Picture credit: AdobeStock

INTO THE GREY

Dave Dixon *explains why all-source fusion is critical to combating hybrid and grey-zone threats to security*

All-source fusion software has always been a helpful tool in creating clarity from complexity. Hybrid warfare means that these tools are now critical as the complexity and dynamic nature of the conflict exponentially increases the threat.

The existence of hybrid threats to national security is not new, yet we are seeing them grow in their sophistication. Intersec readers will be family with the concept. "An interplay or fusion of conventional as well as unconventional instruments of power and tools of subversion," says NATO. These tools are blended in a synchronised manner, it says: "to exploit the vulnerabilities of an antagonist and achieve synergistic effects".

Because they are often unconventional, these competitive interactions can occur among state and non-state actors, such as terrorist organisations. The tactics are used outside the theatre of war to target political institutions, influence public opinion and undermine security. Falling short of formal welfare yet more aggressive than peacetime competition, these activities have become known as 'grey-zone operations'.

Such are their complexities, it has become profoundly challenging to detect, analyse and respond to the many and various methods used often simultaneously by these actors. As I will explain here, all-source fusion software is being adopted widely to meet this challenge. It is technology that aims to bring clarity where there is chaos and confusion.

Throughout history, from ancient times to the present, we see the use of hybrid tactics. The UK, the United States and France, for example, frequently used them in the last century, often referring to them as 'covert' or 'special operations'. In this century, these activities have not been so covert. Consider the headlines on the attempted assassination of Sergei Skripal on the streets of Salisbury in 2018 and the international debate on the tech firm Huawei as an instrument of Chinese state power. The media has recently reported on the conversion by Israeli forces of basic communication devices into bombs to attack Hezbollah operatives. "It is a reminder that – in war, and especially hybrid war – anything can be used as a weapon," reported Sky News' security and defence editor.

The integration of financial intelligence with existing verticals is reshaping how analysts understand and respond to hybrid threats

Notably with the conflicts in Ukraine and Middle East, we see today how sophisticated and multifaceted the threats to national security have become. Globalisation and technological advancement are behind this increasing complexity, making modern states more open, porous and vulnerable. "What is new about attacks seen in recent years is their speed, scale and intensity, facilitated by rapid technological change and global interconnectivity," says NATO. Twenty-first century hybrid warfare has expanded beyond the physical and now resides firmly in the digital and financial spaces. The threshold of war has never been harder to define and such tactics have helped to level the playing field.

"Ultimately, the deliberate application of hybrid tactics, techniques and capabilities is intended to create strategic, operational, and/or tactical dilemmas for an opponent," say Peter Dobias and Kyle Christensen, for Connections: The Quarterly Journal. "Remaining below the threshold of the use of force and avoiding head-to-head confrontations with an opponent has enabled weaker states to challenge stronger states because they no longer need to engage superior adversaries in a head-to-head confrontation."

The authors of this paper refer to hybrid threats as a: "continuum of conflict" or: "competition continuum" in which the area between peace and war is simply an area of conflict by other means. What we are seeing, they say, is a multi-dimensional battle space.

So, how do we manage this multi-dimensional threat? The first step, surely, must be to gather as much useful information about it as possible.

In the context of grey-zone operations, the need for comprehensive intelligence is acute. We witness the havoc such activities play, in the meddling in political elections to the hacking of national databases. They thrive in ambiguity, relying on misinformation, cyber attacks, financial subversion and other tactics that blur the lines between war and peace. In these scenarios, our ability to gather together disparate but related fragments of information and make sense of them has become critical.

To this end, technology alone cannot solve the complexities of grey-zone and hybrid warfare, but it plays a central role in addressing them. With hybrid threats being so vague and hard to define, technological solutions that are able to fuse different sources of intelligence have become increasingly important. These 'all-source fusion platforms' are uniquely equipped to pull together disparate intelligence, from SIGINT (signals intelligence) and OSINT (open source intelligence) to FININT (financial intelligence), helping to create a more coherent operational picture.

Conventional vertical platforms are highly effective at analysing specific intelligence streams. For example, SIGINT platforms can track patterns in electronic communications, while OSINT tools monitor propaganda and disinformation on social media. However, in a hybrid conflict, such as the Ukraine war, isolated intelligence is insufficient to manage the fluid and interconnected nature of modern threats. Here is where all-source fusion software becomes essential.

These software solutions, such as i2 Group's Analysis Studio, pull together all factors and assimilate the information to make sense of it. They operationalise the data, using visualisation technology to help you make sense of the threat and give options to help you address it.

Here are some of the key functions of all-source fusion platforms. Data fusion: combines information from multiple sources, including financial data, law enforcement databases, intelligence reports and open-source intelligence, to create a unified threat picture. Threat assessment: analyses information to identify potential threats, including financial indicators of adversarial activity and assessing their severity. Intelligence dissemination: sharing intelligence information with relevant agencies, ensuring coordinated responses to threats.

MANY ADVERSARIES ARE UTILISING BLOCKCHAIN TECH TO RAISE, MOVE AND LAUNDER MONEY

Collaboration: promoting inter-agency co-operation by fostering information sharing across different intelligence streams. Analysis and prediction: using advanced analytics to predict future threats, including financial subversion and hybrid attacks.

In essence, all-source fusion software serves as a central hub for intelligence gathering and analysis, providing critical information to decision-makers and helping to protect national security. It gives a holistic view of complex situations.

To give an example of its use, we can look at how it is being employed to manage the evolution of financial intelligence (FININT). Financial flows have become a critical source of information, not only in tracing adversary activities, but also in disrupting their operations.

As adversaries are forced to circumvent established anti-money laundering (AML) and counter-terrorism financing (CTF) protocols, many are moving away from fiat currencies, utilising blockchain technologies to raise, move and launder money. Blockchain has therefore become as significant an intelligence source as traditional ones, such as SIGINT and OSINT. In response, all-source fusion platforms have expanded their capabilities to monitor blockchain transactions alongside the more conventional intelligence sources. The integration of financial intelligence with existing verticals is reshaping how analysts understand and respond to hybrid threats, particularly those that operate outside of conventional systems.

In 2022, after the outbreak of the war in Ukraine, the Royal United Services Institute for Defence and Security Studies published a paper, called

The Future of Open Source Intelligence for UK National Security.

"The complex picture of the present-day intelligence environment indicates the importance of all-source fusion, which produces a reinforcing relationship between classified sources and PAI,'" said the report. "It is no longer a matter of selecting one form of intelligence or the other – in isolation, they will not be enough to meet the increasing demands being placed on the UK national security community by the sheer scale of data."

A more agile approach to intelligence gathering and analysis was required, that advanced the cause of integrated all-source analysis, said the report's authors.

IN WAR, AND ESPECIALLY HYBRID WAR, ANYTHING CAN AND SHOULD BE USED AS A WEAPON

Before the conflicts in Eastern Europe and the Middle East, the importance of all-source analysis was becoming clear. "How well and how rapidly the intelligence community integrates emerging technologies into all-source analysis will be vital to its ability to generate timely, relevant and accurate advantage over capable rivals,'" said Brian Katz, a fellow in the International Security Program and Center for Strategic and International Studies (CSIS) and research director of the CSIS Technology and Intelligence Task Force.

As of late-2024, two-and-a-half years into the Ukraine conflict, it is clear that all-source fusion platforms are making a significant difference. As the conflict in Ukraine continues, every NATO member state must be prepared for a sovereign disruption or invasion. They must understand the hybrid threat, specifically how the threat vectors and actors are operating and evolving leading up to a potential kinetic action. Facilitated by inter-agency co-operation, all-source intelligence solutions have adapted to "working with" data, through more functionally rich integrations that respect the need for compartmentalisation, while facilitating near real time interoperability between defence, border control and security.

By integrating intelligence from multiple domains, including the rapidly evolving world of financial intelligence, these platforms have enabled defence forces to better understand and respond to complex hybrid threats. As adversaries continue to operate in the grey zone, leveraging both conventional and unconventional tactics, the ability to fuse and analyse data across all domains will remain essential for national security ●

Dave Dixon is Vice-President of Business Development at i2 Group.

21st-century hybrid warfare has expanded beyond the physical and now resides firmly in the digital and financial spaces