Denys Kolesnyk

Doctrine Demands Information Warfare Components

Recent massing of Russian troops close to the border with Ukraine and escalation of the hostilities in Donbas have again attracted the attention of the international community, focusing once more on the *de facto* unresolved conflict being waged between Russia and Ukraine. In parallel with a reignition of the conflict, so both information warfare operations and propaganda efforts have again begun to blossom.

Since the Russian annexation of Crimea in 2014, the notion of disinformation – or its rather pejorative 'fake news' definition – has entered our daily vocabulary to describe false information, ranging from the 'crucified boy' in the Donbas to interference in the 2016 US presidential election and even the referendum in Catalonia the following year.

In 1989, as Soviet troops withdrew from Afghanistan, an article appeared in the US Marine Corps Gazette, describing the fourth generation of warfare, invoking such termas as 'information overload' and suggesting psychological operations could become *"the dominant operational and strategic weapon."*

The Soviets were well-accustomed to the use of 'active measures,' having deployed them against the West during the Cold War, but the notion of 'Information Warfare' (IW) now migrated to Russia from the US. Russia began work on the issue in the 1990s, becoming one of the first countries to adopt an Information Security Doctrine as early as 2000, updating it in 2016.

Western and Russian approaches to IW differ. For instance, for Russia, the 'information space' is where information and cyber operations occur, where cyber is used as a tool. The West, on the other hand, remains mostly cyber-oriented, with NATO formalising the inclusion of cyber as an 'operational domain' in 2016.

But, though the US, Russia and China have been working on IW for decades, Russia's immediate neighbours and other European states have only recently started to pay attention to it.

For instance, Poland's National Security Bureau (BBN) established a draft Information Security in 2015, a year after the Russian 'blitzkrieg' in Crimea. However, the document was never adopted, due in part to it being an election year, which brought new leadership to power. Additionally, according to several experts, it required additional work. That work was later undertaken, prioritising the National Security Strategy (NSS), which was then updated in May 2020, an update in which Poland decided to separate cybersecurity from the information space. Given that Poland considers Russia as one of the key threats to its national security, such an approach can be considered rather smart.

On the other side of Europe, France has made significant progress in understanding Russian IW since the 2017 presidential election was marked by the 'Macron leaks' and aggressive Russian disinformation. The French Strategic Review was published in the same year. This document identified the new climate of hostility in the world, noting particularly the resurgence of Russia. The issue of cybersecurity received particular attention, with two important points reflected: the difficulties in attributing cyberattacks to their origintors or perpatrators; and the fact that *"some [cyber] attacks, due to their scale and gravity, could be qualified as armed aggression."* Even though the word 'disinformation' appeared for the first time in the official French lexicon in this document, it nontheless reflected the way in which the French approach to IW remained cyber-oriented.

The logic of this was echoed, in 2019, with the publication of two major documents: Offensive Cyber Military Doctrine and Defensive Cyber Struggle Ministerial Policy. The Offensive Cyber Struggle (LIO) mentions *"countering disinformation,"* albeit rather abstractly, in the context of military operations involving troop deployment. Interestingly enough, it resonates with the concept presented by Russian Colonel Sergey Komov in the 1990s, in which IW was seen as an integral part of kinetic conflict.

The Strategic Update *(actualisation stratégique)* was unveiled last January. The objective was to review and evaluate the assumptions made in the 2017 Strategic Review, with most of them being confirmed in the new document.

It notes, without providing aditional contenxt, that Russia is continuing *"its military modernisation and its disinformation campaigns"* on Europe's eastern and northern flanks. The document further acknowledges the importance of the information space, since it indicates that *"the information field, penetrated by digital means, has become a key part of conflicts, affecting forces, institutions and populations."*

But it also notes, however, that the manipulation of information is *"a practice that goes against […] democratic values,"* hinting that France is not considering drastic action in the information space, contrary to the cyber domain.

As for Russia, it announced that work is being conducted on the new National Security Strategy in February 2020 but the document, which promises to include an entire chapter on IW, is yet to be unveiled.

On a doctrinal level, IW is becoming 'a must' for every developed nation. We can expect more emphatic differences in the approach to 'information' and 'cyber,' between the West on the one hand, and Russia, China and Central-Eastern European states on the other.

*Based in Paris, **Denys Kolesnyk** is an expert in information warfare, with extensive knowledge and experience of the current conflict in Ukraine.*