Technological Surprise and Resilience in Military Systems

Alexander Kott[i*]

Keywords: Resilience, organizational recovery, technological surprise, mission impact

[*]Corresponding author: alexander.kott1.civ@mail.mil

Introduction

This paper focuses on ways to build resilience and benefit from it when an unexpected adverse event occur. The specific interest is in approaches – preferably supported by historical evidence of success – that can help an organization overcome a significant negative impact on its ability to continue its mission.

To make the discussion more concrete, the paper focuses on a particular class of detrimental events – technological surprises in warfare. A technological surprise in warfare often unfolds as follows. One of the sides in an armed conflict (let's call that side Red) introduces a weapon system that the other side (let's call it Blue) did not expect to see on the battlefield. The new weapon may drastically reduce the ability of Blue to fight Red. As a result, Blue may experience significant losses in personnel, equipment, territory, etc. If Blue is sufficiently resilient, after a period of time it develops countermeasures – often a combination of new tactics and new technical means – that negate the effect of the new weapon, and restore the initial ratio of capabilities between Red and Blue. Two commonly used examples are (1) in the summer of 1941, the introduction of the Soviet T-34 tank which was nearly invulnerable to the German tanks of the time, and served as unwelcome surprise to the Germans; and (2) also in 1941, the use of the German powerful 88 mm Flak gun against the unprepared British tanks in North Africa. (Finkel & Tlamim, 2011)

Following the above description, and for the purposes of this paper, let's define resilience as the ability of a military organization to (a) avoid complete destruction in face of a technological surprise, and then to (b) recover and return to effective performance against the adversary. This definition is consistent with how resilience is defined by the National Academies of Science (2012) and Executive Orders by both the Obama (The White House, 2013) and Trump Administrations.

For study of resilience, technological surprises are particularly convenient cases: the cause (e.g., a new weapon), the effects (the handicap and the losses), and the resiliency-restoring actions (countermeasures) are usually clearly understood, well documented, and often even quantifiable.

For many countries, technological surprise is becoming a growing concern as technology and science are spreading ever broader across the globe. While generally, this is a highly welcome phenomenon,

[i] U.S. Army Research Laboratory, Adelphi, Maryland, USA

Suggested citation: Kott, A. (2018). Technological surprise and resilience in military systems. In Trump, B. D., Florin, M.-V., & Linkov, I. (Eds.). *IRGC resource guide on resilience (vol. 2): Domains of resilience for complex interconnected systems.* Lausanne, CH: EPFL International Risk Governance Center. Available on irgc.epfl.ch and irgc.org.

the proliferation of knowledge about building sophisticated weapons continues to increase the number of states and non-state actors that could spring a technological surprise at a given country.

The limits of risk-based approaches

By their very nature, technological surprises are hardly amenable to risk-management approaches. Risk-based approaches require identification of threat, vulnerability and consequences. The space of modern technologies is so broad and diverse that Red has almost unlimited opportunities to select a particular research and development direction, and to build a novel effective weapon system. If Blue's intelligence services fail to detect the development (a common occurrence), Blue has no way to know the nature of the new Red weapon, and cannot pursue any meaningful risk-mitigation strategies that could help against the future encounter with the yet-unknown weapon.

In theory, Blue might try to undertake a very broad portfolio of R&D programs in order to investigate the capabilities and the countermeasures against all likely future Red weapons. In practice, such an exhaustive exploration and mitigation is unaffordable even for the wealthiest countries.

Therefore, resilience-based approaches are likely to be less costly than risk-based approaches. Instead of (or perhaps in addition to) investing in a very broad (and very expensive) range of mitigation mechanisms against an infinitely large spectrum of possible technological surprises, the country may prefer to invest in skills and assets that would enable resilient responses to an inevitable technological surprise. Although such investments are substantial, they are most likely to be significantly smaller that potentially unlimited spending on avoiding all possible risks.

The limits of resilience-based approaches

Although potentially cost-effective, a resilience-based approach comes with its own set of drawbacks.

First, it does require significant investments. In order to be resilient to a technological surprise, a military organization must invest in developing skills and competencies of its personnel and leaders. It requires investments in expensive training and exercises. It requires investments in assets that are suitable for resilient responses, and in additional, redundant assets that would be used when the primary assets are destroyed or degraded by the adversary. And, all these investments have to be made in addition to investments into more conventional assets and personnel, which are intended for purposes other than resilience.

Second, as mentioned in the introduction, when faced with a technological surprise imposed by Red, Blue may experience significant losses in personnel, equipment, territory, etc. The resilience of Blue might reduce and contain the extent of such losses, but would not eliminate them entirely.

Finally, and perhaps most perniciously, improving the resilience of a military organization creates a temptation to neglect other preparations for facing the risk of a technological surprise. Similarly, a temptation may exist to remain complacent with an existing collection or technologies or the level of personnel skills. Faced with tight budgets, a decision-maker might be inclined to argue that certain upfront investments in material and personnel for reducing the risk of a surprise are unnecessary because "we will face a technological surprise anyways, and then we will have to improvise some resilient responses, so why do we need to invest in any new weapons at this time?"

Effective resilience in historical examples

Historical experiences with successful adaptations to technological surprises suggest several key elements common to such successes. The following steps (not necessarily sequential, but often taken in parallel) are commonly observed when a military organization (let's call them Blue) successfully – or partly successfully – recovers from a technological surprise.

First, Blue recognizes rapidly that its operation is degraded by a technological surprise, e.g., by a novel Red weapon system. Then, Blue takes agile actions in order to minimize the immediate impact of the surprising threat on Blue's current operations. This usually requires Blue to accept a degree of further deterioration in performance of the Blue organization. One approach is for Blue to isolate itself from the Red threat, e.g., by creating a distance between Blue and the threat, or retreating to well protect positions. For instance, in the battle of Kasserine Pass (February 1943, Tunisia), having been surprised by the effectiveness of German forces, the US Army and its allies retreated to defensive positions in order to minimize the impact of the German forces, to regroup and await reinforcements (Finkel & Tlamim, 2011, p. 271)

While holding off Red, Blue works rapidly to identify weaknesses and vulnerabilities of Red's novel technology. This often involves the need to rapidly perform a forensic analysis of the known engagements with the threat, and to hypothesize, design and execute a series of experiments. These often happen organically, as various subunits of the Blue force try a variety of desperate expediencies to fight back against the Red threat. For instance, in 1943, surprised by the German acoustic torpedo against Allied ships, the British engineers rapidly improved a device that was towed behind the ships and caused the torpedo to explode harmlessly (Handel, 1987). Similarly, in October 1973, when the Israeli air force was surprised by the new Syrian SA-6 anti-aircraft missiles, a scientist at the Rafael Corporation rapidly developed a way for the Israeli planes to jam the radars of the missile batteries. (Finkel & Tlamim, 2011, p. 175)

When the Blue force identifies a vulnerability or weakness of the Red technology, it proceeds to converge on a small set of tactics and techniques that seem to be effective against Red. If feasible, Blue may also develop and implement technical counter-measures against the Red surprise technology. Blue rapidly disseminates instructions for executing these tactics or applying technical countermeasures to all relevant sub-units; obtains additional equipment and performs training as needed. For instance, in the battle of Kasserine Pass, the US and Allied Forces recognized that the German forces would be vulnerable to artillery, and reinforced themselves with experienced artillery units. (Finkel & Tlamim 2011, p. 271)

Finally, the Blue force aggressively and decisively applies the new tactical or technical counter-measures, in conjunctions with any other effects available, against the Red force. This may defeat the Red threat, may reduce or eliminate its efficacy, and may enable the Blue organization to return to near-normal level of performance in its operations.

Desired organizational characteristics

Not every organization is capable of successful execution of approaches described in the preceding section. Let's consider – again, based largely on historical examples -- some of the key characteristics that help an organization to succeed in resilient adaptations to technological surprise.

A particularly widely recognized characteristics of such nature is flexibility: the ability of the organization to change its organizational structure, techniques, procedures, and other forms of its

operation, even if such changes are drastic and contradict established norms and past experiences. For instance, although in 1941 in North Africa the British possessed excellent anti-aircraft guns, the inflexible regimental culture prevented them from using the guns against the German tanks. (Handel, 1987)

Another important characteristic is agility: the organization must be able to perform its actions rapidly and to eliminate any barriers that may cause a delay in decision or execution. This often requires the culture of delegating the authority to the lowest echelon of the organization and encouraging initiative of even the most junior members of the organization. For instance, when in 1986 the Afghan guerrillas started to use Stinger missiles (a technological surprise) against Soviet helicopters, the lack of independent initiative and creativity among the Soviet junior officers was a significant factor in slow (about 18 months) adaptation of the Soviets forces. (Miller, 2014)

Both agility and flexibility must be supported by effective intelligence: the ability of the organization to obtain, analyse and disseminate intelligence about the technological surprise – e.g., the novel weapon system and its effect of the organization's operations and assets, or a new tactical or strategic context – completely and efficiently, in spite of the stress and disruption caused by the threat. For instance, when in 1941 the Germans used their 88 mm gun against British tanks, the British failed to collect sufficient intelligence about the events, and remained unaware of the German weapon for several months after its initial use in a battle. (Handel, 1987)

Last but not least breadth and diversity are vitally important: the organization should combine a diverse set of technical and cultural competencies, as well as assets that are capable of a variety of functions under different conditions. This is necessary in order to re-orient an organization effectively against the technological surprise and to combine the competencies and capabilities in novel ways. For instance, when facing Egyptian anti-tank Sagger missiles – a technological surprise – the Israeli homogenous tank units were unable to adapt until they were belatedly diversified with infantry and artillery. (Miller, 2014)

Conclusions

Analysis of technological surprises in warfare – particularly the study of historical cases of such surprises – is uniquely valuable for identifying the advantages and limitations of resilience-based approaches, the approaches to conducting resilient activities after an unwelcome surprise, and the characteristics that an organization must foster for the sake of improving its resilience.

Historical experiences offer insights into several key elements – typical activities and ways of executing them – that are common to successful adaptations to technological surprises. However, to build capabilities for effective execution of such activities, an organization must develop several critical characteristics. These include flexibility, agility, effective use of intelligence, and breadth and diversity.

While resilience-based approaches are likely to be less costly and more practical than risk-based approaches, leaders of an organization must recognize that improving the resilience of an organization must not lead to neglecting appropriate measures for reducing the risk of a hazardous event.

Annotated bibliography

Finkel, M., & Tlamim, M. (2011). *On flexibility: recovery from technological and doctrinal surprise on the battlefield*. Stanford University Press. Argues that recovery from surprise depends largely on a characteristic of an organization the authors call flexibility. Proves the assertion by considering multiple historical cases of recovery from surprises.

Handel, M. I. (1987). Technological surprise in war. *Intelligence and National Security, 2*(1), 1-53. Offers a typology and conditions of technological surprises, as well as means to enhance or counter the technological surprise; uses a number of historical examples.

Miller, J. H. (2014). Strategic culture as the basis for military adaptive capacity: Overcoming battlefield technological surprises. CUREJ: College Undergraduate Research Electronic Journal, University of Pennsylvania. Uses three in-depth case studies of historical events, connected largely to technological surprises, in order to identify cultural and organizational traits that support resilient adaptation.

National Research Council. (2012). *Disaster resilience: A national imperative.* Washington, DC: The National Academies Press. https://doi.org/10.17226/13457

The White House. (2013). Presidential policy directive: Critical infrastructure security and resilience. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil