Assurances et gestion des risques
Insurance and Risk Management

CHIEF UNCERTAINTY OFFICERS, THE CASE OF THE ARMED FORCES

Paul-Antoine Croizé et Gilles Hilary

Volume 82, numéro 1-2, 2015

URI : https://id.erudit.org/iderudit/1091605ar
DOI : https://doi.org/10.7202/1091605ar

Aller au sommaire du numéro

Éditeur(s)

Faculté des sciences de l'administration, Université Laval

ISSN

1705-7299 (imprimé)
2371-4913 (numérique)

Découvrir la revue

Citer ce document

Croizé, P.-A. & Hilary, G. (2015). CHIEF UNCERTAINTY OFFICERS, THE CASE OF THE ARMED FORCES. *Assurances et gestion des risques / Insurance and Risk Management*, *82*(1-2), 177–189. https://doi.org/10.7202/1091605ar

Assurances et gestion des risques, Mars-juin 2015, Vol. 82 (1-2)
Insurance and risk management, March-June 2015, Vol. 82 (1-2)

CHIEF UNCERTAINTY OFFICERS, THE CASE OF THE ARMED FORCES.

Paul-Antoine Croizé* et Gilles Hilary**

In October 2014, the American Society of Tropical Medicine and Hygiene (ASTMH) held its yearly convention at the Sheraton New Orleans Hotel. One of the most pressing medical issues at the time was the Ebola pandemic. The Louisiana Department of Health & Hospitals had decided that anyone who had been in Sierra Leone, Liberia or Guinea, where the disease had been most prevalent over the preceding three weeks, should not travel to New Orleans to attend the conference. The idea was to minimize the risk of contamination. ASTMH objected to the policy as it would impede understanding of the epidemic. Risk management took precedence over uncertainty management.

This is not unusual. Many organizations have developed an apparatus to manage risk, as have the armed forces. However, what sets the armed forces aside from most organizations is their management of uncertainty. While many organizations have a Chief Risk Officer, very few appoint a Chief Uncertainty Officer.

1. Risk versus Uncertainty Management

Risk is characterized by both the probability and severity of a potential loss that may result from hazards due to the presence of an enemy, an adversary, or some other hazardous condition. It is a "known unknown". Uncertainty is a situation in which the probability and severity of a potential loss is not well understood – an "unknown unknown".

* This document was written by Paul-Antoine Croizé, a former Captain in the French Army (paul-antoine.croize@insead.edu).

** Mubadala Chaired Professor in Corporate Governance and Strategy at INSEAD. (gilles.hilary@insead.edu).

Uncertainty management is not simply an extension of risk management. In fact it can be the opposite of risk management. To illustrate: the French army operates an armored vehicle known as the VAB. The VAB gets slippery in the rain and caused numerous sprained ankles. Military personnel mitigated the risk by adding small wooden duckboards to the vehicle. But this stopgap measure became a serious problem when the modified vehicles were deployed in Afghanistan. Improvised Explosive Devices (IEDs) transformed the duckboards into shrapnel. In this way a safety measure developed to mitigate a peace time risk unexpectedly exacerbated a wartime danger.

Cyber threats are another example. Cyber-risk management involves implementing consistent procedures to protect the network against known problems. However, this homogeneity in response facilitates the propagation of unexpected threats once the system has been penetrated. In contrast, although heterogeneous fragmented systems increase the danger of known threats, they also reduce the likelihood that the entire system will go down in the event of infiltration.

For example, the US Government Printing Office recently suffered from a cyber-attack but it had such an antiquated network that it apparently confused the hackers. The weak risk-management procedures made it easier for the assailants to penetrate the system, but the strong (accidental) uncertainty-management techniques ensured that the penetration was not fully exploited. What turned out to be a fluke in this case can and should be strategically managed. However, while dealing with uncertainty is important, it is also difficult.

2. Leadership Material

The importance of uncertainty in a military context is obvious, the attack on Pearl Harbor being a case in point. But it is also highly relevant in the corporate environment (as the Fukushima catastrophe showed). Research suggests that uncertainty is psychologically painful. Most individuals, from Ethiopian farmers to American actuaries, are willing to pay a substantial premium to avoid projects with uncertain pay-offs. Indeed many organizations simply refuse to deal with it. In contrast, the armed forces not only acknowledge its existence but embrace it.

Managing uncertainty is not simply a defensive posture but can be used to an organization's advantage. On July 9 1943, Allied forces were preparing the invasion of Sicily by a massive combined aero-amphibious force. When a storm blew up, the Axis forces anticipated the prospect

of a much-needed rest. But the Allied commanders decided to commence the invasion. Their paratroopers suffered high casualties and were dropped behind enemy lines, but this created confusion among the defending army and made the amphibious assault easier than anticipated, leading to the overall success of the invasion. The uncertainty created a strategic advantage for the Allied forces.

Given the importance and the difficulty of managing uncertainty, the armed forces have long recognized that it largely falls to senior leaders. As early as the 19th century, the great German strategic thinker von Clausewitz noted in his classic On War that, "War is an area of uncertainty […]. The first thing (needed) here is a fine, piercing mind, to feel out the truth with the measure of its judgment."

The armed forces also recognize the psychological burden of uncertainty. As a consequence, many NATO armed forces systematically provide their senior ops officers (the C-suite) with one-on-one sessions with psychologists after a tour of duty in Afghanistan. In contrast, counselling is less systematic for individuals at a lower level of the organization who are less exposed to uncertainty, although they may be more exposed to physical danger.

3. War, Peace and Uncertainty

Some leaders are better equipped to handle risk; others are better at handling uncertainty. The relative importance of the two and the type of leader required will vary with the context. At the beginning of WWI, the French commander-in-chief Joffre replaced 134 generals appointed in peacetime who were deemed ineffective in wartime.

In time of peace, the dangers are relatively well identified. For example, between 2002 and 2007, road traffic accidents accounted for 25% of fatalities in the French armed forces, 25 times more than combat operations. Addressing these risks requires well-defined procedures that are refined over time and backed by robust enforcement. In other words, the risks are managed through a strong command-and-control structure in which only senior officers have a significant degree of autonomy. Hierarchy is rigidly enforced. Risky activities are identified ex ante and are discouraged by explicit incentives in a quasi-contractual environment. The main goals of organizations dealing with risk are efficiency and reliability.

In times of war, risk ceases to be the main issue; uncertainty and "strategic surprises" become the critical concerns. Dealing with uncertainty requires a different approach from dealing with risk. Soldiers look for leaders rather than managers. Those at a lower level in the hierarchy are given more autonomy and hierarchy is less rigidly enforced. Incentives become fuzzier and rewards are granted based on ex-post outcomes rather than on ex-ante activities. Personal commitment rather than quasi-contractual incentives become the dominant motivation. The main goals of organizations dealing with uncertainty are agility and resilience.

The armed forces once used a powerful signal – a declaration of war – to tell them what to prioritize. For example, the French Army operates its Leclerc tanks in two modes. In peacetime, any anomaly automatically stops the tank, which is then sent for inspection and maintenance – the battle tank leader has no control over this. In wartime, the machine is re-parameterized to give the battle tank full control and the ability to override any safety feature when necessary.

However, the proliferation of low-intensity conflicts and international terrorism has largely negated this clarity. The corporate and military environments have become more similar, and therefore civilian organizations can learn from the solutions deployed by the armed forces to manage uncertainty, information-based solutions and action-based solutions.

4. Deploy Information-based Solutions

The first and most obvious solution is to convert uncertainty into risk, i.e., to transform "unknown unknowns" into "known unknowns". The armed forces have developed elements of doctrine, tools, processes and frameworks to optimize the management of institutional knowledge.

4.1. Filter

Obtaining information used to be the main issue, but the development of technology has created the opposite problem: coping with a huge volume of raw data. Some 85 percent of CFOs and CIOs questioned in a recent survey said that they did not know how to analyze the data they had collected. Meanwhile 54 percent said their greatest barrier to success was their inability to identify the data worth collecting. To quote Leon Platt, former CEO of HP, "If HP knew what HP knows, HP would be three times more effective."

To address this problem, the armed forces filter information through a systematic four-part process (Direction, Collection, Analysis and Dissemination). Direction is essential for efficient information filtering. It defines which information needs to be acquired based on a standardized classification. Intelligence Requirements (IRs) represent the information necessary to fill a gap in the leadership's knowledge and to help it formulate a strategy. For example, knowing the attitude of local influencers towards an insurgency could be an IR. Priority Intelligence Requirements (PIR) represent information necessary to execute strategy. For example, knowing in which valley hostages are located would be classified as PIR.

To illustrate this, in July 2009, the 1st Battalion, 5th Marines were deployed in the Nawa district in Afghanistan, a complex area where they could not go half a mile from their base without being exposed to ever-evolving threats. The Marines approached the situation with a well-structured intelligence approach. First, they set a clear direction for their information-gathering and decided that understanding the local population in their area of operation was a top priority. They issued IR and PIR in line with this strategy. Units reported on a daily basis through radio "chat sessions" with analysts. Thus information was analyzed and disseminated to the right users in real time. Every chat session closed with updated IR. This allowed the battalion to see that the Taliban threatened the local elders' traditional power structure. The Marines were able to relieve the pressure on local elders and to offer them some protection, which fostered good relations with the local population, who ultimately chased the Taliban out. The Marines managed to revive the district and reduce IED incidents by 90%.

4.2. Structure

Data is guaranteed, knowledge is not. For data to be useful, it has to be structured in a mental environment that will provide meaning. This process transforms data into information, and then into knowledge. Cognitive traps conspire to prevent this learning. For example, people are known to suffer from confirmatory bias, the human tendency to look for data to confirm pre-conceptions. Our research shows that executives and financial analysts grow overconfident in their skill and in the amount of risk they take after a string of successes. Managerial overconfidence has been identified as one of the key drivers of the 2007 financial crisis.

The armed forces are not immune to this issue. American signal intelligence units gathered the necessary information to warn the American leadership about the Tet Offensive and the invasion of Saigon by North Vietnamese forces, but the evidence was rejected as it did not fit with the pre-conception of senior officials. To mitigate the problem, armed forces have systematized the use of "red teaming", the use of an independent individual who challenges an organization to improve its effectiveness. For example, the US Army does this even at the company level (approximately 175 people). We witnessed the effectiveness of this approach in recent military operations in the Sahel conducted by the French armed forces. Red teaming also mitigates cultural biases and allows it to understand the thinking process of one's opponent. For example, members of the Chinese Blue Force (the equivalent of the Western Red Teams) are not allowed to use chopsticks.

Naturally the process has its limitations. Red teamers often display biases and make assumptions that are similar to those of the leader. Millennium Challenge 2002, a $250 million war game conducted by the US armed forces, probably the largest in history, opposed a Blue Force (representing the US) and a hypothetical Red Force commanded by retired Marine Corps Lieutenant General Paul Van Riper. Van Riper resigned in the middle of the war game as he thought the exercise was being used to reinforce existing doctrine and notions of infallibility within the US military rather than serving as a learning experience.

4.3. Learn and Educate

Once individuals or divisions have learned from their mistakes, the next challenge is to transfer the acquired knowledge throughout the entire organization. A well-known illustration of this is the fact that General Motors had difficulty transferring lessons from its experience in the Saturn division to the rest of the company. By failing to learn from past events, potential dangers remain unknown. Consider data breaches suffered by companies like Target. The first attack is unlikely to be catastrophic. For example, large financial institutions suffer at least one credible cyber-attack a day. The specific form of attack that may create catastrophic damage remains uncertain until it occurs, but the knowledge built up from less significant attacks may prove to be particularly useful.

One of the key strengths of Western armed forces is their capacity to be learning institutions, which has been achieved through multiple channels. First, an apparatus dedicated to learning has been built. Military academies, think-tanks and academic journals have been organized and funded to work in an integrated eco-system that has built ties with external communities. For example, the creators of the video game Call of Duty received feedback when they developed the game; now the game's designers provide insight to the military.

Second, senior people recognize that learning at the individual level occurs in part through making mistakes, an aspect institutionalized in military doctrine. For example, the US Army doctrine acknowledges that "Humans sometimes make mistakes" and "Successful commanders allow subordinates to learn through their mistakes and develop experience. With such acceptance in the command climate, subordinates gain the experience required to operate on their own." The capacity to learn from mistakes facilitates individual mastery.

Third, at the institutional level, the Analysis After Action (AAA) process is used after every significant mission or exercise to improve the capacity of the system. An AAA is not a critique; it is a dynamic, candid, professional discussion that focuses on unit performance. AAA is institutionalized. For example, the US Army Field Manual (AFM) explicitly states that AAA should be an integral part of the planning for an operation, not an afterthought. They should occur at or near where the operation occurred. In 2013, French troops entered Mali to stop the AQIM's march on Bamako. Despite a strict limit on the number of personnel deployed, French headquarters concluded that the presence of an AAA team was necessary from the very beginning. It played a key role in the overall success of the operation as the troops could learn in real time from their mistakes.

This knowledge is then passed to training centers and used to educate "employees". For example, the US AFM explicitly mentions that "sound knowledge management practices include […] reachback capability to Army schools, centers of excellence, and other resources." Along the same lines, French officers and non-commissioned officers who have served multiple tours of duty on foreign theatres become cultural instructors for fresh troops and for senior officers who have inadequate knowledge of the region they are about to operate in. This enables the diffusion of knowledge through the entire organization. It has the side benefit of improving the perception of self-worth when individuals are brought home after a period of high activity.

4.4. Communicate

In February 2014, General Motors recalled hundreds of thousands of its Chevrolet Cobalt and Pontiac G5 sedans after several deaths on the road were linked to faulty ignition switches. One of the causes of this fiasco may have been poor communication. For example, critical information was located in the "back-up" slides of a 72-slide PowerPoint deck. In addition, terminology was neither standardized nor clear. Employees used the expression "does not perform to design" instead of the better-defined word "defect."

Armed forces follow a structured process to mitigate the possibility of miscommunication. The format of an order is standardized. It systematically follows a 5 part structure:

- Situation: This ensures that there is common vision of the context
- The mission the leader received from her superior: This helps understand what the whole unit will do and what the critical aspects of the mission are.
- Execution: Sub-units receive their mission. They are then free to decide how to proceed, as long as it remains legal and ethical.
- Coordination: This ensures quick reactions to emerging threats.
- Logistic: This ensures that everyone possesses the means to perform her duty.

Interestingly, all key terms are so standardized that they can be graphically translated. For example, all NATO officers can understand the main components of a mission regardless of the language used to describe them.

5. Deploy Action-based Solutions

Aside from information-based solutions, the armed forces use action-based solutions to mitigate the effect of uncertainty. The approach takes a systemic view of uncertainty, which is to see the organization as a collection of parts that interact. The role of the leader here is not to deal with every possible contingency but to facilitate the functioning of the system (through the development of an appropriate structure and culture) and to ensure that the system is not drawn into a situation beyond its recovery capacity. An efficient army at war stands on the edge of chaos, stretched but not broken. The role of a leader in this

context is to ensure that the organization does not stand idle, unresponsive to enemy maneuvers until it is too late (as the allied armies stood during the Phoney War) but also that the organization does not spiral out of control in a chaotic way (as the same allied forces did a few months later).

5.1. Simplify

The biggest lever of internal uncertainty is complexity. Anyone managing IT programs can attest to the fact that complexity breeds failure caused by some unexpected sources. Consistent with this view, research has shown that system efficiency declines as complexity increases.

A system is designed to reach certain objectives through a series of elementary steps. At the conceptual level these are easy to execute, but soldiers realize the difficulty of performing the most basic things in times of crisis. As noted by Clausewitz, "Everything is very simple in war, but the simplest thing is difficult. These difficulties accumulate and produce a friction." The role of the leader is to "cut through the frictions". However, not all frictions are equally important. Some are non-linear, i.e., the output is not proportional to the input. Not realizing the importance of these non-linear frictions can be fatal. The role of a leader in this context is to identify these critical frictions.

To combat the natural tendency of systems to drift toward complexity, the armed forces have developed a structured approach. For example, the United States Marines Corp applies the KISS principle: Keep it simple, stupid. The KISS principle is critical especially in periods of turmoil such as military operations and corporate turnarounds. In particular, it imposes structure. The normal project management structure in the armed forces is "A leader, some resources, an objective." Despite its many advantages, matrix environments increase complexity and therefore internal frictions. As a consequence the decision process slows down and misunderstandings are more likely to occur as people struggle to see the big picture and the extent of their decision rights.

In 2011, the French Army abandoned this principle to introduce Louvois, a new software to handle salary and benefits payments. The compensation policy was highly complex, with payments changing from month to month. No single individual was in charge of the project, diluting responsibility throughout the organization. It was an abject failure, resulting in the abandonment of the software after $580m had been spent on the project.

5.2. Decentralize

On January 20 2008, Société Générale (SocGen) discovered that one of its traders, Jerome Kerviel, had traded well beyond his limit, putting the very existence of SocGen was at stake. CEO Daniel Bouton was later quoted as saying on that day: "This is happening to us. We are a world leader in the most sophisticated sector in the world! We have the greatest mathematicians. We hire a third of the graduates from Polytechnique [the French MIT] every year, and our mission is precisely to negate all risks through the sheer power of calculations, of correlations, of controls. This is happening to us!"

Historically, there have been two competing conceptions of warfare in Western strategic thinking: rigid and flexible planning. The first is exemplified by Alfred von Schlieffen, whose 'Schlieffen plan' envisioned the complete destruction of the French army in six short weeks in the summer of 1914. His approach negated the importance of frictions. Rigid and detailed planning coupled with a centralized command structure would overcome "events". The army was a huge machine that functioned based on precise rules and calculations. Despite its initial success, the German army was finally stopped by a series of internal and external surprises, and eventually defeated.

The second approach is exemplified by Helmut von Moltke, who embraced the existence of frictions. "In war, everything is uncertain as soon as operations have started with the exception of what the leader brings in terms of willpower and energy." His approach was based on two principles. The first was to entrust subordinates with the capacity to analyze a situation and to act based on their analysis. The second was to create a strong military culture based on a thorough understanding of the prevailing doctrine by officers. In other words, Moltke dealt with uncertainty through principle-based management rather than rule-based management. He led the Prussian armies through a series of successful campaigns, culminating with the invasion of France in 1870.

Despite the extraordinary development of means of communication, leaders get only a fragmentary picture of their global operations, hence micromanagement is counterproductive. As General Patton once said, "Never tell people how to do things. Tell them what to do and they will surprise you with their ingenuity." To illustrate, during the Falklands war, the British commanding officer at the Battle of Goose Green did not allow his sub-unit commanders to exercise initiative, which brought

the British forces to the brink of disaster. They eventually prevailed but only after the initial commander was killed in action and replaced by his deputy, who gave more flexibility to his subordinates.

5.3. Plan

Decentralizing decisions does not mean lack of planning. It means deciding on the strategic objectives, identifying the resources that are required, and then delegating the execution. However, most individuals suffer from over-optimism about what is achievable with the available resources. For example, mergers and acquisitions are regularly done on the premise of synergies for which the acquirer is ready to pay a large premium. Yet the success rate is around 50%. M&As can quickly turn into a nightmare scenario, as the recent case of Autonomy shows.

Scenario analysis ensures a better handling of contingencies. In a military context, commanders consider two options to combat this problem: the most likely case and the worst case scenario. This is particularly useful to understand the behavior of a complex environment with numerous moving parts. Scenario planning also helps identifying weaknesses. For example, most high-level military meetings occur in the early morning. Unfortunately, this is also the best time to attempt suicide attacks as a suicide bomber is more likely to suffer from "buyer remorse" as the day progresses. Scenario planning along the lines of "How would I attack my organization" helps identify this type of issue.

5.4. Build resilience

No matter what they do, organizations will be hit by unexpected hazards. One important aspect of uncertainty management is the capacity that organizations must respond rapidly to shocks by adapting a stable configuration.

One way to deal with unexpected shocks is to optimize the use of reserves. In 2003, American armed forces created a 100-people unit, known as the Agile Development Center, to develop an efficient crash program to fulfill specific needs that could not be foreseen. This was only possible because the US military had a strategic reserve of manpower and organizational slack. But keeping idle reserves is costly. Many firms prefer to manage their inventory "just in time" rather than "just in case".

A more sophisticated form of reserve is the distribution of skills in the organization based on the principle of "serial incompetence". The idea is to avoid the presence of subject-matter experts specializing in one area for years. Rather, a typical career in the armed forces is organized around two-year assignments during which individuals are driven to achieve proficiency before moving on to the next area. This approach mitigates the risk that thinking becomes ossified and ensures that knowledge is distributed throughout the organization rather than concentrated in a limited number of individuals. It also keeps resources active even if they serve as a de facto reserve.

Another essential tool to build system resiliency is modularity. It is included in the NATO doctrine through the taskforce concept, and its importance has been one of the key learnings from the conflict in Afghanistan. Subsequently it was successfully applied in Mali in 2013, where ad hoc cross-functional teams were created at the "sub battlegroup" level (around 150 individuals) for each operation.

Conclusion

While risk management is now considered to be a managerial, an organizational and sometimes a legal imperative, uncertainty management is much less understood or recognized. Managing risk sometimes helps managing uncertainty (and vice versa). But counter-intuitively, managing one often has a detrimental effect on the other.

At the individual level uncertainty is psychologically painful to address. At the organizational level, there is typically no champion to push for its management. Before they arise, little is done to prepare the organization for unknown shocks. When negative surprises do arise, it is often convenient to refer to "black swans" and allow fate to absolve everyone from his or her past responsibility. Uncertainty is thus left unmanaged.

However, much is to be gained from handling uncertainty in a structured framework. Understanding the requirement to systematically gather and analyze intelligence, to form robust organizational structures and develop efficient communication channels reduces its importance. The ability to react to surprises, to be bold and to make decisions with incomplete information mitigates its consequences.

Senior leadership obviously has a key role to play in this context. A first (often neglected) step is to recognize the existence of uncertainty, or better, to embrace it. As with risk management, leaders have to formalize the organizational appetite for uncertainty. They have to develop and implement policies, oversee the use of tools and procedures, and nurture an appropriate culture. Unlike risk management, they operate in a fuzzier world with fewer tried-and-tested tools and methodologies. Perhaps the most critical task of the leadership is to recognize when managing risk should be the priority and when managing uncertainty should be the priority.

Not all leaders are equipped to manage uncertainty. For example, in a recent operation, a senior commanding officer who was excellent at managing risk had to be replaced by another who was better at handling uncertainty. This has implications for boards engaged in the oversight of risk and uncertainty.