18th ICCRTS

"C2 in Underdeveloped, Degraded and Denied Operational Environments"

C2 Failures: A Taxonomy and Analysis

Topics:
(1): Concepts, Theory and Policy
(2): Approaches and Organizations

Marius S. Vassiliou
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311
USA
+1-703-887-8189
+1-703-845-4385
mvassili@ida.org

David S. Alberts
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311
USA
+1-703-845-2411
dalberts@ida.org

Point of Contact:

Marius S. Vassiliou
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311
USA
+1-703-887-8189
+1-703-845-4385
mvassili@ida.org

ABSTRACT

Command and Control (C2) is a function that creates value by mobilizing available information and resources. Although 'perfect C2' is no guarantee of mission success, C2 shortfalls and failures can adversely impact the ability of organizations to accomplish their missions. We examine 20 situations, including combat operations and responses to terrorist attacks and disasters, that have been characterized as experiencing 'C2 failures' of varying degrees of severity. We develop a taxonomy that helps us better understand these failures and their mission impacts. This improved understanding can form the basis of efforts to improve C2, making such failures less likely and mitigating adverse impacts when they occur. We identify three categories of C2 failures: (1) failures attributed to *a priori* structural defects in C2 approach, or a mismatch between the C2 approach and the mission; (2) failures attributed to an inability to communicate, including a lack of access to appropriate information, individuals, or organizations; and, (3) behavioral failures to communicate or interact. Different C2 approaches, of varying degrees of decentralization, may have different failure propensities. For example, a collective that is distributed, but not properly integrated, may sometimes be more adversely affected by communication failures than a traditional hierarchy.

1. INTRODUCTION

We have studied 20 operational situations that have been characterized as experiencing one or more command and control (C2) failures of varying severity[1]. By "C2 failure," we mean an observed inability to carry out adequately the functions associated with C2. In some cases, the C2 failure(s) had an obvious detrimental effect on the mission, and in others the operational effect was more difficult to discern, or was overwhelmed by other factors. Thus, not all of the cases where C2 failures were observed also involved mission failure. In fact, in many cases, the overall mission was judged a success despite these C2 failures.

The situations under discussion and some basic data about them are listed in Table 1. Some involve military operations, including ones from the First and Second World Wars; Operation Desert Storm; the United States Iranian Hostage Rescue mission of 1980; the Russia-Georgia war of 2008; and others. Others involve the run-up, and response to, terrorist attacks such as those of September 11th, 2001. Still others revolve around the responses to major disasters, such as Hurricane Katrina, or responses to smaller emergencies, such as London's King's Cross Underground Fires of 1989. The list is by no means exhaustive, nor is it a uniform sample of all C2 failures in the past hundred years. Rather, it is an illustrative collection of notable incidents involving a recognized failure in C2.

[1] In all of the cases considered here, the literature describing what happened explicitly refers to "command and control failure."

Table 1 Situations Discussed: Basic Data

Military Operations				
Incident	**When**	**Where**	**Result**	**Notes**
Great Retreat of 1914, First World War	1914, Aug. 24-31	France	Unraveling of the British Cavalry Division	[1]
Run-up to 1st Battle of the Marne, First World War	1914, Aug. & Sep.	France	Allied Victory in the ensuing battle on 5-12 September 1914; 550,000 estimated total casualties in ensuing battle.	[2]
1st Battle of Savo Island, Guadalcanal Campaign, Second World War	1942, Aug. 8-9	Savo Island	Allied defeat; 1135 combat deaths, of which 1077 allied.	[3]
Mayaguez Incident	1975, May 12-15	Koh Tang Island, Gulf of Siam	Mission success for US after heavy fighting; c. 88 dead, 105 injured (combatants, both sides)	[4]
US Hostage Rescue Mission	1980, Apr. 24-25	Iran	Mission failure; 8 US servicemen dead.	[5]
US Invasion of Grenada	1983, Oct. 25	Grenada	Mission success for US; 89 deaths, 533 injuries (combatants, all sides).	[6]
First Gulf War, Operation Desert Storm	1991, Jan. 17 - Feb. 28	Iraq	Coalition victory; 358 coalition combat & theater deaths; c. 22,000 Iraqi military deaths.	[7]
Russia-Georgia War	2008, Aug. 7-16	Georgia, Abkhazia, South Ossetia	Russian victory; estimates of total combat deaths (all sides) vary from c.500-3200	[8]

Terrorist Attacks				
Incident	**When**	**Where**	**Result**	**Notes**
Oklahoma City Bombing	1995, Apr. 19	United States (Oklahoma)	168 deaths, 680 injuries	[9]
911 Attacks	2001, Sep. 11	United States (New York, Virginia)	2996 deaths, over 6000 est. injuries, $40B in insurance claims, unquantifiable total impacts	[10]
7/7 London Bombings	2005, Jul. 7	United Kingdom (London, England)	56 deaths, c. 700 injuries	[11]
2011 Norway Attacks	2011, Jul. 22	Norway (Oslo and Utøya Island)	77 deaths, 319 injuries.	[12]

Disasters and Emergencies				
Incident	**When**	**Where**	**Result**	**Notes**
King's Cross Underground Fire	1987, 18 Nov.	United Kingdom (London, England)	31 deaths, 100 estimated injuries.	[13]
Clapham Railway Junction Accident	1988, Dec. 12	United Kingdom (London, England)	35 deaths, 500 estimated injuries.	[14]
Hillsborough Stadium Disaster	1989, Apr. 15	United Kingdom (Sheffield, England)	96 deaths	[15]
Hurricane Andrew	1992, Aug. 24	United States (Florida)	26 direct deaths, 39 indirect.$20B estimated damages.	[16]
Columbine High School Shootings	1999, April 20	United States (Colorado)	13 deaths, 24 injuries	[17]
Indian Ocean Tsunami	2004, Dec. 26	Indonesia, India, Sri Lanka, Thailand, Maldives	227898 deaths, c. 1.7 million people displaced	[18]
Hurricane Katrina	2005, Aug. 23-30	United States (Louisiana, Mississippi, and environs)	1836 deaths, $75B damage, $110B total economic impact	[19]
Black Saturday Fires	2009, Feb. 7	Australia (Victoria)	173 deaths, $4B(Aus) in economic impact	[20]

NOTES to Table 1: [1] Gardner (2009). [2] Fuhrmann, et al. (2005); Winter (2010). [3] Frank (1990). [4] Government Accountability Office (1976). [5] Holloway (1980); Bowden (2006). [6] Cole (1997). [7] Tucker (2010). [8] Independent International Fact-Finding Mission on the Conflict in Georgia (2009). [9] Shariat, et al. (1998); Oklahoma Department of Civil Emergency Management (2003). [10] Makinen (2002). [11] Lieberman and Cheloukhine (2009). [12] Commission on 22 July (2012). [13] Fennell (1988); Croome and Jackson (1993). [14] Hidden (1989). [15] Hillsborough Independent Panel (2012). [16] Rappaport (2005). [17] U.S. Fire Administration (1999). [18] US Geological Survey (2013). [19] Knabb, et al. (2005). [20] Parliament of Victoria, 2009 Victorian Bushfires Royal Commission (2010).

2. C2 FAILURES

C2 failures manifest themselves in a limited number of ways, but the causes of these failures are more varied. Although the manifestations are readily apparent and are usually what is reported in the literature when failures are noted, the root causes of C2 failures often require some work to discern. Our attempt to categorize the incidents and situations listed in Table 1 benefited from the conceptual foundation laid by the C2 research community, specifically: the tenets of Network Centric Warfare (NCW)[2], the North Atlantic Treaty Organization (NATO) Network Enabled Capability (NEC) C2 Maturity Model[3], and the more recent work on C2 Agility[4]. The tenets of NCW consist

[2] Alberts et al. (1999)

[3] Alberts et al. (2010)

[4] Alberts (2011)

of a hypothesized value chain that begins with the degree to which a force is networked—that is, the degree to which it is able to communicate, share information, coordinate, and collaborate. The tenets move on to consider the extent to which this capability translates into actual information-related behaviors. By this, we mean the sharing of information and other information-related interactions, and the impact that such behaviors have on the quality of awareness and shared awareness. The major hypothesis contained in the NCW tenets is that, at some point, shared awareness enables synchronization, including self-synchronization, and that this results in improvements in mission effectiveness. These tenets provide one part of a framework for considering C2 failures, since what creates value should by its absence adversely impact value. Thus, the tenets provide a point of departure for classifying specific C2 failures. For example, was the failure one of a lack of shared awareness, and if so, what was its cause? Was it a technical cause, or was it rooted in individual or social behaviors?

The NCW tenets assume a certain amount of relevant intelligence information is available, and that there is a proper focus on getting the most from this information. The absence of intelligence information—an "intelligence failure"—can destroy a mission even if everything else is functioning perfectly. Intelligence failures are a subject unto themselves, and we do not consider them here.

The NATO NEC C2 Maturity Model contributes to a taxonomy of C2 failures in two ways. First, it provides a structured way to describe and characterize an observed C2 approach. Second, it allows us to categorize observed C2 approaches and determine if the approach in practice (as it was implemented) differed from the intended or doctrinal approach. C2 Agility Theory states that there is no universal C2 approach, and that the most appropriate C2 approach depends on the nature of the mission, situation, and environment. Thus, the theory suggests that an inappropriate C2 approach could be a cause of C2 failure. C2 Agility involves recognizing that one's C2 approach is inappropriate for the situation, and adopting a more appropriate one. Thus, the initial adoption of a "wrong" approach can be remedied by timely recognition and a transition to a more appropriate approach. This adds yet another category of C2 failure, namely a lack of agility. Ultimately, many C2 failures are likely involve a lack of agility, since a timely change of approach might increase the ability of the C2 enterprise to recover from technical or behavioral failures.

Figure 1 presents a taxonomy of C2 failures, informed by both C2 theory and common themes that emerged from our review of the incidents listed in Table 1.

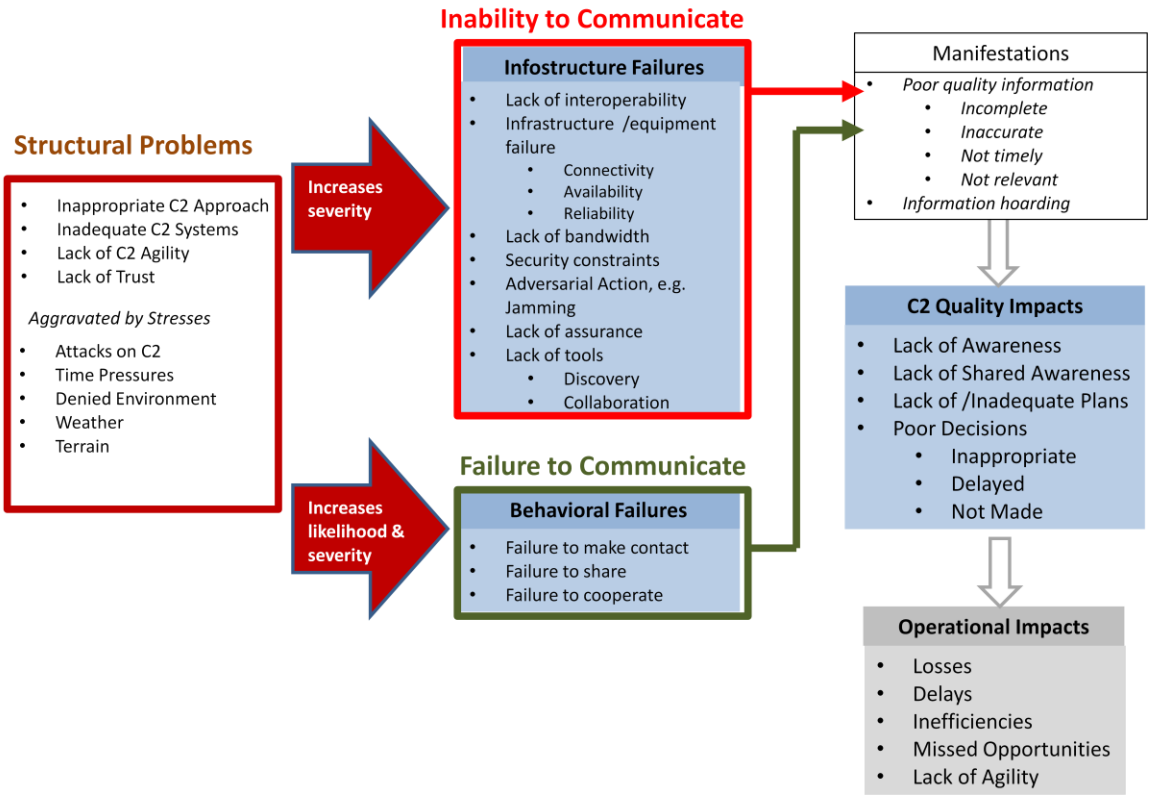

Figure 1. Causes, manifestations, and impacts of C2 failures

C2 failures generally manifest themselves as a lack of access to information or an absent, incomplete, irrelevant, delayed, or erroneous transfer of information from those who have it to those who need it. This lack of information quality may be caused by failure of the information infrastructure, or "infostructure," to satisfy the requirements of the mission or circumstances. It may also be caused by behavioral failures. These causes may in turn be a result of pre-existing or *a priori* problems, or current stresses with which individuals, organizations and/or systems cannot adequately cope. Some C2 failures can thus be traced back to poorly designed organizations, or sometimes inherently good organizational design that is mal-adapted for a particular mission or circumstance.

We make a distinction between an *inability* to communicate information and a *failure* to do so, in a timely manner, when it would have been appropriate. An *inability* to communicate information may result from infrastructure failure, equipment failure, equipment or bandwidth shortages, interoperability problems, hostile action, security constraints, or any number of reasons. A *failure* to communicate, when the means to do so are available, may result from human error, organizational silos, or mistrust. A failure to communicate may occur when the technical ability to communicate is present, but the knowledge of how to communicate is missing, sufficient incentives are not present, and/or individuals and organizations are unwilling to communicate with one another.

A lack of communication, whatever the cause, can have an adverse impact on operations, possibly resulting in mission failure. Even if the mission ultimately succeeds, C2 failure(s) may cause missed opportunities, duplication of effort, delays, and reduced

effectiveness. This can happen even if the organization design is sound and appropriate, although good organization design may make the system more resilient to communication problems. Conversely, an inappropriate organization or C2 approach does not guarantee a failure to communicate, but it makes such failures more likely. It also makes a lack of communication potentially more serious.

With this failure taxonomy in mind, we will review the C2 failures and their causes in the 20 incidents studied in this paper.

3. *A PRIORI* STRUCTURAL PROBLEMS

C2 failures often occur because of a predisposition to such failures that is inherent in the organization and the systems that support C2. This was the case for many of the situations and incidents discussed in this paper.

For example, in the run-up to the attacks of September 11th, 2001 the organizations responsible for military air defense and those responsible for the management of civil air traffic each had their own independent hierarchical structures and silos that promoted vertical communication. This lack of effective cross-coordination mechanisms resulted in sufficient delays that there was not enough time to shoot down the hijacked planes that successfully collided with the World Trade Center in New York and the Pentagon in northern Virginia.[5]

In the immediate response to the September 11th attacks, significant organizational seams between the New York Police Department (NYPD), the Fire Department of New York (FDNY), and the Port Authority Police Department (PAPD) proved problematic. These seams, exacerbated by the communications difficulties discussed below, resulted in redundant searches for civilians and other instances of inefficient resource deployment.[6]

The failed Iran Hostage rescue attempt, discussed in more detail in the sections below, involved U.S. Army Delta Force, U.S. Army Rangers, U.S. Air Force pilots, and U.S. Navy helicopter pilots, among others, in a highly complex operation. The mission was adversely impacted by an inadequate approach to C2 that suffered from compartmentalization and evidenced mutual distrust between and among these service components. There was also a lack of unified command with no single component commander to unify the Air Force airplanes and Navy helicopters, and no single ground commander to unify Delta Force and the Rangers.[7] These seams, combined with the communications problems described in Section 5 and a good bit of bad luck, led to mission failure and eight dead U.S. servicemen.

Similarly, the U.S. service components involved in the *Mayaguez* response of 1976 were not organized to form a fully cohesive task force. The planning process was disjointed,

[5] Grant (2006)

[6] National Commission on Terrorist Attacks Upon the United States (2004)

[7] Anno and Einspahr (1988); Gass (1992); Holloway (1980); Thomas (1987)

as described in Section 4, and there was insufficient unity of effort between the U.S. Marines, Air Force, and Navy.[8] There were also shortages of communication equipment on the ground, as discussed in Section 5. On top of all this, there was unfortunate micromanagement and interference from the upper echelons in Washington, District of Columbia. At one point in the heat of battle, Marines had to respond to an information request from Washington: did they have a Khmer interpreter with them?[9] Although the United States achieved victory in the Battle of Koh Tang and recovered the *Mayaguez* and ultimately its crew, the fighting was very difficult and the margin of victory was small. C2 problems were ultimately overcome by initiative and heroism.[10]

The Russian armed forces, although they won their war with Georgia fairly quickly in 2008, arguably had too difficult a time doing so, and suffered too many casualties. C2 failures involving coordination and communication were part of the problem, as discussed in Sections 4 and 5. Here we observe that the Russian military was organized along Cold War and even World War II principles, for large fights involving massive armies. There was little overall coordination between the Army, Air Force and Navy suitable for joint prosecution of a relatively small operation. One retired general argued that the subordination of Army aviation to the Russian Air Force (*Voyenno-Vozdushnyye Sily*—VVS) was at the core of the failures to provide close air support to ground combat forces, and called for the return of such tactical aviation to the control of Army ground units.[11] It is worth noting that the Georgia war served as a stimulus for reform of the Russian military, away from its Soviet legacy and towards better performance in smaller, faster operations.[12]

The "Great Retreat" of the British forces in 1914, in the face of an initial German offensive, offers another example of an inappropriate approach to C2. The heads of cavalry brigades were used to taking initiative and not being micromanaged. This served the British well in the various "small wars" of the world-spanning empire, but created problems in the huge conflict that was the First World War. Thus, while retreating cavalry brigades had difficulties in communicating with General Allenby at his headquarters, this was not the only cause of the communication deficit, since they were not terribly inclined to communicate in the first place. As the brigades retreated, they completely lost touch with each other and headquarters, and the British Cavalry effectively disintegrated as a viable unit for a time. This had significant adverse consequences on the ability to accomplish the mission. In the battle of Le Cateau on 26 August, Allenby was unable to offer any assistance to the Second Army Corps—his brigades were effectively gone.

During Operation Desert Storm, there was a lack of coordination between the U.S. Army and the U.S. Air Force over the crucial placement of the Fire Service Control Line

[8] Toal (1998)
[9] Toal (1998)
[10] Toal (1998)
[11] McDermott (2009)
[12] Cohen and Hamilton (2011)

(FSCL).[13] The FSCL is the boundary within which all air strikes must be coordinated with ground commanders to avoid fratricide, and outside of which air strikes are more freely conducted. The Army tended to want to position the line relatively far out, to give themselves more room to operate. The problem was that if the Army did not move fast enough to justify such a placement, the line was typically not re-positioned. This hampered the Air Force from pursuing fleeing enemy forces, and served to shield significant portions of the Iraqi Army. As one observer put it, "the safest place for an Iraqi to be was just behind the FSCL."[14]

Turning now to disaster response, organizational deficits have been a persistent problem in responses to major disasters.[15] In the response to the Indian Ocean Tsunami of 2004, there were militaries from 11 countries involved. Each had a somewhat different relationship with the Indonesian Government. A case study undertaken in support of NATO SAS-065 noted many examples of a lack of shared intent.[16] There was a lack of coordination between the various military establishments involved, between military establishments and international non-governmental organizations (NGOs), between international NGOs and Indonesian NGOs, and between U.S. and United Nations (UN) agencies. A Humanitarian Information Center was established in an effort to provide some oversight for hundreds of NGOs. Their daily meetings were characterized as being "unwieldy" and as "a shambles."[17]

In the response to Hurricane Katrina, the roles of various U.S. federal agencies were not properly delineated. There was overlap and conflict among them, and between them and the states of Louisiana and Mississippi, as well as local agencies and other actors.[18] As an example, both local police and the National Guard were working at the Louisiana Superdome, which served as an evacuation center, but each side said the other was supposed to lead. This led to security problems, and many responders left.[19] The House of Representatives report on Katrina[20] specifically mentions structural *a priori* coordination deficits between the Department of Defense (DoD) and the Federal Emergency Management Agency (FEMA), and between both of them and the State of Louisiana. Similar observations about the lack of proper role delineation and interagency coordination can be found in the reports on the responses to other disasters and emergencies. During Australia's Black Saturday fires of 2009[21], the State of Victoria's Country Fire Authority (CFA) and Department of Sustainability and the Environment (DSE) reportedly followed distinct and inconsistent operating procedures. In the response

[13] McDaniel (2001)
[14] McDaniel (2001)
[15] Donahue and Tuohy (2006)
[16] Huber, et al. (2008)
[17] Huber, et al. (2008)
[18] Moynihan (2006); U.S. House of Representatives (2006); U.S. Senate (2006)
[19] Moynihan (2006)
[20] U.S. House of Representatives (2006)
[21] Parliament of Victoria, 2009 Victorian Bushfires Royal Commission (2010)

to London's King's Cross Underground fire in 1987[22], there was poor coordination between the London Underground and police and fire agencies.

It is worth noting that even relatively decentralized and supposedly "nimble" organizations, such as terrorist groups, are not always immune to organizational seams and structural problems. A study of the decline of Al-Qaeda in Iraq recounts that cells often became bureaucratic and compartmentalized, with a Military Officer, Security Officer, *Sharia* Officer, and Administrative Officer. One individual was quoted as saying that "there is little cooperation between the four elements."[23]

In many observations of the situations and incidents discussed in this paper, there is a recurring refrain that "no one was in charge." Table 2 compiles many quotes to this effect. To see them all in one place is quite striking. However, we must note that, in complex endeavors, there may indeed *be* no one in charge. It may not be necessary or desirable to have a single organization "in charge,"[24] as long as the effort is properly coordinated, participants understand their roles and possess sufficient shared awareness, and communication channels are available if required.

Table 2. "No One in Charge"

Incident	Quote	Reference
Black Saturday Fires Response	"...roles of the most senior personnel were not clear, […] no single agency or individual in charge…"	Parliament of Victoria, 2009 Victorian Bushfires Royal Commission (2010), p.8
Hurricane Andrew Response	"...failure to have a single person in charge with a clear chain of command."	Florida Governor's Disaster Planning and Response Review Committee (1992), p. 60
9/11 Attacks	"...no one was firmly in charge of managing the case...Responsibility and accountability were diffuse." [about intelligence]	National Commission on Terrorist Attacks upon the United States (2004), p.400
King's Cross Fire Response	"...uncertainty over which of the London Underground staff was in charge…"	Fennell (1988), pp. 73-74
Iran Hostage Rescue	"…confusion about 'who was in charge'"	Anno & Einspahr (1988), p.10
	"…uncertainty as to who was in charge."	Thomas(1987) p.10
	"…no one..who was in overall charge…"	Gass (1992), p.15
	"...no way to quickly find out or locate who was in charge…"	Holloway (1980), p. 51
Mayaguez Incident Response	"[planning activity] lacked coordination…No one seemed to be in charge."	Toal (1998), p.18
Hurricane Katrina Response	"...no single individual who took charge…"; "State officials and FEMA disagreed about who was in charge…"	Moynihan (2006), pp. 22,24
	"Too often, because everybody was in charge, nobody was in charge."; "…no consensus on who was in charge."; "... disagreed on who was in charge,could not find out who was in charge, or did not know who was in charge…"	U.S. House of Representatives (2006), pp. xi, 185, 186
Indian Ocean Tsunami Response	"...coordinating meetings were 'very unwieldy' and 'internal coordinating meetings were a shambles.'"	Huber et al. (2008), p.4
Columbine High School Shootings	"…'Who's in Charge?' No one could answer the question."	Moody (2010), p.39

[22] Fennell (1988)

[23] Fishman (2009)

[24] Alberts et al. (2010)

4. BEHAVIORAL FAILURES: FAILURE TO COMMUNICATE

Many problems in C2 arise from a failure to access available information, or to communicate necessary information to those who need it. We are not speaking here of an *inability* to communicate, as in Section 5 below. The *means* to communicate may exist, but communication does not take place for any number of reasons, including a lack of *will* or *incentives*. In this section we consider communication deficits caused by any number of organizational problems, such as poorly delineated roles and responsibilities, bureaucratic silos that ignore or even mistrust each other, or simple human error. The types of *a priori* structural problems discussed in Section 3 above do not guarantee failures of communication, but they create the conditions making such failures more likely, particularly under the stress of a battle or a disaster response.

An example of a failure to communicate occurred during the Guadalcanal campaign of late 1942, during the Second World War. The Guadalcanal campaign is generally credited as a success for the Allied powers, although it involved some significant losses in individual battles, and the Allies did not achieve full dominance in the regional waters around Guadalcanal. One of the battles in the campaign that the Allies lost outright was the Battle of Savo Island on 8 August, 1942. The communication failure occurred in the cruiser groups constituting the Allied screening force guarding against a Japanese naval attack.[25] On the night of the battle, the commander of the screening force, Rear Admiral Victor Alexander Charles Crutchley, took his ship out of the southern cruiser group in order to attend a conference with Admiral Richard Turner. However, he did not inform his second in command, Captain Frederick Riefkohl, who was in the northern cruiser group. Riefkohl remained ignorant that he was now in command of the screening force. When the Japanese attacked, there was no coordinated response. Moreover, a crucial radio message warning of an impending attack was not relayed to Riefkohl, because of human error. These C2 failures were not the only causes of the loss of the Battle of Savo Island, but they certainly adversely impacted the mission.

Another example of a C2 failure not caused by technical means can be found in the planning of the U.S. response to the capture of the *Mayaguez*. Planning cells were physically separated from each other and did not exchange much information. Many staff members were also absent. As a result, there was not a unified and coordinated plan, and many participants remained unaware of whatever plans there were.[26]

Responses to natural disasters have been rife with failures to communicate. Consider Hurricane Katrina. Moynihan[27] gives many examples, but here we will recount only two for the sake of illustration. The Louisiana Superdome football stadium served as a collection center for people who would later be further evacuated. FEMA had an evacuation plan and was more or less ready to execute. The commander of Joint Task

[25] Hone (2006)
[26] Toal (1998)
[27] Moynihan (2006)

Force Katrina, General Russel L. Honoré, told the National Guard to cancel the plans—but he did not inform FEMA. This delayed the evacuation by at least a day. In another example, New Orleans mayor Ray Nagin declared the Ernest N. Morial Convention Center as a refuge, but did not broadly communicate this decision. FEMA and the Department of Homeland Security (DHS) did not realize until two days later, when about 19,000 people were stranded at the convention center without supplies.

Similar failures have also occurred in the responses to lesser emergencies. In the 1989 Hillsborough Stadium incident, "communications between all emergency services were imprecise and inappropriately worded, leading to delay, misunderstanding, and a failure to deploy officers to take control and coordinate emergency response."[28] After the Oslo bombing of 2011 but before the mass shootings on the same day, a citizen gave police a description of the likely perpetrator, as well as his vehicle license number. The officers did not pass the information up the command chain for at least 20 minutes, and it did not reach the right people for two hours, by which time the shootings on Utøya Island had already begun.[29]

5. INFOSTRUCTURE FAILURES: INABILITY TO COMMUNICATE

There are many cases where it is simply not possible to access or share information, or for two or more entities to coordinate. An inability to communicate may result from many causes. Communication may be physically impossible with current technology or the systems available. Even if communication is theoretically possible from a technical point of view, there may be:

- a failure of infrastructure or equipment, or a shortage of appropriate equipment, leading to problems of availability, connectivity, or reliability
- a shortage of bandwidth
- adversarial action, such as jamming
- security procedures and constraints
- a lack of interoperability

The problems above have occurred with regularity in the situations examined here.

5.1 Failure of infrastructure

Infrastructure failure is a common and serious problem during major disasters.[30] The disaster that creates the conditions demanding a response also destroys or incapacitates the communications infrastructure. This happened during Hurricane Andrew,[31] Hurricane Katrina,[32] and the Indian Ocean Tsunami.[33] Even if not substantially destroyed, infrastructure may be overwhelmed by the communication demands imposed

[28] Hillsborough Independent Panel (2012)
[29] Dennis (2012)
[30] Donahue and Tuohy (2006)
[31] Florida Governor's Disaster Planning and Response Review Committee (1992)
[32] Moynihan (2006); U.S. House of Representatives (2006); U.S. Senate (2006)
[33] Huber et al. (2008)

by the response to the emergency. This was a factor in the responses to the September 11th attacks[34] and Australia's Black Saturday fires,[35] as well as the responses to the Oklahoma City bombing[36] and the Hillsborough Stadium disaster.[37]

5.2 Shortage of appropriate equipment or bandwidth

In almost all the incidents considered here, there was a shortage of appropriate communications equipment or bandwidth. The following are some examples.

During Russia's 2008 war with Georgia, the Russian forces did not have enough communications equipment, and what they did have was antiquated and often not interoperable (see section 5.3). Commanders ended up relying on personal mobile phones for C2. Worse yet, the calls had to go through the enemy's infrastructure, as the South Ossetian cellular networks were run by Georgia. In one instance, the 58th Army Commander, Lieutenant Anatoliy Khrulev, reportedly had to borrow a satellite telephone from a journalist in order to communicate with his forces.[38]

During the British "Great Retreat" of 1914 in the beginning of the First World War, communications collapsed completely as cavalry brigades separated from each other. Communications depended greatly on motor vehicles, and the roads of northern France had become so clogged as to be almost impassable.[39]

In another example from the early stages of the First World War, the German offensive of 1914 was hampered severely by coordination failures resulting from an inability to communicate.[40] The Germans depended on cars and motorcycles to pass messages, and also on wireless communications for distances up to about 130 miles. The presence of a French jamming station on top of the Eiffel Tower severely limited the effectiveness of wireless communications. Messages often had to be repeated several times. This, along with security procedures of encoding and decoding, meant that it often took 12 hours and sometimes longer to successfully pass a wireless message. As German armies in the west spread over hundreds of miles, and as commanders made field decisions that resulted in deviations from the original Schlieffen plan, a coordination problem was produced that could not be solved with the slow and unreliable communications available. This contributed to the German defeat in the First Battle of the Marne, which in turn dashed German hopes for a quick victory and also signaled the end of mobile conflict and the beginning of bloody trench warfare.

---

[34] National Commission on Terrorist Attacks Upon the United States (2004)
[35] Parliament of Victoria, 2009 Victorian Bushfires Royal Commission (2010)
[36] Oklahoma Department of Civil Emergency Management (2003)
[37] Hillsborough Independent Panel (2012)
[38] McDermott (2009)
[39] Gardner (2009)
[40] Fuhrmann et al. (2005)

In the *Mayaguez* incident of 1976, a serious communications problem was precipitated by the destruction of Ultra-High-Frequency (UHF) radios in a helicopter crash. The remaining Very-High-Frequency (VHF) radios were overloaded, making communication between aircraft and Marines on the ground very difficult. This resulted in crucial problems coordinating air strikes.[41]

In the 1983 U.S. Invasion of Grenada, besides the interoperability problems discussed in the Section 5.3, there was also a shortage of satellite communications.[42]

During the response to the September 11th attacks, FDNY radios performed very badly inside buildings. A repeater system that had been set up to solve such problems was not properly activated because of human error. A shortage of bandwidth also plagued both the NYPD and FDNY.[43] In an earlier instance of radios having problems working indoors, responders to the King's Cross Underground Fire in London had severe difficulties with radio communication underground.[44] In the response to Hurricane Andrew, there was a severe shortage of High-Frequency (HF) radios.[45]

5.3 Interoperability

Communications equipment is of little use if it cannot talk to other communications equipment. A lack of interoperability between communications equipment or information technology systems was a common problem in many of the situations studied. During the failed Iran hostage rescue attempt, for example, various operational units could not talk to each other. The Army Rangers who were guarding the landing site in the Iranian desert used radios that could not communicate with Delta Force or Air Force personnel. They were also unable to inform ground commanders in a timely fashion when a bus full of Iranian civilians appeared, complicating the operation. The landing site could also not talk to the helicopter fleet.[46] These interoperability failings, coupled with the communications security constraints imposed on the mission and discussed in Section 5.4, certainly contributed to the failure of the mission.

Another U.S. military example is the successful invasion of Grenada in 1983. During this invasion, Marines in the north and Army Rangers in the south used their radios in such a way that interoperability was impeded, and they could not talk to each other. When the Marines ran into trouble at one point, the Rangers did not know about it for an unacceptably long time. Interoperability problems also led to a highly publicized incident in which a soldier had to call for air support by placing a commercial long distance telephone call from Grenada to Fort Bragg, North Carolina.[47]

---

[41] Toal (1998)
[42] Anno and Einspahr (1988)
[43] National Commission on Terrorist Attacks Upon the United States (2004)
[44] Fennell (1988)
[45] Florida Governor's Disaster Planning and Response Review Committee (1992)
[46] Anno and Einspahr (1988)
[47] Anno and Einspahr (1988)

Interoperability problems plagued the Russians during their war with Georgia in 2008. Ground units were unable to communicate with space-based and electronic intelligence assets. As a result, the Russians could not employ their electronic warfare systems to full advantage to suppress Georgian air defenses, and could not make full and effective use of satellite targeting support or precision guided munitions. There were also interoperability problems between the units of different services of the Russian armed forces. Ground commanders had very little control over needed air support. Reportedly, Colonel General Aleksandr Zelin directed air operations personally by mobile phone from Moscow.[48]

In the run-up to the September 11th, 2001 terrorist attacks, there was no interoperability between the information technology and C2 systems of the Federal Aviation Administration (FAA) and the North American Aerospace Defense Command (NORAD).[49] In the immediate aftermath of the attacks, units of first responders on the ground often found that they were unable to communicate with each other. For example, the Port Authority Police Department had radios that could not talk to those of the FDNY.[50]

In responses to major disasters and other emergencies, interoperability problems occur with depressing regularity. They are identified in carefully researched official after-action reports, only to occur again in future incidents.[51] In the aftermath of Hurricane Katrina, the U.S. Department of Defense did not have an information sharing protocol that might have enhanced communication and situational awareness between all the deployed military units. There were also major interoperability problems in communication between units of different federal, state, and local agencies on the ground. Joint Task Force Katrina, the National Guard, and the States of Louisiana and Mississippi did not have interoperable communications equipment.[52] Similar problems occurred in other disasters. During Australia's Black Saturday fires of 2009, the metropolitan and regional police forces had incompatible radio systems, and there was no interoperability between different emergency services agencies.[53] In the response to the 1987 King's Cross Underground fire in London, there was also no interoperability between the different emergency agencies, and between them and the London Underground. Despite being identified as a problem in the Fennell Report of 1988,[54] such difficulties recurred at least partially in the response to the 2005 "7/7" London bombings.[55]

[48] McDermott (1990)
[49] Grant (2006)
[50] National Commission on Terrorist Attacks Upon the United States (2004)
[51] Donahue and Tuohy (2006)
[52] U.S. House of Representatives (2006); U.S. Senate (2006)
[53] Parliament of Victoria, 2009 Victorian Bushfires Royal Commission (2010); Au (2011)
[54] Fennell (1988)
[55] Guardian (2011)

A study of 192 U.S. cities published in 2004[56] reported that 86% of them did not have interoperable communications with their state transportation department; 83% were not interoperable with the U.S. Department of Justice or the Department of Homeland Security; 60% were not interoperable with their state emergency operation centers, and 49% lacked interoperability with state police.

5.4 Security Constraints

During military operations, there is an ever-present tension between the need to communicate information and the need for security and stealth. The proper balance is often very hard to reach. Sometimes, security procedures may restrict information availability to the point that the mission is harmed. This happened during the failed 1980 U.S. attempt to rescue the hostages being held at the U.S. Embassy in Iran. The security constraints further exacerbated a situation that was already plagued with structural organizational problems and communications interoperability issues, as discussed above.

A C-130 transport airplane heading to the rendezvous landing site ("Desert One") encountered a large desert dust cloud (known in Iran as a *haboob*). The *haboob* was not a major problem for the airplane, but it was potentially a serious threat to the eight helicopters following far behind it. The airplane did not warn the helicopters because of a strict dictate of radio silence. There was a chance the aircrew could have used a secure satellite radio to issue the warning, but unfamiliarity with the equipment made them unable to work out the coding parameters.[57]

The helicopters thus entered the *haboob*. Because of radio silence, they could not tell each other what they were doing or where they were going. One helicopter had to abort because of a suspected blade failure, and two others left the *haboob* and landed. One of the two that landed prematurely was that of the group's leader. The leader made a secure call to a U.S. command center in Egypt and was told to proceed to the rendezvous landing site ("Desert One"), but none of the other helicopters could hear the conversation. The other pilot that had landed prematurely was no longer in visual contact. Because of readings indicating malfunctions and the difficulty of flying again through the *haboob*, he made an independent decision to return to the aircraft carrier *Nimitz*. To make things worse, his was the helicopter carrying all the spare parts needed for possible repairs. None of the helicopters could talk directly to Desert One and thereby learn that the rendezvous landing site was clear. Later, the pilot who returned said he would have continued had he known that fact.[58] The inability to communicate led to the loss of needed helicopters and crucial spare parts at Desert One. This contributed in no small measure to the ultimate failure of the mission.

[56] U.S. Conference of Mayors (2004)

[57] Anno and Einspahr (1988); Bowden (2006)

[58] Anno and Einspahr (1988)

6. DISCUSSION

Table 3 summarizes the factors discussed above for the 20 incidents in Table 1. A glance at the table reveals that an *a priori* structural defect (organizational or systems) was a problem in almost all the cases, and that this led to a failure to communicate in most cases. Interoperability problems were a specific factor less frequently, but were serious when they occurred. The inability to communicate because of security constraints was not particularly prevalent in the situations studied, but was disastrous in one case, the failed 1980 US attempt to rescue the hostages in Iran.

Another pattern that emerges in Table 3 is that responses to major disasters such as Hurricane Katrina have been plagued across the board by all the problems identified here. The nearly total chaos produced by such disasters stretches all systems and organizations to the breaking point.

Table 3. Situations Discussed: C2 Characterization

(Shaded box means heading is applicable to incident)

Military Operations

			Inability to Communicate				
Incident	**Structural Problems**	**Failure to Communicate**	Lack of Interoperability	Infrastructure/Equipment Failure	Equipment or Bandwidth Shortage	Security Constraints	Notes
Great Retreat of 1914, First World War	■	■			■		[1]
German army in runup to 1st Battle of the Marne, First World War	■	■			■		[2]
1st Battle of Savo Island, Guadalcanal Campaign, Second World War	■	■					[3]
Mayaguez Incident	■	■			■		[4]
US Hostage Rescue Mission	■	■	■	■	■	■	[5]
US Invasion of Grenada			■		■		[6]
First Gulf War, Operation Desert Storm, FSCL	■						[7]
Russia-Georgia War	■		■		■		[8]

Table 3 Situations Discussed: C2 Characterization (cont.)

(Shaded box means heading is applicable to incident)

Terrorist Attacks

			Inability to Communicate				
Incident	**Structural Problems**	**Failure to Communicate**	Lack of Interoperability	Infrastructure/Equipment Failure	Equipment or Bandwidth Shortage	Security Constraints	Notes
Oklahoma City Bombing Response	■		■		■		[9]
911 Attacks Response and Possible Prevention	■	■	■	■	■	■	[10]
7/7 London Bombings Response			■	■	■		[11]
2011 Norway Attacks Response	■	■					[12]

Table 3 Situations Discussed: C2 Characterization (cont.)

(Shaded box means heading is applicable to incident)

Disasters and Emergencies

			Inability to Communicate				
Incident	**Structural Problems**	**Failure to Communicate**	Lack of Interoperability	Infrastructure/Equipment Failure	Equipment or Bandwidth Shortage	Security Constraints	Notes
King's Cross Underground Fires Response	■	■	■	■	■		[13]
Clapham Railway Junction Accident Response	■	■		■	■		[14]
Hillsborough Stadium Disaster Response	■	■		■			[15]
Hurricane Andrew Respnse	■	■	■	■	■		[16]
Columbine High School Shootings Response	■		■				[17]
Indian Ocean Tsunami Response	■	■	■	■	■		[18]
Hurricane Katrina Response	■	■	■	■	■		[19]
Black Saturday Fires Response	■	■	■	■	■		[20]

NOTES to Table 3: [1] Gardner (2009). [2] Fuhrmann et al. (2005). [3] Hone (2006). [4] Toal (1998); Government Accountability Office (1976). [5] Anno and Einspahr (1988); Holloway (1980); Bowden (2006); Gass (1992); Thomas (1987). [6] Anno and Einspahr (1988); Cole (1997). [7] Tucker (2010). [8] Cohen and Hamilton (2011); McDermott

(2009); Independent International Fact-Finding Mission on the Conflict in Georgia (2009). [9] Oklahoma Department of Civil Emergency Management (2003). [10] Grant (2006); National Commission on Terrorist Attacks upon the United States (2004). [11] Guardian (2011); Lieberman and Cheloukhine (2009). [12] Commission on 22 July (2012); Dennis (2012). [13] Fennell (1988). [14] Hidden (1989). [15] Hillsborough Independent Panel (2012). [16] Florida Governor's Disaster Planning and Response Review Committee (1992). [17] U.S. Fire Administration (1999). [18] Huber, et al. (2008). [19] Moynihan (2006); U.S. House of Representatives (2006); U.S. Senate (2006). [20] Parliament of Victoria, 2009 Victorian Bushfires Royal Commission (2010); Au (2011).

The hypothesis being examined by NATO SAS[59]-085, that more network-enabled C2 approaches are more agile, implies that C2 approaches of varying degrees of decentralization may have different susceptibilities to the sources of failure outlined above. For example, an organization that is distributed in nature, but not properly networked, may be more prone to communication failures than more centralized approaches. Consider the case of the German advance of 1914. The Germans followed the doctrine of *auftragstaktik*, or mission command, that allowed considerable individual initiative to field commanders whose abilities and extensive training were presumed to imbue them with the proper level of shared intent. Mission command[60] worked well for the Germans in the Austro-Prussian War of 1866 and the Franco-Prussian War of 1870-71.[61] However, those wars involved smaller armies and much smaller fronts, which were easier to handle with more rudimentary communications capability. In the offensive of 1914, the deviations from the original offensive Schlieffen Plan, caused at least in part by field commanders taking initiative and responding to unfolding tactical conditions[62], created a need for command, control, and communications technological capability that simply did not exist in 1914 to coordinate the movements of huge armies. The field commanders were taking actions without full knowledge of what other commanders were doing (they lacked shared awareness), without the immediate knowledge of headquarters (they lacked awareness), and—crucially—without vital information that was often known to headquarters and other commanders (a lack of shared information). This ultimately resulted in the failure of the offensive because the conditions necessary for successful mission command were not established.

A different effect can be discerned in the run-up to the attacks of September 11th, 2001. A hierarchical structure with vertical communications channels did not function effectively in the face of an unanticipated threat unfolding with great rapidity. Thus failures to communicate can be present in any form of organization, and have deleterious effects.

The Russian armed forces were stymied in their nonetheless successful war with Georgia in 2008 by a highly hierarchical and disjointed Soviet-legacy organization. However, given the communications difficulties from which they suffered, it is not clear that a more decentralized approach would have served them better. Arguably, a more decentralized

[59] System Analysis and Studies, a panel of the North Atlantic Treaty Organization's Science and Technology Organization

[60] This differs in important ways from the way the term "mission command" is used in a recent white paper of the same name issued by US Chairman of the Joint Chiefs of Staff [Dempsey (2012)].

[61] Fuhrmann, et al. (2005)

[62] For example, General von Kluck's turn to the Southeast away from Paris on 31 August 1914, and Prince Rupprecht of Bavaria's counterattack in Lorraine on 8 August. See Fuhrmann, et al. (2005)

and net-centric approach would have required better communications equipment with much more interoperability in order to function effectively.

7. CONCLUDING REMARKS

We have studied 20 operational situations that have been characterized as having command and control (C2) failures of varying severity. Some have involved military operations; some the run-up, and response to, terrorist attacks; and others involved the responses to major disasters or smaller emergencies. In some cases, the C2 failure had an obvious detrimental effect on the mission, and in others the effect was more difficult to discern, or was overwhelmed by other factors. While these failures all involved information that was not communicated, the key to avoiding such C2 failures or reducing their adverse impacts lies in the *reasons* behind the lack of information transfer or lack of shared information. The lack in all cases was caused either by a behavioral failure to communicate, or a physical or technical inability to do so. In most cases, there were *a priori* structural and organizational problems resulting in a reduced propensity to communicate in the first place.

The inability to communicate is addressable with continuing investments in Research, Development, Technology, and Engineering (RDT&E) in information and communications science and technology (ICT), as well as smart and effective acquisition policies for communications equipment and ICT. The behavioral failures to communicate are addressable with training, doctrine, and proper organization design, as well as agile C2 approaches.

The role played by flawed or inappropriate organization in these incidents is too pervasive to ignore. As we have seen in our discussion of the various examples, different C2 approaches, of varying degrees of decentralization, may have different failure propensities under different circumstances. For example, a collective that is distributed, but not properly integrated, may sometimes be more adversely affected by communication failures than a traditional, tightly-knit hierarchy. The relatively decentralized mission-command paradigm of the German Army at the beginning of World War I, discussed above, represents a case in point.

If the collection of participating organizations—or units of the same organization—were able to adopt an appropriate approach to C2, it seems likely that the frequency of these failures would have been significantly reduced or their impacts mitigated. Many of the disaster-response cases discussed in this paper were characterized by chaotic conditions, with no one knowing "who was in charge." However, it may not always be necessary or desirable to have a single organization "in charge" of a complex endeavor, as long as the effort is properly coordinated, participants understand their roles and possess sufficient shared awareness, and communication channels are available if required.

With a better understanding of the C2 approach options that are available and the need of an organization (or collection of organizations) to be able to adopt more than one approach to C2, the capabilities of the systems that support C2 can be expected to evolve

over time. Specifically, these systems can be expected to be designed to support not one, but a variety of C2 approaches and, as a result, will themselves be better able to cope with unexpected communications and interoperability challenges as well as mission stresses. This should lead to even fewer C2 failures.

Acknowledgements

This work was performed under Institute for Defense Analyses Contract No. DASW01-04-C-0003, task order AK-2-2701. We thank David Jakubek for helpful discussions. We also thank the paper's reviewers for their valuable suggestions.

Disclaimer

The views expressed are those of the authors and do not reflect the official policy or position of the Department of Defense or the United States Government.

REFERENCES

Alberts, David S. (2011). *The Agility Advantage*. Washington, D.C.: United States Department of Defense, Command and Control Research Program (CCRP Press), 615pp.

Alberts, David S., John J. Garstka, and Frederick P. Stein (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, D.C.: United States Department of Defense, Command and Control Research Program (CCRP Press), 284pp.

Alberts, David S., Reiner K. Huber, and James Moffat (2010). *NATO NEC C2 Maturity Model*. Washington, D.C.: United States Department of Defense, Command and Control Research Program (CCRP Press), 365pp.

Anno, Stephen E., and William E. Einspahr (1988). *Command and Control and Communications Lessons Learned: Iranian Rescue, Falklands Conflict, Grenada Invasion, Libya Raid*. Air War College Research Report No. AU-AWC-88-043. Maxwell Air Force Base, Alabama: Air War College.
http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA202091

Au, Andrew (2011). "Analysis of command and control networks on Black Saturday." *Australian Journal of Emergency Management* Volume 26, No. 3, pp. 20-29.

Bowden, Mark (2006). *The Desert One Debacle*. *The Atlantic Monthly*, May, 2006, pp. 62-77.

Cohen, Ariel, and Robert E. Hamilton (2011). The Russian Military and the Georgia War: Lessons and Implications. Carlisle, PA: Strategic Studies Institute, United States Army War College.
http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1069.pdf

Cole, Ronald H. (1997). *Operation Urgent Fury: The Planning and Execution of Joint Operations in Grenada, 12 October - 2 November 1983*. Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff.

Commission on 22 July (2012). *Norwegian Government Investigation 2012:14, Report of the Commission on 22 July: Preliminary English Version of Selected Chapters*. [Original: *Norges Offentlige Utredninger 2012:14, Rapport fra 22.juli kommisjonen*]. Oslo, Norway: Government of Norway, Commission on 22 July.

Croome, Desmond F.; Jackson, Alan Arthur (1993). *Rails Through the Clay: A History of London's Tube Railways*. Capital Transport.

Dennis, Steve (2012). "Independent Inquiry into Norway Killings Reveals Significant Failings by Police." London: Desroches Group. Online.
http://www.desrochesgroup.com/investigation-academy-articles/department-of-serious-crime-articles/independent-inquiry-into-norway-killings-reveals-significant-failings-by-police/

Dempsey, Martin (2012). *Mission Command White Paper*. Washington, D.C.: U.S. Department of Defense, Office of the Chairman of the Joint Chiefs of Staff.
http://www.jcs.mil/content/files/2012-04/042312114128_CJCS_Mission_Command_White_Paper_2012_a.pdf

Donahue, Amy K., and Robert V. Tuohy (2006). "Lessons We Don't Learn: A Study of the Lessons of Disasters, Why We Repeat Them, and How We Can Learn Them." *Homeland Security Affairs*, Vol. II, No. 2.

Fennell, Desmond (1988). *Investigation into the King's Cross Underground Fire*. London: Her Majesty's Stationery Office.
http://www.railwaysarchive.co.uk/documents/DoT_KX1987.pdf

Fishman, Brian (2009). *Dysfunction and Decline: Lessons Learned from Inside Al Qa'ida in Iraq*. West Point, New York: Combating Terrorism Center.
http://www.ctc.usma.edu/wp-content/uploads/2010/06/Dysfunction-and-Decline.pdf

Florida Governor's Disaster Planning and Response Review Committee (1992). *Final Report*. ("The Lewis Report" on the response to Hurricane Andrew). Collingdale, Pennsylvania: Diane Publishing Company.
http://www.floridadisaster.org/documents/Lewis%20Report%201992.pdf

Frank, Richard B. (1990). *Guadalcanal: The Definitive Account of the Landmark Battle*. New York: Penguin Group.

Fuhrmann, Matthew C., Nathan D. Edwards, and Michael D. Salomone (2005). "The German Offensive of 1914: A New Perspective." *Defense & Security Analysis* Vol. 21, No. 1, pp. 37–66.

Gardner, Nicholas (2009). "Command and Control in the "Great Retreat" of 1914: The Disintegration of the British Cavalry Division." *Journal of Military History* Vol. 63 No. 1, pp. 29-54

Gass, Gregory P. (1992). *Command and Control: The Achilles Heel of the Iran Hostage Rescue Mission*. Newport, Rhode Island: Naval War College.
http://www.dtic.mil/dtic/tr/fulltext/u2/a249903.pdf

Government Accountability Office (1976). The Seizure of the Mayaguez: A Case Study of Crisis Management. Report B-133001. Washington, D.C.: Government Accountability Office [then called General Accounting Office].
http://www.gao.gov/assets/240/233910.pdf

Grant, Tim (2006). "Measuring the Potential Benefits of NCW: 9/11 as case study." *Proc. 11th International Command and Control Research and Technology Symposium*, Cambridge, England, Sept. 26-28. Washington, D.C.: United States Department of Defense, Command and Control Research Program.
http://www.dodccrp.org/events/11th_ICCRTS/html/papers/103.pdf

Guardian [Newspaper] (2011). "7/7 rescue operation hampered by poor radio communications, inquest hears." The Guardian, Feb. 8 2011, Online.
http://www.guardian.co.uk/uk/2011/feb/08/7july-inquest-rescue-operation-radio-communication

Hidden, Andrew (1989). *Investigation into the Clapham Junction Railway Accident*. London: Her Majesty's Stationery Office.
http://www.weathercharts.org/railway/Clapham_Junction_Collision_1988.pdf

Hillsborough Independent Panel (2012). *Hillsborough: The Report of the Hillsborough Independent Panel*. Report HC581. London: The Stationery Office.
http://hillsborough.independent.gov.uk/repository/report/HIP_report.pdf

Holloway, J. L. (1980). [Iran Hostage] *Rescue Mission Report*. Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff.
http://www.history.navy.mil/library/online/hollowayrpt.htm

Hone, Trent (2006). " 'Give Them Hell!': The US Navy's Night Combat Doctrine and the Campaign for Guadalcanal." *War in History* Vol. 13 No. 2, pp. 171-199.

Huber, Reiner, Tor Langsaeter, Petra Eggenhofer, Fernando Freire, Antonio Grilo, Anne-Marie Grisogono, Jose Martine, Jens Roemer, Mink Spaans, and Klaus Titze (2008). *The Indian Ocean Tsunami. A Case Study Investigation by NATO RTO SAS-065 Part II: The Case of Aceh and North Sumatra*. Washington, D.C..: United States Department of Defense, Command and Control Research Program.
http://www.dodccrp.org/files/case_studies/Tsunami_case_study.pdf

Independent International Fact-Finding Mission on the Conflict in Georgia (2009) ["Tagliavini Report"]. *Independent International Fact-Finding Mission on the Conflict in Georgia, Report, Vol. II*. Brussels: Council of the European Union.
http://www.ceiig.ch/Report.html

Knabb, Richard D., Jamie R. Rhome, and Daniel P. Brown (2005). Tropical Cyclone Report: Hurricane Katrina, 23-30 August 2005. Miami, Florida: National Hurricane Center.
http://www.nhc.noaa.gov/pdf/TCR-AL122005_Katrina.pdf

Lieberman, Charles A., and Serguei Cheloukhine (2009). "2005 London Bombings." Chapter 13 in M. R. Haberfeld and Agostino Von Hassell (Eds.) *A New Understanding of Terrorism: Case Studies, Trajectories and Lessons Learned*. Pp. 233-248. New York: Springer.

Lindsey, Brian W. (2004). MAFFS and Military Support to Civil Authorities: A Study in Command and Control. Report AFIT/GMO/ENS/04E-11 [Master's Thesis]. Wright Patterson Air Force Base, Ohio: Air Force Institute of Technology.
http://www.dtic.mil/dtic/tr/fulltext/u2/a460033.pdf

McDaniel, John R. M. (2001). "C2 Case Study: The FSCL in Desert Storm." *Proc. Sensemaking Workshop*, Vienna, Virginia. Washington, D.C.: Command and Control Research Program.
http://www.dodccrp.org/events/2001_sensemaking_workshop/pdf/C2_FSCL_doc.pdf

McDermott, Roger N. (2009). "Russia's Conventional Armed Forces and the Georgian War." *Parameters*, Spring 2009, pp. 65-80.

Makinen, Gail (2002). *The Economic Effects of 9/11: A Retrospective Assessment*. Report RL31617. Washington, D.C.: Library of Congress, Congressional Research Service.
http://www.fas.org/irp/crs/RL31617.pdf

Moody, Theodore J. (2010). *Filling the Gap Between NIMS/ICS and the Law Enforcement Initial Response in the Age of the Urban Jihad*. Master's Thesis. Monterey, California: Naval Postgraduate School.
http://www.dtic.mil/dtic/tr/fulltext/u2/a531492.pdf

Moynihan, Donald P. (2006). "What Makes Hierarchical Networks Succeed? Evidence from Hurricane Katrina." *Annual Meeting of the Association of Public Policy and Management*, Madison, Wisconsin, November 2-4.
http://www.lafollette.wisc.edu/appam/moynihankatrina.pdf

National Commission on Terrorist Attacks upon the United States (2004). *The 9/11 Commission Report: Final Report of the National Commission on terrorist Attacks upon the United States*. Washington, D.C.: National Commission on Terrorist Attacks upon the United States.
http://www.9-11commission.gov/report/911Report.pdf

Oklahoma Department of Civil Emergency Management (2003). *After Action Report: Alfred P. Murrah Federal Building Bombing, 19 April 1995 in Oklahoma City, Oklahoma*. Oklahoma City, Oklahoma: Department of Central Services Central Printing Division, Publications Clearinghouse of the Oklahoma Department of Libraries.
http://www.ok.gov/OEM/documents/Bombing%20After%20Action%20Report.pdf

Parliament of Victoria, 2009 Victorian Bushfires Royal Commission (2010). 2009 Bushfires Royal Commission Final Report. Melbourne, Victoria, Australia: Government Printer to the State of Victoria.
http://www.royalcommission.vic.gov.au/finaldocuments/summary/pf/vbrc_summary_pf.pdf

Rappaport, Ed (2005). Preliminary Report: Hurricane Andrew. (Updated). Miami, Florida: National Hurricane Center.
http://www.nhc.noaa.gov/1992andrew.html

Shariat, Sheryll, Sue Mallonee, and Shelli Stephens-Stidham (1998). Summary of Reportable Injuries in Oklahoma: Oklahoma City Bombing Injuries. Oklahoma City, Oklahoma: Oklahoma State Department of Health.
http://web.archive.org/web/20080110063748/http://www.health.state.ok.us/PROGRAM/injury/Summary/bomb/OKCbomb.htm

Toal, Mark J. (1998). *The Mayaguez Incident: Near Disaster at Koh Tang*. Quantico, Virginia: Marine Corps War College.
http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA529638

Thomas, Charles S. (1987). *The Iranian Hostage Rescue Attempt*. Report AD-A183-395. Carlisle, Pennsylvania: U.S. Army War College.
http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA183395

Tucker, Spencer C. (Ed.) (2010). *Encyclopedia of Middle East Wars*. Denver, Colorado: ABC Clio.

U.S. Conference of Mayors (2004). *The United States Conference of Mayors Interoperability Survey: A 192-City Survey*. Washington, D.C.: United States Conference of Mayors.
http://usmayors.org/72ndAnnualMeeting/interoperabilityreport_062804.pdf

U.S. Fire Administration (1999). Wanton Violence at Columbine High School, Littleton, Colorado. Report USFA-TR-128. Emmitsburg, Maryland: U.S. Fire Administration.
http://www.usfa.fema.gov/downloads/pdf/publications/tr-128.pdf

U.S. Geological Survey (2013). *Earthquakes with 1,000 or More Deaths since 1900*. Online.
http://earthquake.usgs.gov/earthquakes/world/world_deaths.php

U.S. House of Representatives (2006). *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*. 109th Congress, 2nd Session, Report 000-000. Washington, D.C.: U.S. Government Printing Office.
http://www.c-span.org/pdf/katrinareport.pdf

U.S. Senate (2006). Hurricane Katrina: A Nation Still Unprepared. Special Report of the Committee on Homeland Security and Governmental Affairs, United States Senate, Together with Additional Views. 109th Congress, 2nd Session, Report S. Rept. 109-322. Washington, D.C.: U.S. Government Printing Office.
http://www.gpo.gov/fdsys/pkg/CRPT-109srpt322/pdf/CRPT-109srpt322.pdf

Winter, Jay (2010). "Demography." Chapter 17 in John Horne, Ed., *Companion to World War I*. pp. 248-New York: Wiley-Blackwell.