Intelligence College in Europe
Collège du Renseignement en Europe

Webinar European security Challenges

Conclusions summary – March 2021

Due to the health situation experienced since March 2020, the Intelligence College in Europe has had to question traditional methods of exchange and reflection and find new ways of dialogue.

With the support of the Steering Committee, three member countries (Italy, Romania and Finland) proposed a seminar, under the format of an interactive webinar, dedicated to the new European security challenges for intelligence services.

This webinar addressed three topics, which constitute designated shared challenges from the part of all members:

- **The impact of digital technologies on national security, based on the work carried out by Dr Donatella Sciuto and Dr Stefano Zanero from the Dipartimento di Elettronica, Informazione e Bioingegneria from the Politecnico of Milano, Italy. Developments in this field require our countries to adapt quickly in order to remain in this "race for innovation".**
- **Propaganda, disinformation, covert information operations, referring to the work of Dr Cristina Ivan from the "Mihai Viteazul" National Intelligence Academy. These concepts, far from being purely theoretical, raise questions about the role of the intelligence services, their perception within our societies, their dialogue also with our national and European decision-makers, as well as with civil society.**
- **Hybrid Warfare, based on an academic report in Finland. Although this is not a new phenomenon, its use is growing rapidly in a world marked by the reduction of "conventional" conflicts, thanks to technological developments.**

Several member countries helped to broaden the perspective of the initial contributors by sharing with members their national views and strategic analysis of the discussed subjects. The various contributions enabled a global discussion of points of view marked by the specific threat analysis prisms inherent in each country. In this sense, this webinar contributed to share concepts and analyses. It was also an opening to consider these sometimes diverging readings of threats, in order for each member to better understand its European counterparts. This publication is a summary of these exchanges.

We would like to thank all those who took an active part in the success of this first webinar. This success and the fruitful discussions over these three topics on which members share, for the most part, similar views, pave the way for further exchanges within the College. The topics, which are in line with the theme of the British Presidency in 2021 (*Fusing intelligence and policy to build resilience in the 21st century*), will most likely be addressed again, and completed with yet more subjects on which members will be able to confront views and strengthen their mutual strategic understanding.

The impact of digital technologies on national security

Digital technologies, declined at various levels (space, quantum computing, artificial intelligence (AI), machine learning (ML)) are altering the national security landscape and creating new potential angles of attack. They have a profound impact on economic and social balances and raise questions in terms of law. They have resulted in a hyperconnected society which will intensify with the deployment of 5G and new satellite constellations.

The evolution of digital technologies' impact is characterised by the following aspects:

- Technological advances will enable a wider range of actors to acquire sophisticated capabilities that were previously available only to well-resourced states. The civilian sector, following market logics, drives technology and can provide even more resources.
- Digital technologies may reshape the relationship between capital and labour in the world economies, and the relationship among those economies in turn.
- While they provide new tools for intelligence services, they also create new threats. AI and ML may be used by the intelligence community to assist in determining the truth, it also provides the means for adversaries to create and spread convincing false information. Machine learning is also susceptible to adversarial attacks. In many intelligence and defense settings, a capable adversary might be willing and able to attack the systems either through poisoning of training data, or through careful shaping of the data subject to analysis.
- Even if individuals expose certain information relative to their private life on the Internet, society is paradoxically becoming increasingly sensitive to the issue of sharing personal data. Consequently, the concept of privacy by design according to which the processing of each piece of information must offer a high level of protection for personal data has become prominent. Thus, the main issue emerges: access to clear data. Indeed, data, as an important source for intelligence services, is developing at high speed, but it will be increasingly difficult to detect the relevant decrypted data.

Can this game-changer generate a redistribution of military power at the international level? It should be noted that if the military was a key driver in technology and inventions on a practical level, on the more strategic level, profound inventions have initially always been of a civilian character. In addition, although AI is used today in offensive computer warfare as well as defensive computer warfare, the technologies in use are still very modest and will not respond to such a forecast for a long time to come.

In conclusion, unanimously, the paradigmatic shift that is decreasing control by states on technology, its development, export and exploitation, requires the Intelligence community to become more agile and innovative to deal with an ever more volatile world. But as one researcher pointed out: What's new in the fact that the intelligence community has to keep up with developments? This implies in particular the need for European sovereignty in digital technologies but also of a legitimisation, by law, of the intelligence services' action, in particular with regard to access to data.

Propaganda, disinformation, covert information operations

Propaganda, disinformation and covert information operations have gained increased attention in the past years in the West, from both security institutions and society at large. In the field of informational interference, we can distinguish three levels of information manipulation. They range from the classic political and diplomatic propaganda offensive, often endorsed at the highest level of the foreign state, to covert information operations and hybrid warfare. Between the two lies a wide span of disinformation techniques. This may consist of both relaying and amplifying current events in order to give more echo to a previously defined state narrative, thus helping to strengthen its credibility, or of concerted actions and messages aimed to disrupt, seed distrust and turn an enemy state's population against its own governmental authorities.

Propaganda represents an intensive manipulation of information to influence perceptions and the ability of the target audience to make objective decisions. It does not exclude facts, but it presents them in convenient and sometimes distorted ways so that it can persuade at all costs. The aim is to obtain strategic advantages, political capital, even financial gain, or simply to boost the image of a ruler. It must be perceived as an appeal to rationality or as information that sheds light on a new perspective on a given problem. It often appeals to a heavy load emotional baggage which dismisses the rational understanding of facts.

Disinformation refers to an entire array of tactics and strategies used to propagate false, inexact or out of context information that have been hijacked from their real meaning. Its intention is to provoke damages and profit and it can severely affect democratic processes, national security, and social cohesion. If propaganda is accomplished via state institutions whose ties are theoretically easily traceable, disinformation operations take a great deal of effort in covering primary sources. Disinformation represents a form of propaganda whose main purpose remains illegal and clandestine.

A hostile information operation can be defined as the array of covert or semi-covert actions that make disinformation possible and enhance its effectiveness. They include a systematic and concerted use of tactics such as counterfeiting documents, falsifying evidence, manipulating facts and accounting events erroneously. The so called "troll farms" generate and replicate conspiracy theories that undermine the target's credibility and legitimacy.

Disinformation operations in the context of the COVID 19 pandemic

Nowadays, threats generated by propaganda and disinformation are made effective by exploiting the systemic vulnerabilities of our digital ecosystems, the massive volume of information and the ability to use algorithms to push dissemination. The COVID 19 pandemic is an illustrative example of this phenomenon.

The Global Health Organisation attracted attention as early March on the fact that fake news about Covid 19 "are spreading faster than the virus itself" and labelled this phenomenon "as an infodemy of planetary proportions". For instance, between January 22nd and March 25th, the EU vs. Disinfo database collected no less than 39 cases of fake news, which attributed the Coronavirus to the United States, and another 24 that supported the conspiracy theory that COVID 19 was used as a biological weapon against China and its economy. Also notably, between January 22nd and April 1st, 2020, the public database Eu vs. Disinfo collected no less than 150 examples of pro-Kremlin fake news focused on the Covid 19 pandemic. One of the most circulated disinformation themes is that of the actual inexistence of the pandemic that would be global hoax aimed at advancing an occult agenda to control the world population. So called interviews with "reputed scientists and experts" are used to dis-inform on the

gravity of the disease, by circulating fake data on the impact of the pandemic and offering "medical advice" which come in direct contradiction with medical expertise. It demonstrates the global character of the infodemic, narratives being circulated and adapted according to local target audience.

Since then, public awareness was raised and governments, health and security institutions, as well as international organizations have actively contributed to providing reliable sources of information and exposing the fake nature of disinformation narratives.

How to tackle with these phenomena?

Security measures have always been at the forefront. Yet, state institutions have to also become pro-active in building community resilience to propaganda, to consolidate trust and involvement with the democratic practices of debate, as well as long-term education for critical thinking, digital literacy and rational debate. It requires a whole of society approach.
Countering disinformation can be done by acting on two levels:

- The message : exposing the logic error, verifying facts, figures, etc.;
- The source: exposing the real source, making the public aware on disinformation modus operandi.

To this end, several actions can be carried out by states:

- Expose information operations and their modus operandi through media, democracy watch-dog civil society organizations, academic research etc.;
- Promote the use of reliable fact checking organizations;
- Encourage the use of plugins that make fact checking globally available;
- Involve social media platforms and tech companies to take consistent action to timely identify and ban disinformation spreading accounts[1];
- Empower citizens understand, check and contribute to the grass-root movement of fighting propaganda and disinformation.

Intelligence communities in particular need to reconsider their role, consolidate dialogue and engagement with both decision makers and the larger public, actively promote a shared set of values and a common security culture and, last but not least, always be ready to get involved in sanitised, fact based, rational and consistent debate.

It should be kept in mind that it is not illegal to post and say nonsense. This is a constitutional right of every citizen. It only becomes dangerous, if it happens as part of an information operation. This leads to the problem how to distinguish between freedom of speech and a malicious information attack. In addition to the mentioned actions, intelligence communities might try to use technology to attribute a message to the source (in an anonymous manner).

[1] In September 2018, a group of online platforms, social networks, advertisers and advertising industry bodies brought together by the European Commission, agreed upon a self – regulatory Code of Practice on Disinformation to address the spread of online disinformation and fake news

Hybrid Warfare – a very short introduction

Hybrid warfare, if carried out against European countries, would pose a particular challenge for Europe. The term "hybrid threats" itself has aroused scepticism and reticence among some defence and national security actors. Its massive use in the debates in the EU and NATO has turned it in a vague, catch-all and unsubstantial concept.

Considering this, **defining the concept is necessary**. The criteria of hybrid warfare can be summarised in the following:

- A hybrid threat is characterised by the recourse by a hostile foreign actor, whether state or non-state, to an integrated combination of deliberately ambiguous and asymmetric modes of operation for offensive purposes of disruption, intimidation or destabilisation that may lead to the long-term weakening of states and societies.
- This concept refers to a comprehensive strategy of engagement by hostile actors that have achieved a high level of integration, at the political and strategic levels, of their civilian, military and intelligence apparatus. This global strategy consists of a set of actions at the tactical and/or strategic level combining various means (military or not, conventional or not, etc.), possibly in conjunction with the use or threat of use of force. These actions, while remaining below the threshold of armed aggression and of Article 5 for NATO and Article 42.7 of the TEU, aim to intimidate or destabilise the adversary by reducing its ability to allocate and respond, and may even paralyse them.
- From terror, sabotage and subversion, to guerrilla warfare, conventional warfare and even the nuclear domain, all possible levels of escalation can be included or even combined.
- Although hybrid warfare has implications for the operational and tactical level, it is primarily of a strategic nature, making use of multiple and shifting centres of gravity in a flexible and dynamic manner.
- Hybrid warfare can start long before the 'shooting war' begins, and in an extreme case, it even offers the option to win a war despite military defeat. It can be perceived as "the art of creating power".
- It impedes a fast, unified response either from the adversary or the international community creating ambiguity in the following interfaces :
    - Between war and peace: operating in a "grey zone", in order to blur traditional lines of order and responsibilities and to contribute to their subsequent dissolution.
    - Between friend and foe : the actions cannot be clearly attributed to them in due time
    - Between intrastate and interstate conflicts and therefore between domestic and external security, involving state, non-state and pseudo-state actors.

That being said, **hybrid warfare is not a new phenomenon**. It has existed throughout the entire history of warfare and it does not present a fundamentally "new challenge". The concept has been widely addressed for instance by Sun Tzu, the Byzantine strategists, Clausewitz or more recently by General A. Beaufre or the military theorist D. Galula. To take recent examples, the "below the threshold" confrontation with Iran in the 1980s or the conflict in Côte d'Ivoire in 2004 that involved proxies are examples of hybrid warfare. The use of ruse and subterfuge is a constant in military strategy even if one researcher notes that *"war is nowadays rarely declared as it was in the good old times"*.

The strategic surprise of the annexation of the Crimea, as well as the outbreak of the conflict in Donbass, gave to hybrid warfare an appearance of novelty, while focusing almost exclusively on the Russian threat, however, other countries, notably Iran, and non-state actors (Hezbollah, Daech) are also able to use such strategies. **The real game changer lies in the new vulnerabilities we are facing**:

- Globalization, close international interaction, internal vulnerabilities of democratic societies and their socio-economic and cultural cleavages and interconnected societies have the potential to open up additional starting points for hybrid methods of warfare.
- The evolution of our strategic environment is favouring an increase of confrontations below the threshold of open conflict. Dividing lines within European societies for instance are growing and deepening.
- Disintegration of multilateral instruments and the return to uninhibited and unashamed power policies are encouraging this trend.
- From the a military point of view, and in particular with regard to the issue of cyber-attacks, hybridity as a new paradigm for understanding the plural reality of cyber-conflictuality is consistent with the reality of the "cyber field".

How to address this challenge? Awareness is the first precondition. It is important to recognize hybrid conflicts at an early stage and to prevent the transition to a large-scale, aggressive phase.
Countering hybrid warfare successfully in the long run requires far more forces, resources and efforts than offensive hybrid operations do. In addition to long-term measures to build resilience, the ability to constantly perform in-depth analyses of specific war/conflict situations, related actors and strategies will become a key capability in countering and responding to hybrid methods of warfare.
This includes a whole-of- government approach, a whole-of-nation/society approach, as well as international cooperation and coordination, particularly between EU and NATO.

For this reason, strategies are developed at the national level (French 2017 Strategic Review of Defence and National Security or Estonian National Defense Act).

At the EU level, hybrid warfare is considered as a new strategic challenge, which led to the adoption of a common framework for fighting hybrid threats, composed of 22 actions designed to make progress in three areas (situation assessment, resilience and response capabilities). The organisation of European work in the fight against hybrid threats, initially split between several fora, now benefits from the creation of the Horizontal Group to Strengthen Resilience and Combat Hybrid Threats, whose first meeting took place in July 2019.

In addition, identification of hybrid threats is a strategic priority for EU-NATO cooperation as stated in the Warsaw and Brussels Joint Declarations (2016, 2018).