

The transformation of intelligence services in light of the war in Ukraine

YVAN LLEDO-FERRER

After two decades marked by the “war” on terror, the war in Ukraine constituted a brutal reawakening of power struggles and conventional warfare on European soil. While the “war” on terror created a lasting impact on the framework and methods of intelligence services, we are already seeing certain changes starting to emerge in response to the war in Ukraine. This allows us to anticipate the profound transformations that these services are set to undergo.

On 15 August 2021, the fall of Kabul occurred – somewhat symbolically – mere weeks before the commemoration of the 20th anniversary of the 9/11 attacks. The US’ retreat from Afghanistan marked a clear change of priorities within the American administration; the latter considered that the terrorist threat had been contained to an acceptable level and that the “war” on terror could not, by definition, be won.

Nevertheless, the last twenty years have profoundly marked the framework and methods of intelligence services, which have dedicated a great deal of their resources to counter-terrorism. During this period, the French intelligence community was articulated as a result of the “knowledge and anticipation” function of the 2008 French White Paper on Defense and National Security. What’s more, the creation of France’s National Intelligence Coordination in 2009 – which became France’s National Intelligence and Counter-Terrorism Coordination in 2017 – brought the notions of intelligence and counter-terrorism closer together, despite the former being broader than the latter.

When faced with non-State actors, capable of blending in with the local population without requiring the latter’s support, intelligence services began to implement targeting methods to identify and eliminate terrorists, while limiting collateral damage.

Intelligence services also developed the ability to collect and analyze immense quantities of technical data, of which only a fraction proved relevant for

fighting terrorism. The Snowden case brought to light the so-called “mass surveillance”, designed for a context in which the “enemy” becomes a shifting concept; as the target is an individual who spend most of its time as a common citizen, yet can devote part of its time to preparing an attack against a nation’s interests.

From the very beginning of the war in Ukraine, intelligence services have approached the situation according to a framework largely inherited from the “war” on terror. However, the skills and methods required to face this new reality are quite different and are not easily transferable.

Open source intelligence (OSINT) has played a key role in the war in Ukraine. Unlike terrorists, massive movements of troops and military equipment are not particularly discreet, making them easy to detect through analyses of both social networks and commercial satellite imagery. Naturally, this form of intelligence – which is legal, abundant and inexpensive – can be complemented with classic technical intelligence practices.

The United States extensively declassified its intelligence analyses, which it shared with its allies and later released to the media. This was done as part of the “integrated deterrence” concept described in the United States’ National Security Strategy. According to this principle, it is of vital interest for the United States to deter external aggression – beyond nuclear and conventional deterrence – through the integration of all areas of power, including intelligence. The aim of the US declassifying its

intelligence was to deter Russia from invading Ukraine, by depriving it of the element of surprise and thereby influencing its cost calculations¹.

The war in Ukraine is certainly not the first case of intelligence data being declassified. However, these new circumstances are truly different in nature. Until now, declassified intelligence data was descriptive, *ex-post* (e.g. the [use of chemical weapons in Syria](#)) and aimed at legitimizing future action by the declassifying State (e.g. [Operation Hamilton](#)). However, in the Ukrainian context, intelligence data is predictive, *ex-ante* and aimed at dissuading another State from taking action. Despite French intelligence's efforts to [strengthen its predictive capabilities](#) at the turn of 2015, it remained unable to anticipate Russia's intentions.

From a purely pragmatic point of view, this predictive strategy is a win-win. If the predicted event occurs, it validates the initial analysis *a posteriori* (that being said, the possibility of a self-fulfilling prophecy cannot be ruled out). If the event does not occur, the deterrent effect is deemed effective – instead of leading to the conclusion that the initial prediction was based on a flawed analysis.

Thus, this new strategic environment is sure to have a permanent impact on the field of intelligence. While it is still too early to identify all of the changes that the war in Ukraine will bring about within the intelligence community, several trends can already be highlighted.

Firstly, we are witnessing the **return of political intelligence**. This form of intelligence is destined to predict other States' decisions, in order to give political authorities a comparative advantage. This implies broadening the scope of intelligence analyses in order to include all of the parameters that are likely to influence decision-making, be it in the cultural, political, economic, social or military spheres. In order to understand these various influences, detailed knowledge of other countries' strategic cultures and histories will prove essential. Building stable and coherent career paths in the field of intelligence has become a matter of urgency, as establishing and supporting long-term analytical expertise is of the essence. In this regard, relations with the academic world need to be developed in order to take full advantage of the ecosystem that has been set up over the last few years (France's Intelligence Academy, the [College of Intelligence](#) in Europe, Interaxions and the Intelligence Campus).

1. Surprisingly, this deterrence strategy turned out to be a failure, one that was nonetheless overshadowed by the success of the intelligence forecast.

The waves of expulsions targeting Russian and Western intelligence officers under diplomatic cover require us to **rethink the way human intelligence (HUMINT) is gathered**. Conducting intelligence in Moscow has never been an easy task, yet the working conditions of intelligence officers on the ground are only going to get worse, thereby forcing intelligence services to take their methods to a new level of creativity. On the other hand, Russia and its intelligence community will also adapt to this new reality, forcing Western counter-intelligence services to readjust their methods in turn. The [Skripal case](#) demonstrated Russia's ability and determination to carry out lethal actions. Depending on how the war unfolds, counter-intelligence services may well be faced with an escalation in Russian clandestine actions on European soil.

The war in Ukraine also highlights the importance of maintaining a technological advantage. Intelligence agencies will have to play an enhanced role in **protecting industrial know-how from foreign threats**. It should also lead to **the facilitation and further securing of arms exports** to help finance the next generation of equipment, thereby allowing France to maintain an independent and top-level Defense Technological and Industrial Base (DTIB).

The adaptive measures we take today will determine how effective intelligence services will be down the line. Given the time required to instate profound legal reforms, it would be a mistake to launch a reform based on the 2022 threat environment. Instead, the priority should be to support intelligence services in their ability to adapt to an environment in which unpredictability will likely be the only predictable feature. ■

Yvan Lledo-Ferrer, PhD, is a research associate at IRSEM. He has served as an advisor to France's Ministry of the Armed Forces and Ministry of Foreign Affairs.