regarding the situation at the Underground led the police strategic command to believe that there had been five explosions, and not three. This can be seen by the press conference at 11:15 where the Commissioner of the MPS reported that there had been a total of six explosions – five in the underground and one on Bus no. 30 (London Assembly, 2006, p. 13). This means that the strategic leadership, during the initial phase, worked with the assumption that there had been five and not three attacks against the Underground. As the London Assembly notes:

> "*Chaos and confusion are the defining characteristics of the early stages of a major incident, and especially multiple incidents at different sites across London. However, there is scope for improving the systems by which information is gathered and shared among London's transport, emergency and other services involved in the response.*" (ibid.)

How this error regarding the situation came to be are uncertain, but due to the fractured ways of relaying information up the chains of command, as noted in chapter 07.03.03, this is likely to have played a part in this erroneous situational understanding. That this understanding still stands more than two hours after the incident began supports this theory, as it by then must have been clear to other levels down the chain of command that there was "only" three bombsites in the Underground. A proper situational understanding could have helped in identifying that the information coming in does not seem to match the assumption that five targets in the Underground had been hit, but rather three. How this could have altered the response is uncertain, but what is clear is the fact that operating with a wrong premise carries with it a high risk of diminishing the quality of the response.

08.02.03 – 22nd July 2011

As already mentioned in chapter 07.03.04 there was several breakdowns in the flow of information up the chain of command on 22 July 2011, which in turn affected the situational understanding of both the local strategic command in Oslo police district, and also at the national strategic level of the police; POD. Central in the assessment of the situational understanding during the initial phase of the terror attack is the point of activating the specialized terror plans[142] as mentioned in chapter 07.03.04. The 22nd July Commission describes these plans as: "*Plans of this kind are developed specifically for the purpose of rapidly and effectively initiating actions that experience have shown are the right ones in such chaotic situations.*"[143] (NOU 2012:14, 2012, p. 156). The general effect that can be expected from these plans include increased capacity regarding police resource, potentially limiting freedom of

[142] The specifics of the plans itself will not be debated here as they are classified (NOU 2014:14, 2012, p. 155). Also, since they were not activated during the golden hour, it would not be as relevant to debate the specifics of them either way, as it is the fact that they were not activated that is the point here.

[143] Author's translating. The original text in Norwegian reads: "*Planverk av denne typen er utviklet nettopp med det formål å raskt og effektivt kunne iverksette en del handlingsmønstre som erfaringsmessig er de riktige i kaotiske situasjoner.*" (ibid., p. 156)

movement and freedom of operation for the attackers, and safeguarding potential high-risk targets (ibid., p. 155).

The terror plans can be activated by the police chief in an affected district if it is considered necessary and the situation is urgent. Naturally, POD are to be alerted as soon as possible if a district does this. But the standard procedure dictates that the National Police Commissioner, via POD, have the primary responsibility to activate these plans (ibid., p. 154-157). Neither the acting commissioner (Assistant National Commissioner) or the National Police Commissioner considered activating these plans. It appears that in the leadership of POD and the staff, there were initial confusion as to if they were faced with a terror attack or some other form of incident. The police in Oslo were from the start aware of the fact that this was a terror attack.

The initial message from the first unit on the bombsite, designated S20, which arrived on scene less than 4 minutes after the blast, reported up the chain of command that a bomb had exploded in the Government quarters (ibid., 85-86). Few minutes after, the tactical commander on the scene reported up the chain of command that a terror attack was taking place, that the staff needed to be mobilized, Delta needed to be called out and that all patrols were to arm themselves. In addition, the 22nd July Commission notes: "*Further he told the operations centre to ' ... press the biggest button'.*"[144] (ibid., p. 87). There appears to have been a general understanding within most of the police (ibid., p.90-91), the strategic level within the FRM-services (ibid., p. 201-202) and the military ibid., p. 216-217 & 230-231) that this was in fact a terror attack. This initial, general understanding of the situation does not appear to be the preceded by any specific communication between these units, but rather a general understanding that a massive explosion at the very centre of political power in Norway, is most likely terror.[145] Why this understanding did not reach the staff in POD are unknown. One possible reason is that because it appeared to be so obvious to those closer to the situation, that they did not see the need to relay that information up the chain of command.

The 22nd July Commission further notes that later that day, at times when it was obvious to the staff in POD that a terror attack was taking place, the terror plans was still not considered

[144] Author's translating. The original text in Norwegian reads "*Ytterligere ba han operasjonssentralen om '... å trykke på den aller største knappen'.*" This is a colloquial term within the Norwegian police which refers to pressing a panic button, i.e. activating any and all resources available.

[145] It is also a point to note that as electricity, and not gas, are used for heating and the likes in Norway, a gas-explosion of that size (also without any continuing fire due to leaking gas) will probably be dismissed by most as a highly unlikely reason for such an explosion.

activated. Part of the reason may have been that the National Police Commissioner was new in this position (having acceded the position two weeks earlier from a position outside the police), and he was not aware of the existence of such plans. Several parts of the military went on a heightened state of alert as ordered by FOH at 16:19 and this was extended to all military units in-country at 17:46 (ibid., p. 231), but there was at no time considered from POD that the police should do the same (ibid., p. 156). While, at this point, most people knew that a terror attack was taking place, it can be debated whether or not the consequences of this was understood. In other words, that the understanding of the situation at hand was unclear. The lack of plans one can lean on for assistance in such chaotic situations may cause a further loss of situational awareness, due to information overload or the lack of processed and analysed information (as described in chapter 03.03 with the intelligence cycle).

Perhaps the clearest example of the dissonance between what was known and what was understood is shown in the initial use of the Delta units for search and rescue at the bombsite in Oslo. As mentioned earlier (see chapter 06.03) Delta are the polices' primary hostage-rescue and counter-terrorism unit. Being the only *de facto* special operations capability the police has, they can be considered a strategic resource in that such a unit can be deployed as a means to regain the initiative during such attacks, and that they generally have a higher capacity then the rest of the police force. The 22nd July Commission (2012:14, 2012, p. 104) comments on that while the unit proved a valuable resource in the search and rescue work, their continuing capacity to respond to potential secondary attacks was diminished by using manpower for this kind of work, also increasing the time they would need to re-deploy to another attack. The attrition on the personnel would also limit their ability to remain on stand-by for a longer amount of time. Likewise, the risk and potential for a secondary attack was well known among both the strategic and operational leadership, and had been considered a potential scenario almost since the instant the bomb exploded (ibid., p. 95-97). In addition, it does not seem that the risk of a secondary bomb attack *at the primary bomb site,* aimed at incapacitating the responding forces, was taken into account when deploying such a large part of a strategic resource to a location where their primary mission are not applicable, although this being a known risk. (ibid., p. 87) (Aman, 2007, p. 45-47 & 81) (Bolz, Dudonis & Schulz, 2012, p. 222, 240 & 315).

A clear message of intent, based on maintaining an as-strong-as-possible secondary response capability, from the strategic level seems to be lacking here, thus affecting the deployment of resources. While this cannot be attributed to POD, as they are not supposed to have such direct command over the operational or tactical level, the strategic staff in the Oslo police district should, ideally have seen this and acted upon it, as force protection with the intent of maintaining strategic capabilities, can be seen as a responsibility of the strategic level. Typically, a clear message of intent with regards to the use and deployment of special resources should cover this. This is of course a trade-off between force protection and saving lives, and second-guessing such decisions is often not the right thing to do. However, the problem here is that it appears that there was not taken a decision regarding this, it just happened on its own.

08.03 - Summary

As with communication in chapter 07, it is here also seen that functioning contingency plans, or the lack thereof, potentially can impact the situational understanding and the strategic levels' ability to transform their situational understanding into a set of commander's intents. While confusion, and often contradictory or competing information, are to be expected during the initial phase, it is the strategic levels' responsibility to gather the information and create an understanding of the situation at hand, in order to be able to act accordingly. While the challenges of this manifests itself differently in the three attacks, the result and reasons for this have some things in common.

Due to the extraordinary circumstances of the 11th September 2001 attacks, the top strategic level here had to react directly to information from both the tactical and the operational levels, while at the same time attempting to maintain their strategic overlook of the situation. Compounding these challenges was the fact that there was no plan of action for such RENEGADE scenarios. This combination of information overload and the need to make up the plan as they went along caused an inability to filter out information and forcing them to react to an erroneous understanding of the situation, such as responding to a plane that was no threat, responding to a plane that had already crashed, and a lack of overview regarding the resources at hand.

On 7 July 2005 a fragmented system of channelling information led to a misunderstanding of the scope of the situation that continued out the entire golden hour. This lack of clear lines of communication also led to the transport sector not having the same situational understanding as the police, despite it being their objects that was being attacked. Also, keeping the 2004 Madrid attacks in mind, it is unclear whether or not the risk of gathering people outside Underground stations was taken into consideration by the strategic command in the police. Considering their erroneous understanding that there had been five, and not three explosions, the potential vulnerability such a massing of people right outside the very objects that were under attack, does not appear to have been fully considered. While an evacuation obviously is necessary and the prudent course of action, there needs to be available resources to further complete the evacuation by clearing the surrounding area of the masses of people. Looking at 22 July 2011 it becomes clear that the strategic leadership in POD did not have the same situational understanding as the other strategic and operational commands. As an example, the fact that the contingency plans for terror attacks was unknown to them, and the fact that the potential that this in fact was a terror attack was not considered in the beginning, shows a dissonance between PODs understanding of the situation, and the rest of the police and security apparatus. The military began preparing resources they know could be called upon by the police and increased the security at their own bases, and the police in Oslo took similar actions.

What is seen as a recurring factor here is the lacking in the ability of the strategic levels to correctly understand and interpret the information that comes to them. Due to their responsibility to formulate an overall response, the strategic levels not only has to acknowledge what is happening, but also consider what this means, how to respond, and – most important of all – the consequences of their response. As debated in the beginning of this chapter, this is the difference between *understanding* versus just *knowing* what is happening. And it is this understanding that appears to be somewhat lacking, albeit for different reasons. It also seems that the understanding of one's own role as the strategic level, and the responsibilities that comes with that are fully not understood. Namely responsibility to actively seek information and actively lead, and not simply be passive recipients of information. In understanding the importance of a proper situational understanding, one can also be expected to understand the importance of linking up with the relevant chains of command on one's own accord, if the information received is seen as insufficient.

09 – Conclusions

As shown throughout, the capacity of the strategic levels command and control capabilities are very much dependant on its capacities in regards to communication and situational understanding. Likewise, it is important for these systems to have at least a minimum of capacity in regards to system resilience. These factors of communication and situational understanding are themselves are, and one is dependent on the other to function properly. The situational understanding are dependent on the ability to communicate in order to request and receive the necessary information needed to get that understanding. Likewise, communication is dependent on the situational understanding for the strategic level to be able to direct its communication to the correct resources. In addition, while these two are interconnected, they are both depending on a functioning systemic resilience in order to prevent a lapse in either of them. If either fails it will have an impact on the other one as well, and the system resilience is key to both preventing one or the other from failing and – equally important – to mitigate the negative outcome should one of the capacities in communication or situational understanding fail.

What is seen as a recurring challenge throughout the three attacks is a lack of relevant contingency plans and an understanding of ones role as the strategic part of the response effort. Crisis management in the initial phase are an incredibly complex task for all the levels, and especially for the strategic level in regards to the topics being discussed in this thesis. It is therefore likely that the more complex an attack is,[146] the more pronounced any challenges the strategic level has with these topics will become, and the resulting negative influence will follow.

As is seen throughout the three attacks, the entire system itself seems to have an innate systemic resilience against disruptions to the strategic levels' capacity. However, this does not appear to be centred around the strategic level, but rather the operational. When the operational level senses that the strategic level is not functioning according to how they expect, they will begin to act on their own to fill the gap. Such as when either a lack of situational understanding or a lack of ability to communicate results in the strategic level not being able to convey their

[146] Either by the size, scope or technicality of the attack. A "low-tech" attack like Mumbai or Paris would be complex due to its scope and the use of multiple simultaneous attacks, and a more "high-tech" attack such as a single RENEGADE plane would also be complex due to the methods one would have to bring to bear to respond to it.

commander's intents, the operational level seems to fall back to the basic, and obvious, intent, which is to stop the attack, prevent further attacks and save lives. Such as with the closing of the national airspace over continental USA without prior clearance from the top-level of the FAA, the activation of the ACCOLC-system in London or activation of terror plans by the Oslo police district and not POD. All these happened, to one extent or the other, outside of the supposed chain of command. The fact that such a "fail-safe" exists within the system is in itself a good thing, but it can also be argued that it also poses some challenges.

For the first part, if the strategic level partly fails due to a lack of contingency plans, it is fair to assume that backup-plans that would allow the operational level to take over their role, would not be better than the ones that were available to the strategic level – and whom was obviously not good enough. This would force the operational level to take command and act on their own initiative. Without this being based on standing orders and regulations, a highly hierarchical system would probably be less likely to go against the perceived chains of command, and perhaps not act at all, or in the very least overly cautious. This fail-safe also hedges on that people, whom most likely already are occupied with their own primary responsibilities in the situation at hand, does this by their own initiative. This makes this fail-safe potentially highly vulnerable. Also, the lack of communication does not have to be because the strategic level is not working properly.

As seen with the mentioned ACCOLC-activation in London, this was not done because the GCG had not considered this. They had in fact considered this very option, but decided against it, as they feared the consequences would outweigh the gains from it. COLP was not aware of this, but activated the system because they saw it as necessary and they had not been made aware of the GCG's denial of the use of this system. There is no reason to believe that any of the parties here acted with anything other than the best interests in mind, but this serves to demonstrate the importance of communication of intent. Because what makes a commander's intent different from a specific order is that is, as described earlier, contains both the desired end-state *and* the parameters for which to act to achieve this. So by taking the initiative and stepping in when one are under the impression that the strategic level are not functional, one also runs the risk of acting against reasoning taken by someone with a – possibly – better situational understanding.

The other, and more potent risk, in relying on lower levels of the chain of command to "pick up the slack" is exemplified by the various deployments of fighter planes during the 11th September attacks; the lack of coordination between these actions. Several sets of fighter planes were scrambled but no one had the full overview of the extent of this deployment of military assets. Besides the ethical sides of deploying powerful offensive military capabilities on domestic territory without the proper authorizations, this creates a highly dangerous situation. As the planes was unaware of one another, they ran the risk of engaging each other or responding to the same target differently. One can only imagine the chaos that would ensue in the NCA if a fighter plane they were not aware of shot down a civilian plane. In addition, considering the confusion in the different parts of the strategic and operational commands regarding what planes were actually RENEGADE and which was not, the risk of shooting down the wrong plane would also be present. This is of course an absolute worst-case scenario, but it serves to demonstrate the key challenge for when operational levels, or lower strategic levels for that matter, are forced or feel that they are forced, to take over the role of the strategic command. Thus showing the need for systemic resilience, and the lack thereof during the three attacks.

Because, as disruptions in both the communication and the situational understanding of the strategic level's occurred in all the three attacks, it can be argued that what partly made those disruptions influence the situation to such an extent, was the lack of proper systemic resilience to shore up any such disruptions. As previously argued, an understanding of one's role, in the wider sense of the word, seems to have been lacking. This is also something that could have had a clear systemic resilience function, in addition to proper contingency plans. Understanding the general role of the strategic level and the responsibilities that follow, gives an increased capacity to act when contingency plans either come up short or are non-existent. This is because the role of the strategic level in coordinating the effort, in relaying its intent and in gathering the information to use to formulate a commanders intent, forces the strategic level to seek out information, seek out the other parts in the chain of command and identify lacks in the situational understanding.

To one extent or another, the combination of this lack of understanding the role of the strategic level and the lack of having (or lack of use of) proper contingency plans, can be said to have had an adverse effect on the strategic levels' capabilities to function, in the immediate response after the terror attacks in the US in 2001, England in 2005 and Norway in 2011, regarding communication and situational understanding. It is worth noting that while the capability is seen to increase as the time goes and the response moves into towards the post-incident / recovery phase, it is in the critical golden hour a proper functioning system are of highest importance.

Bibliography

Alberts, D.S. (1996). *The Unintended Consequences of Information Age Technologies: Avoiding the Pitfalls, Seizing the Initiative*. Washington DC: National Defence University Press.

Alberts, D.S., Gartska, J.J., Hayes, R.E. & Signori, D.A. (2001). *Understanding Information Age Warfare*. Washington DC: Office of the Assistant Secretary of Defence; Command and Control Research Program.

Alberts, D.S., Garstka, J.J. & Stein, F.P. (2000). *Network Centric Warfare: Developing and Leveraging Information Superiority*. (2nd edition). Washington DC: Office of the Assistant Secretary of Defence; Command and Control Research Program

Alberts, D.S. & Hayes, R.E. (2006). *Understanding Command and Control*. Washington DC: Office of the Assistant Secretary of Defence; Command and Control Research Program.

Allard, K. (1996). *Command, Control and the Common Defence. Revised edition*. Washington DC: National Defence University, Institute for National Strategic Studies.

Aman, M. (2007). *Preventing Terrorist Suicide Attacks*. USA: Jones and Bartlett Publishers.

Aven, T. (2015). *Risikostyring*. (2nd edition). Oslo: Universitetsforlaget.

BBC. (2015, 9 December). Paris attacks: What happened on the night. *BBC News*. Retrieved 6 May 2017 from http://www.bbc.com/news/world-europe-34818994

Bergen, P. (2011). *The Longest War: The enduring conflict between America and al-Qaeda*. New York: Free Press

Bjørgo, T. (2013). *Strategies for Preventing Terrorism*. UK: Palgrave Macmillian.

Boin, A. & McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. *Journal of Contingencies and Crisis Management, 15*(1), p. 50-59.

Bolz, F.jr., Dudonis, K.J. & Schulz, D.P. (2012). *The Counterterrorism Handbook: Tactics, Procedures, and Techniques.* (4th edition). Florida: CRC Press.

Buckley, J. (2014). *Managing Intelligence. A Guide for Law Enforcement Professionals*. Florida: CRC Press.

Builder, C.H., Bankes, S.C. & Nordin R. (1999). *Command Concepts: A theory derived from the practice of command and control.* Washington DC: RAND National Defence Research Institute.

Callimachi, R., & Schmitt, E. (2017, 3 June). Manchester Bomber Met With ISIS Unit in Libya, Officials Say. *The New York Times*. Retrieved 3 June 2017 from https://www.nytimes.com/2017/06/03/world/middleeast/manchester-bombing-salman-abedi-islamic-state-libya.html

Cherry, R.G. (1921). The Initiative in War. *The Journal of the Royal United Service Institution, 66*(461), p. 87-100.

Civil Contingencies Secretariat (2011). *Towards Achieving Resilient Telecommunications: Interim Guidance*. UK: Cabinet Office. Retrieved 23 May 2017 from https://www.gov.uk/government/publications/resilient-communications-documents

de Graaf, B. (2012). *Evaluating Counterterrorism Performance. A comparative study*. New York: Routledge.

Direktoratet for Samfunnssikkerhet og Beredskap (DSB). (2004). *Erfaringer etter terrorangrepet i Madrid. Krisehåndtering og ressurstilgjengelighet i forbindelse med en tenkt tilsvarende hendelse i Oslo*. Norge: DSB.

Direktoratet for Samfunnssikkerhet og Beredskap (DSB). (2012). *Samfunnets sårbarhet overfor bortfall av elektronisk kommunikasjon*. Norge: DSB

Direktoratet for Samfunnssikkerhet og Beredskap (DSB). (2014). *Nasjonalt risikobilde 2014*. Norge: DSB. (Also available in English from https://www.dsb.no/rapporter-og-evalueringer/national-risk-analysis-2014/ as per 16 January 2017).

Dunlap, C.J. Jr. (2005). The Thick Green Line: The Growing Involvement of Military Forces in Domestic Law Enforcement. In Newburn, T. (ed.), *Policing. Key Readings*. (p. 786-796). UK: Routledge.

Engen, O.A.H. et.al. (2016). *Perspektiver på samfunnssikkerhet*. Oslo: Cappellen Damm Akademisk.

Etterretningstjenesten. (2015). *Fokus 2015. Etterretningstjenestens vurdering.* Retrieved 25 August 2016 from http://forsvaret.no/ForsvaretDocuments/FOKUS2015-endelig.pdf

Etterretningstjenesten. (2016). *Fokus 2016. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.* Retrieved 25 August 2016 from http://forsvaret.no/fakta_/ForsvaretDocuments/Fokus%202016.pdf

Etterretningstjenesten. (2017). *Fokus 2017. Etterretningstenesta si vurdering av aktuelle tryggningsutfordringar*. Retrieved 6 February 2017 from https://forsvaret.no/fakta_/ForsvaretDocuments/Fokus2017.pdf

Europol. (2016). *Te-Sat 2016. European Union Terrorism Situation and Trend Report 2016.* The Netherlands: Europol. Retrieved 6 November 2016 from https://www.europol.europa.eu/sites/default/files/documents/europol_tesat_2016.pdf

Fjelland, R. (2009). *Innføring i vitenskapsteori*. (6th issue). Oslo: Universitetsforlaget

Flage, R. & Aven, T. (2009). Expressing and communicating uncertainty in relation to quantitative risk analysis. *Reliability and Risk Analysis: Theory and Applications*. *2*(13), p. 9-18.

Flin, R. (1996). *Sitting in the Hot Seat: Leaders and Teams for Critical Incident Management*. UK: John Wiley & Sons Ltd.

Forsvaret. (2013). *Etterretningsdoktrinen*. Oslo: Forsvaret.

Frattini, B. et.al. (2016). Prehospital rescue organization during the November 2015 Paris terrorist attacks. *Journal of Emergency Medical Services*. *41*(5), p. 24-30. Retrieved 3 June 2017 from http://www.jems.com/articles/print/volume-41/issue-5/features/prehospital-rescue-organization-during-the-november-2015-paris-terrorist-attacks.html

Gill, P. & Phythian, M. (2012). *Intelligence in an Insecure World.* (2nd edition). UK: Polity Press

Gladwell, M. (2003). Connecting the dots: The paradoxes of intelligence reform. *The New Yorker, 2003*(10), p. 83-88.

Grønmo, S. (2011). *Samfunnsvitenskapelige metoder.* (4th edition). Bergen: Fagbokforlaget

Hammervoll, T. (2014). *Beredskapslogistikk*. Bergen: Fagbokforlaget.

Her Majesty's Coroner. (2011). *Coroner's Inquest into the London Bombings of 7 July 2005*. UK: Home Office (In addition: Full transcripts available as of 15 December 2016 from http://webarchive.nationalarchives.gov.uk/20120216072438/http:/7julyinquests.independent.gov.uk/)

House of Commons report no. 1087 (05-2006). (2006). *Report of the Official Account of the Bombings in London on 7th July 2005*. UK: The Stationary Office Limited

Hoffman, B. (2006). *Inside terrorism. Revised and extended edition*. New York: Columbia University Press.

ISC (Intelligence and Security Committee). (2006). *Intelligence and Security Committee: Report into the London Terrorist Attacks on 7 July 2005*. UK: The Stationary Office Limited.

ISC (Intelligence and Security Committee). (2009). *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attack on 7 July 2005*. UK: The Stationary Office Limited

Johannessen, A., Tufte, P.A., Christoffersen, L. (2011). *Introduksjon til samfunnsvitenskapelig metode.* (4th edition, 2nd issue). Oslo: Abstrakt forlag

Johansson, B.J.E. & Pearce, P.V. (2014). Organizational Agility: An Overview. In Berggren, P. (ed.), Nählinder, S. (ed.) & Svensson, E. (ed.), *Assessing Command and Control Effectiveness: Dealing with a Changing World*. (p. 71-82). UK: Ashgate.

Johnson, P. (2015, 7 July). Ten years on from 7/7: How London responded to the terror attack. *The Telegraph*. Retrieved 3 June 2017 from http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/11715557/Ten-years-on-from-77-How-London-responded-to-the-terror-attack.html

Kiesling, E.C. (2001). On War Without the Fog. *Military Review. 2001*(5), p. 85-87.

Kölle, R., Markarian, G. & Tarter, A. (2011). *Aviation Security Engineering. A Hollistic Approach*. Boston: Artech House

Lerner, E.B. & Moscati R.M. (2001). The Golden Hour: Scientific Fact or Medical Urban Legend. *Academic Emergency Medicine. 8*(7), p. 758-760.

Lia, B. (2005). *Globalisation and the Future of Terrorism. Patterns and Predictions*. UK: Routledge

Lindo, S., Schoder, M. & Jones, T. (2011). *Al Qaeda in the Arabian Peninsula*. Washington DC: Centre for Strategic and International Studies, Transnational Threats Project. Retrieved 25 August 2011 from https://www.csis.org/analysis/al-qaeda-arabian-peninsula

London Assembly. (2006). *Report of the 7 July Review Committee*. UK: Greater London Authority

London Emergency Services Liaison Panel. (2015). *LESLP Major Incident Procedure Manual.* (Version 9.4). London: Metropolitan Police

Marshall, C. & Rossmann, B.R. (2016). *Designing Qualitative Research*. (6th edition). USA: Sage Publications.

Mazzetti, M. (2016, 15 July). In 9/11 Document, View of a Saudi Effort to Thwart U.S. Action on Al Qaeda. *The New York Times*. Retrieved 9 November 2016 from http://www.nytimes.com/2016/07/16/us/28-pages-saudi-arabia-september-11.html

Meld. St. nr. 21 (2012-2013). (2013). *Terrorberedskap. Oppfølging av NOU 2012:14 Rapport fra 22. juli-kommisjonen*. Oslo: Justis- og Beredskapsdepartementet.

Meld. St. nr. 29 (2011-2012). (2012). *Samfunnssikkerhet*. Oslo: Justis- og Beredskapsdepartementet.

Nafday, A.M. (2009). Strategies for Managing the Consequences of Black Swan Events. *Leadership and Management in Engineering, 9*(4), p. 191-197.

NOU 2012:14. (2012). *Rapport fra 22. juli-kommisjonen*. Oslo: Departementenes Servicesenter.

Petersen, R.E. (2004). *Continuity of Operations (COOP) in the Executive Branch: Background and Issues for Congress*. Washington DC: Congressional Research Service, Library of Congress.

Petersen, R.E. & Seifert, J.W. (2005). *Congressional Continuity of Operations (COOP): An Overview of Concepts and Challenges*. Washington DC: Congressional Research Service, Library of Congress.

Politidirektoratet. (2011). *PBS 1. Politiets beredskapssystem del 1. Retningslinjer for politiets beredskap*. Norway: Politidirektoratet.

Politidirektoratet. (2014). *Etterretningsdoktrine for politiet.* (Version 1.0). Norway: Politidirektoratet.

Quiggin, T. (2007). *Seeing the Invisible. National Security Intelligence in an Uncertain Age*. Singapore: World Scientific Publishing co.

Rabasa, A. et.al. (2009). *The Lessons of Mumbai*. California: RAND Corporation. Retrieved 5 November 2016 from www.rand.org/pubs/occasional_papers/OP249.html

Samuelsen, R.J., (2015, 21 May). Bin Laden hadde norske rapporter i bokhylla. *Aftenposten*. Retrieved 22 May 2015 from http://www.aftenposten.no/verden/Bin-Laden-hadde-norske-rapporter-i-bokhylla-39519b.html

Shpiro, S. et.al. (2011). *SAFE-COMMS: The Terrorism Crisis Communication Manual for Public Authorities*. Israel: Bar-Ilan University. Retrieved 14 March 2012 from https://faculty.biu.ac.il/~sshpiro/pdf/SAFE%20COMMS%20Manual%20final_en_0605.pdf

Smith, D. & Ackerman, S. (2016, 15th July). 9/11 report's classified "28 pages" about potential Saudi Arabia ties released. *The Guardian*. Retrieved 9th November 2016 from www.theguardian.com/us-news/2016/jul/15/911-report-saudi-arabia-28-pages-released

Taleb, N.N., Goldstein, D.G. & Spitznagel, M.W. (2009). The Six Mistakes Executives Make in Risk Management. *Harvard Business Review, 87*(10), p. 78-81.

Tangredi, S.J. (2013). *Anti-Access Warfare. Countering A2/AD Strategies*. Maryland: Naval Institute Press.

The 9/11 Commission Report (2004). *Final Report of the National Commission on Terrorist Attacks upon the United States. Authorized edition.* New York: W.W. Norton & Company

Thornberry, W. & Levy, J. (2011). *Al Qaeda in the Islamic Maghreb*. Washington DC: Centre for Strategic and International Studies, Transnational Threats Project. Retrieved 4 September 2011 from https://www.csis.org/analysis/al-qaeda-islamic-maghreb

Townsend, N et.al. (2015). *Cardiovascular disease statistics 2015*. London: British Hearth Foundation. Retrieved 17 January 2017 from https://www.bhf.org.uk/-/media/files/publications/research/bhf-cvd-statistics-2015-final.pdf

Trnka, J. & Woltjer, R. (2014). Characteristics of Command and Control in Response to Emergencies and Disasters. In Berggren, P. (ed.), Nählinder, S. (ed.) & Svensson, E. (ed.), *Assessing Command and Control Effectiveness: Dealing with a Changing World*. (p. 83-102). UK: Ashgate.

van der Veer, H. & Wiles, A. (2008) *ETSI White Paper no. 3: Achieving Techical Interoperability – the ETSI Approach*. (3rd edition) France: European Telecommunications Standards Institute. (Retrieved 20 January 2017 from https://portal.etsi.org/CTI/Downloads/ETSIApproach/IOP%20whitepaper%20Edition%203%20final.pdf)

Vassiliou, M.S., Alberts, D.S. & Agre, J.R. (2015). *C2 Re-envisioned: The Future of the Enterprise*. Florida: CRC Press.

Wright-Neville, D. (2010). *Dictionary of Terrorism*. Cornwall: MPG Books Group Limited.

Zubrzycki, W. (2013). Russian RENEGADE Aircraft Joint Initiative. In Czulda, R. & Los, R. (ed.), *NATO. Towards the Challenges of a Contemporary World*, (p. 129-140). Warsaw: University of Lodz

Abbreviations / explanations

A2/AD	Anti-access / area denial
ACCOLC	Access overload control
AO	Area of operations
AQAP	al-Qaeda in the Arabian Peninsula
AQC	al-Qaeda core (referring to the leadership / central command of al-Qaeda)
AQIM	al-Qaeda in the Islamic Maghreb (Islamic Maghreb is a reference to North Africa west of Egypt)
BTP	British Transport Police
C2	Command and control
C3	Command, control and communication
C3I	Command, control, communication and intelligence
CAP	Combat Air Patrol
COBR	Cabinet Office Briefing Rooms, also known as COBRA
COLP	City of London Police
DSB	Direktoratet for Samfunnssikkerhet og Beredskap (EN: *Norwegian Directorate for Civil Protection*)
EPA	Emergency preparedness analysis
EUROPOL	The European Police Office
FAA	Federal Aviation Administration
FDNY	The New York Fire Department
FOH	Forsvarets operative hovedkvarter (EN: *The Norwegian Military Operational Command*)
FRM	Fire-, rescue- and medical services
GCG	Gold Coordination Group
GICM	Groupe Islamique Combattant Marocain (EN: *Moroccan Islamic Combatant Group*)
HRS	Hovedredningssentralen (EN: *Joint rescue coordination centre*)
IED	Improvised explosive device
ISC	Intelligence and Security Committee
ISIS	Islamic State in Iraq and al-Sham (AR: *al-Dawlah al-Islamiyah fi ‘l-Iraq wa-sh-Sham*), also known as ISIL (Islamic State in Iraq and the Levant), IS (Islamic State) and Daesh.
KRIPOS	Kriminalpolitisentralen (EN: *National Criminal Investigative Service*)
LESLP	London Emergency Service Liaison Panel
MENA	Middle-East and North-Africa
MI5	Military Intelligence, Section 5, primarily known as The Security Service
MPS	Metropolitan Police Service, also known as “the Met”
NATO	North Atlantic Treaty Organization
NCA	National Command Authority
NCC	London Underground’s Network Control Centre (now known as Network Operations Centre)
NEADS	Northeast Air Defence Sector
NMCC	National Military Command Center
NORAD	North American Aerospace Defence Command
NYPD	The New York Police Department
PBIED	Person-borne improvised explosive device
POD	Politidirektoratet (EN: *National Police Directorate*)
PST	Politets Sikkerhetstjeneste (EN: *Norwegian Police Security Service*)
RENEGADE	A hijacked aircraft that is intended to be used as a weapon in a terroristic manner
ROE	Rules of engagement
SAR	Search and rescue
UXO/IED	Unexploded ordnance/improvised explosive device
VBIED	Vehicle-borne improvised explosive device
WTC	The World Trade Centre