OPERATIONAL RESILIENCE: APPLYING THE LESSONS OF WAR

GERHARD WHEELER | Head of Reserves, Universal Defence and Security Solutions

ABSTRACT

We live in an age of disruption. Our open and highly networked societies are becoming increasingly vulnerable to threats that once often remained local in scope but can now unfold shockingly quickly and cause damage across the globe. The imperative for businesses to become more resilient – better able to survive operational disruptions – is clear, but where should they look for inspiration? This paper suggests that a good start point is to look at lessons learned by military commanders who run organizations that are specifically designed to respond to crises. Drawing on historical examples from military campaigns, it outlines a battle-tested framework for resilience. Built around the need to anticipate, detect, deter, withstand, respond, and recover from threats, the framework describes resilience tactics that are as applicable to the boardroom as they are on the battlefield.

1. INTRODUCTION

We live in an age of disruption. The openness and global connectivity that characterize our highly networked societies deliver many benefits but also make it far harder for organizations to contain threats. Risks that often remained local in scope can now unfold shockingly quickly, cross national borders unchecked, cascade over system barriers, and cause damage across the globe. We saw it when a cyber cryptoworm devised to extort ransoms from Microsoft users crippled the U.K.'s National Health Service for days; when a pastor threatening to burn Qurans in Florida incited violent protests in Afghanistan; and when the outbreak of a novel coronavirus in a Chinese city triggered a global recession. The imperative for businesses to become more resilient – better able to survive operational disruptions – is clear, but where should they look for inspiration? A good starting point is to look at lessons learned by military commanders who run organizations that are specifically designed to respond to crises.

Although corporate buzz phrases are often shot through with military terminology – takeover battles, dawn raids, ad campaigns – business is not war. Military decisions are rarely framed by customers, profits or shareholders: business executives can succeed without defeating an enemy or inflicting casualties. Nevertheless, there are some military concepts that can be applied in a corporate context. Operational resilience travels well from the battlefield to the boardroom because it addresses a universal need to be able to continue to operate in disruptive environments. It is also relevant because it is so fundamental to the output of armed forces that it receives a level of study and development by military thinkers that few management gurus can match.

A health warning first. Military organizations are inherently better equipped to deal with crises than most businesses. The majority of companies spend much of their time operating and only occasionally train to deal with a crisis. Armed forces do the opposite. They spend the bulk of their time preparing to deal with the occasional crisis; all of their people know how to respond in an emergency before it happens. Modern corporate organizations tend to favor flat management structures, which can be highly effective in a stable environment but less robust in a crisis than the traditional hierarchical structures employed by military forces. The unrelenting drive to achieve efficiencies in the corporate world favors the use of lean supply chains. Military organizations, on the other hand, hold levels of reserves that would be unaffordable for most corporate entities to retain but that allow them to better absorb shocks. Despite these structural advantages, military doctrine still has much to offer to business.

Armed forces assume that they will operate in environments that they describe as VUCA – volatile, uncertain, complex, and ambiguous. They accept that there will be periods when disruptive events will control their actions, forcing them to become reactive. Their resilience models are, therefore, structured to allow them to regain the initiative as quickly as possible. They employ tactics that are built around the need to anticipate, detect, deter, withstand, respond, and recover from threats. Set out below are some of the key lessons that can be drawn from this battle-tested resilience framework.

2. ANTICIPATE

Military history is littered with the debris of armies that failed to anticipate a threat. One of the most striking examples resulted in the spectacular fall of Singapore in 1942. The Imperial Japanese Army attacked the fortress island city on 31 January 1942. The strength and direction of their assault came as a shock to the British-led garrison defending the strategic port. The British Empire's pre-war analysis of the threat to Singapore had concluded that any invasion force would have to come from the sea to the south of the island. An assault through the thick jungles of the Malay Peninsula to the north of the island had been discounted as impossible. As a result, the British decision to center its defense on the building of coastal fortifications proved to be a fatal miscalculation. Just weeks after the surprise attack by the Imperial Japanese Navy on the U.S. Fleet in Pearl Harbor, Japanese ground troops, supported by their air force, surged through Thailand and down the Malay Peninsula. The jungle had proved to be a minimal obstacle to their well-trained troops – some of whom were even mounted on bicycles. The Japanese crossed into Singapore across the narrow Straits of Jahore on the north-west side of the island on 8 February 1942. After a short period of intense fighting, seven days later, the British Commander, Lieutenant General Arthur Percival, raised the white flag of surrender over Singapore.

The disastrous defense of Singapore – over 130,000 Allied troops were taken prisoner – was blamed on several reasons but key among them was a failure to anticipate the true nature of the threat. To combat this failure in imagination, modern military planning techniques promote the use of red-teaming. Red teams are planners who view the problem from an opponent's viewpoint. They are deliberately isolated from a primary planning team so that they can provide an alternative analysis of the threat. They are separated from the primary planners to avoid the danger of "group-think" – a human bias towards agreeing with the majority viewpoint. Once planning has finished, they stress-test the primary plans during war games.

Red teams can be highly effective in identifying gaps in resilience plans. During a 1932 wargame, Rear Admiral Harry E. Yarnell devised a simulated air attack on Pearl Harbor that closely matched the tactics employed by the Imperial Japanese Navy nine years later. However, these prophets of doom are not always welcomed by the senior leadership of an organization. Admiral Yelland's analysis of the threat to Pearl Harbor was dismissed by his superior officers as an unlikely scenario.

3. DETECT

Even when a threat has been correctly assessed, it is not uncommon in war to fail to detect the signals that warn of an impending crisis. During the Cold War, the only way the Soviet Union would allow Russian Jewish emigres to emigrate to Israel was by first traveling by train to Vienna. On September 28, 1973, the Chopin Express train was hijacked just inside the Austrian border by an armed group that called itself the Eagles of the Palestinian Revolution. They took five Jewish emigres and an Austrian customs official hostage. In exchange for the safe release of the hostages the hijackers demanded the closure of the Schoenau transit camp in Vienna, which housed Russian Jewish emigres waiting to be processed for onward flights to Israel. The Austrians quickly capitulated and allowed the hijackers to fly to safety in Libya in exchange for the lives of the hostages.

The Schoenau Ultimatum became a cause célèbre in the Israeli press. The incident consumed the attention of the Israeli cabinet for several days. The Israeli prime minister, Golda Meir, even diverted her return flight from the Council of Europe in Strasbourg to go to Vienna to try and persuade the Austrian chancellor not to close the Schoneau Camp. Her appeal fell on deaf ears. After her meeting on October 2, 1973, she flew back in indignation to Tel Aviv to face the press. Three days later, Egypt and Syria launched a joint invasion of Israel that nearly destroyed the fledging Jewish state in what was later called the Yom Kippur War.

There is no concrete evidence to prove that the Schoenau Ultimatum was designed to distract Israeli senior leaders in advance of the Yom Kippur war, although the Eagles of the

Palestinian Revolution proved to be a cover name for a Syrian-backed group, As Sa'iqa. However, what is certain is that this incident and other failures in intelligence meant that warning signals that Egyptian and Syrian forces were mobilizing on Israel's borders were ignored by Israel's senior leadership. In effect, a threat that had been widely anticipated was not detected.

To try and ensure weak warning signals are not missed, modern military command and control systems favor the use of "empowered" deputies whose job it is to remain focused on a different set of priorities to the head of a leadership team during a crisis. This tactic is designed to counter the inevitable tendency of members of a leadership team to work on the priorities and agenda of the head of the organization in a crisis and ignore warning signals from other emerging threats.

4. DETER

In most cases, it is better to deter a threat than incur the costs of a crisis that it can create. The U.K.'s defense review of 1981, which proposed significant cuts to the Royal Navy in response to extreme financial pressures, is a case in point. Named after the U.K.'s defense minister of the time, the Nott Review's proposals included the decommissioning of HMS Endurance, a survey ship that represented Britain's only persistent naval presence in the South Atlantic. To the military junta ruling Argentina at that time, the publication of the Nott Review confirmed the junta's perception that the U.K. was no longer serious about trying to deter Argentina's long-held objective to seize the Falkland Islands and claim them for Argentina as Las Malvinas. As a result, in May 1982, the junta dispatched an Argentine fleet to capture Britain's South Atlantic dependency. Although the invasion was initially successful it proved to be a miscalculation by the junta. To their surprise, Britain's prime minister, Margaret Thatcher, ordered a carrier taskforce to retake the Falklands. The ensuing war lasted several weeks and resulted not only in the liberation of the Falkland Islands but the eventual political collapse of the Argentine junta, at the cost of hundreds of lives. In hindsight, there is little doubt that if Britain had adopted a slightly different military posture ahead of the war, it would have been enough to deter the junta from risking an invasion.

The Falklands War underlined the difficulties resilient organizations face in deterring threats. Physical measures can be effective but modern military doctrine recognizes that deterrence is ultimately a psychological process. To deter a human-directed threat requires the ability to understand the mindset of those posing the threat and an ability to influence their behavior. Ultimately, those that have the potential to pose a threat must perceive that the cost of hostile action is not worth the benefit. Key to this process is the idea of influence operations – the synchronized co-ordination of actions and messages across a number of channels with the aim being to change an opponent's behavior. This is probably the most complex area of resilience doctrine; in its most sophisticated form it encompasses behavioral science ideas such as game theory, which was applied to nuclear deterrence and won its author, Thomas Schelling, the Nobel Prize. At its simplest, however, it is the application of the stick and carrot approach to behavior. It does, though, depend on the requirement to recognize the need to deter in the first place, which Britain had clearly forgotten in the run-up to its conflict with Argentina over the Falkland Islands.

5. WITHSTAND

When deterrence fails, an organization should plan to be able to withstand a threat, at least in the short term, to provide leaders with the time and space needed to regain the initiative. The Finnish Winter War at the beginning of the Second World War is a notable example. On November 30, 1939, Stalin invaded Finland with a Soviet army comprising over 600,000 troops. The Finnish army only numbered 300,000, which included all of its reserves and conscripts, had only a few tanks, barely any aircraft, and hardly any ammunition to supply its small artillery force. However, it and every element of the civilian society that supported it was prepared to withstand the threat it faced. Most of its soldiers were expert skiers, experienced hunters, and knew how to survive in the cruel winter of the Arctic Circle. Few of the Soviet conscripts sent into the frozen wilderness were even equipped with snow shoes let alone skis. The Finns drew the invading Soviets further and further into the snow-covered Finnish hinterland. As they did so, they split into small independent units and used their superior mobility to conduct harassing attacks designed to grind down the ill-equipped Soviet troops. The Soviets were forced to remain in unwieldy columns on roads and tracks while the Finns enjoyed complete freedom of movement. The warring parties agreed a peace deal after 105 days of hostilities. The Finns lost 11 percent of their territory but retained their sovereignty. The Soviets lost over 200,000 men, compared to Finnish casualties of 25,000, and took a significant hit to their international reputation.

The Finnish Winter War of 1939 illustrates how to plan to withstand a threat. Unlike many business plans, which focus on an optimistic view of success, good military planning assumes failure. It recognizes that in a volatile environment things will go wrong, or, as the 19th Century Prussian General von Moltke noted, “No plan survives contact with the enemy”. As a result, effective military resilience plans are designed to absorb losses, disperse assets, build in redundancy, focus protection on vital resources, maintain reserves, secure supply chains, disguise strengths, and defend in depth. Most importantly, they ensure that the whole of the organization is prepared and trained to act in a crisis.

6. RESPOND

Ultimately, to regain the initiative in a crisis, an organization must be able to respond to a threat at a faster pace than the threat can adapt. The Battle of Britain is famous for the exploits of “The Few”, the brave Spitfire and Hurricane Royal Air Force fighter pilots who prevented the planned Nazi invasion of Britain. In the summer months of 1940, they were able to stop the German Luftwaffe’s attempt to achieve air supremacy over the skies of southern England by responding to threats at a faster rate than their numerically superior opponents could muster them. The ability of Britain’s Royal Air Force to respond to the existential crisis the U.K. faced in 1940 was down to several factors, but key among them was the command and control system they employed: the Dowding System.

Prior to the Second World War, Air Chief Marshal Sir Hugh Dowding recognized that Britain needed a new way to co-ordinate its air defenses if it was to be able to respond at a rapid enough pace to get ahead of emerging airborne threats. His approach was to fuse new technology, information, and weapon platforms into one system underpinned by a leadership culture of delegated responsibility. The system was based on a chain of aircraft detection sites using the newly-invented radar technology and human air observers to detect incoming raids. Sightings were passed to the Filter Room at the headquarters of Fighter Command. Once the direction of a raid had been established, the Filter Room sent the information to the relevant group headquarters responsible for a U.K. region. They then sent the data to their subordinate sector stations that “scrambled” the fighters into action. The system then passed real-time updates across the network, both to the fighters and anti-aircraft guns on the ground. The system was revolutionary in its ability to pass information across the battlespace at speed but also in trusting junior commanders to use their initiative. In a break from established British command culture, the system adopted the German Auftragstaktik or mission-type tactics system, which shunned prescriptive orders and replaced them with mission statements that concisely explained what needed to be done and why but left the method to the initiative of the commander that received the mission.

The Dowding System is the foundation of modern military response systems. For businesses, it offers some key insights.

First, the imperative to communicate data immediately during a crisis. In civilian management systems, it is not unusual for a manager to respond to a new issue by examining it and trying to solve it before telling others. Military leaders responding to a crisis do the opposite. They are trained to immediately pass new information across their network – above, below, and sideways – before they act. This ensures that everyone is alerted to a situation that could expand rapidly and quickly engulf bystanders. It is better to shout "fire!" first before trying to put a blaze out.

Second, military senior leaders instinctively focus on the wider implications of an incident rather than get sucked into the detailed co-ordination of the response. The senior leader's job is to look wider and deeper so that they can predict what resources or actions need to be put in place in the near term. If you think you will run out of fire extinguishers in an hour's time then someone needs to make a decision to get more now and not when it happens. The leader can leave the operation of the extinguishers to others.

Third, however well a leader has developed a consultative leadership style, they must remember that there are times when a more directive style might be required. A crisis is often that moment. There may not be the time for discussion with subordinates who are looking for decisive action; often an early response based on incomplete data is more effective than a late response informed by better information.

Fourth, it is important to have at least one person in a crisis response detached from the fray – someone needs to record what is happening so that incident leaders can wind back to check what decisions were made when and keep a handle on important data. This person must be relentless in confirming data – the old adage is often true: the first report of the enemy is always wrong.

Finally, the mission-type tactics system works well in a crisis but only if it is already part of the culture of the organization. Senior leaders must have already learned how to communicate their intent without being prescriptive and to trust subordinates to use their initiative. For their part, junior leaders have to learn how to understand the bigger picture. They must know not only what their boss wants them to achieve but also what their bosses' boss wants; they need to able to think "2 Up", as in two levels above them. Finally, leaders must run rehearsal exercises and lead by example. Handing over control to a consultant at the time of danger is unlikely to work: consultants advise, leaders decide.

7. RECOVER

It is human nature to focus on the response to a crisis rather than the recovery from it, but without an effective recovery from a crisis an organization is doomed to repeat past mistakes. On 11 January 1942, the German Navy began Operation Drumbeat, its campaign against allied merchant shipping along the U.S. East Coast. The U.S. Navy seemed unprepared for the onslaught it would face from the German U-boat wolfpacks. In a six-month period, 117 German U-boats conducted 168 patrols along the northeastern seaboard. They sank 240 allied ships. A parallel U-boat operation in the Caribbean sank another 234 allied ships. Over 6,800 sailors and passengers were lost at sea. Only five German U-boats were sunk during this period. However, in June 1942 the U.S. Navy changed tactics and adopted the convoy system for protecting merchant vessels. Merchant ships were grouped into packets and escorted by warships. In two weeks, the U.S. Navy sank seven U-boats. The tide had turned. Admiral Doenitz, supreme commander of the U-Boat fleet, called an end to Operation Drumbeat.

There are various theories why it took six months for the U.S. Navy to adopt the convoy system already in use by Britain's Royal Navy. Some cite the need to reinforce the U.S. Pacific Fleet following the shock of the Japanese surprise attack on Pearl Harbor, others the demand to guard troop ships ferrying American soldiers to the U.K. allowing Britain to release troops for its North African campaign, and others believe it lay in an early institutional failure to learn fast enough. Whatever the reason, the terrible events of that period underscore the cost of failing to adapt during a crisis.

Recovery depends on the need to learn and adapt at pace. Best learning practice in modern military organizations places a premium on the "After-Action Review" process. This process revolves around group debriefing sessions after every incident. The aim is to identify lessons, irrespective of whether the incident was deemed a success or failure. During the review, the team talks through the chronology of the events that occurred. Participants are encouraged to be honest about the actions they took and critical of both themselves and others.

This can sometimes be difficult to achieve when it involves criticizing the actions of superiors, but it is not impossible. When employed properly it can significantly accelerate the learning process. The results of the After-Action Reviews are fed into a lessons branch where they are analyzed and promulgated as widely as possible. Importantly, new lessons are called “Lessons Identified” until it has been confirmed that the organization has determined that the lessons have actually been learned by the institution and embedded into standard processes. An organization that learns will become more resilient.

8. CONCLUSION

The period when organizations could afford to operate without being operationally resilient is over. Our highly networked societies are becoming increasingly vulnerable to risks that can expand at exponential rates. The frequency of crisis events occurring is only likely to increase as criminal organizations, hostile states, and the effects of climate change place pressure on the weak points of our economies and the systems that support them. To combat these threats, it is worth examining how the best military organizations have adapted to cope with the most extreme crises. The framework of anticipate, detect, deter, withstand, respond, and recover, combined with the tactics that underpin each of its elements, are an excellent starting point for any organization that is seeking to become operationally resilient. To quote the old Latin adage: if you want peace, prepare for war.