EVOLVING THREAT

Different adversaries present different combinations of threats

Picture credit: Crown Copyright

Jules Werner *considers the importance of security and defence in the complex threat landscape*

It would be a mistake to assume today that multi-domain threats are limited purely to an all-out, conventional 'shooting war'. There are now numerous examples of conventional and asymmetric adversaries; these are characterised by an ability to blend new technology and the tactics of irregular warfare into new complex threat combinations.

Since the disastrous consequences of direct conflict are well understood by NATO, its allies and its peer/near-peer adversaries, we look to the shadowy, chaotic 'grey zone'. This is the domain in which states – both large and small – compete through underhanded strategies that include proxy forces, economic coercion and information operations.

Unconventional warfare has existed for as long as there has been imbalance between opposing sides. However, today's non-state actors, extremist organisations, proxy forces and other asymmetric aggressors exploit opportunities that never existed before. This is due to changes in the geopolitical landscape, lessons learned from direct conflict with the West and a willingness to rapidly evolve tools and tactics. Such combatants have shown, repeatedly, that they can simply outlast conventional forces – winning by default. Just look at Afghanistan, Vietnam and Iraq as obvious examples. Amidst all of this uncertainty and deniability, we can see the emergence of multi-threat, complex situations. Gone are the days in which only a peer or near-peer competitor could present a true complex threat.

Different adversaries present different combinations of threats. When one combatant plays by conventional rules of war, against one that doesn't, it can be a protracted conflict to achieve the goals through legal warfare means. Technology has originated new varieties of threat, increasing the variety of attacks to expect and consequentially prepare for.

Complex threats demand higher levels of interoperability, across domains and allied forces. Receiving a complex, simultaneous attack across multiple domains and partners requires each operational domain (and partner nation) to understand capabilities that were traditionally outside of their remit. One of the biggest issues with this scenario is partner nation interoperability, especially in areas like communication, which can be a real challenge due to the different types of technology used across a multi-nation force. Problems also stem from differing weapons systems, and a lack of interchangeability in data and stores.

This creates dilemmas: multiple, complementary threats that each require a response, thereby exposing vulnerabilities to other threats and producing the real possibility of being overwhelmed. Complex threats can force an opponent into multiple dilemmas across multiple domains. And a combination of multiple dilemmas (as opposed to superiority in any single domain) can press the overall, decisive advantage. So what are some of the threats that we might expect to come from asymmetric adversaries?

KNOW YOUR ENEMY

The importance of knowing one's enemy has been reiterated since Sun Tzu wrote *The Art Of War*, but the modern use of proxies can make it a difficult principle to follow. For centuries, adversaries have employed a variety of proxies to do their 'dirty work'. Such forces allow for plausible deniability and may also possess the capability to employ multiple means of attack. Today, this is further aggravated and influenced by international terrorism, failed or failing states, violent organised crime, populism and other often interrelated factors.

For a developed nation, deploying its own army overseas is expensive. In return for putting their lives on the line for their country, soldiers can very reasonably expect a salary and a pension – or compensation for their families if killed in service. To save money, an unscrupulous state may outsource its military operations to the soldiers of less developed nations, or private militias, who will do the job for less. There is also a political factor to consider with proxy forces. News of sovereign troops being killed in unpopular foreign wars can quickly turn the tide of public opinion. A government may therefore use proxies to make a conflict more palatable to citizens. Using proxies also makes it easier to conceal intent from other nations or deny involvement altogether. It can also provide cover for aggressive and unethical tactics that contravene international law, without those actions being attributable.

Multiple proxy forces in operation at any one time further increase the likelihood of multi-domain threats. Many such forces are highly motivated by identity politics (for example a focus on ethnicity, religion and culture). They often possess a 'home field advantage' – along with training and equipment that, if not for their state sponsors, would be well beyond their means. They are not to be taken lightly and, because of their commitment to their cause, are less receptive to de-escalation.

What's the difference between an insurgent and civilian? Decades of conflict later and in many cases, we're still unsure. Examples include irregular militias who wear uniforms in conflict when it suits them or insurgents who operate and then melt back into the populace that they came from. Such adversaries may not wear camouflage, but they blend seamlessly into the human terrain of the zone of conflict. The use of proxies, perhaps deploying in unmarked uniforms or posing as allies or civilians, may form part of a concerted attempt to make the battlespace more confusing and ambiguous to defending forces.

Advances in commercial, off the shelf (COTS) technology now affords attackers with a range of cheap and readily available unmanned craft. Opponents go after UAVs, sea-based drones, land-based unmanned vehicles and more. Such devices come in a huge variety of configurations and with a range of uses. This will only increase as the technology becomes cheaper, more capable and more ubiquitous. Even space-based threats are a future possibility – with an increasing reliance on space-based assets, the proliferation of cheap micro satellites and the price to launch continuing to fall.

THE CHALLENGE LIES IN BEING ABLE TO DEFEND AGAINST MULTIPLE THREATS AT ONCE

Approximately 1,000 commercial flights were diverted or cancelled across three days in December 2018, amid reports of a COTS drone flying in London Gatwick airport's airspace. The incident affected around 140,000 passengers, cost the airlines an estimated £50-million, and produced a policing bill of almost £800,000. It's impossible to put a figure on the total economic impact of the disruption – but it was felt domestically, and at the airport's many destinations. The effect of the incident can be likened to a Distributed Denial of Service (DDoS) attack played out in the physical world. Its deniability is underscored by the fact that no drones were ever seized and no criminal charges brought.

The same commercial technology advances also drive the proliferation of 'swarm' capable attackers. Modern swarming uses developments in communications and navigation technology to augment numerical superiority via co-ordination. Swarming is very often encountered in asymmetric conflicts where one side has a conventionally superior (but not necessarily numerically superior) force. Swarm tactics use numerous, fast-moving forces that can quickly converge upon an adversary from multiple angles – using target saturation to gain the advantage. This overwhelms the target's ability to respond in time to the sheer volume of threats now confronting them. Swarm devices are often rudimentary or easy to access machines, using their numbers over sophistication. Last year for example, multiple Iranian boats ran alongside the aircraft carrier USS Abraham Lincoln as she sailed through the Strait of Hormuz.

This is done in order to maximise the ability of the swarm to attack simultaneously and retreat quickly. Such threats can come from unmanned craft or manned ones, like small fast attack craft boats at sea. The challenge here lies in being able to defend against multiple threats at once, with munitions specifically designed to handle swarms, as many ship-based weapons for example are not suitable for this type of defence.

> **THE IMPORTANCE OF KNOWING ONE'S ENEMY HAS BEEN REITERATED SINCE *THE ART OF WAR***

Hybrid warfare tactics evolve rapidly as nimble, underdog opponents apply the very real lesson of 'evolve or die'. Such fighters are unconventional and unrestricted – they lack the bureaucracy of conventional military forces and possess the motivation and means to change very quickly. As such, threats can and should be expected to evolve, and to come from where we least expect them. Doctrine and training should be comprehensive and reflect this new reality

Many in the West haven't expected to face a true complex threat since the collapse of the Soviet Union. Asymmetric opponents may seem to be all there is right now, but peer and near-peer multi-domain conflicts haven't ended either. Consider The Falklands, Desert Storm and Desert Shield as more recent examples. And, looking to the current day and into the future there is the recent re-emergence of peer or near-peer adversaries. The rise of these credible, multi-domain threats drives Western forces to examine how well they currently integrate air, land, sea, cyber and space capabilities.

Just as adversaries have proven their willingness to quickly evolve, so should the West. Properly tackling complex threats demands greater interoperability between allied nations and warfighting domains. As such, training for complex threats requires a multi-domain, multinational approach that considers the many simultaneous threats that enemies both large and small may present. By training in environments that replicate any of the above scenarios of complex threats, forces can better equip themselves to counter these growing threats. So, as the old adage says: "Train like you fight" ●

Jules Werner is Business Development Manager at QinetiQ. Prior to joining QinetiQ, Jules was the head of Physical Training at the Royal Navy Air Station, Yeovilton, responsible for all aspects of physical training, planning and management to meet defence policy directives.

Drones and UAVs come in a huge variety of configurations and with a range of uses

Picture credit: US Dept. of Defense