IRIS INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

PROGRAMME EUROPE, STRATEGY & SECURITY

THE HYBRID THREATS AND POWER PLAY CHALLENGES FACING THE EUROPEAN UNION

General (2S) Jean-Marc Vigilant /
Associate Research Fellow, IRIS

February 2025

AUTHOR'S PRESENTATION

General (2S) Jean-Marc Vigilant / Associate Research Fellow, IRIS

Jean-Marc Vigilant is an associate researcher at IRIS, specializing in military and defense issues. He is the founder and president of BeVigilant and also serves as the president of the EuroDéfense-France association and a member of the Institute for Research and Communication on Europe (IRCE).

As an Air Division General, Jean-Marc Vigilant has held numerous joint-force responsibilities, primarily in an international context, often at the strategic level in the politico-military field, advising senior civilian and military authorities, both French and allied. He also served as the director of the War College from 2020 to 2022.

PROGRAMME
EUROPE,
STRATEGY &
SECURITY

The Europe, Strategy, Security programme aims at deciphering the changes in Europe and its regional environment at the political and strategic levels. Recognized for its expertise both nationally and internationally, IRIS is a partner and coordinator of international projects with main research centers in Europe, which allow the Institute to build strong links with decision makers.

iris-france.org

@InstitutIRIS

@InstitutIRIS

institut_iris

IRIS

IRIS - Institut de relations internationales et stratégiques

We are living in dangerous times as the world lurches from one geopolitical period to another and nations are again engaged in power play, not afraid to resort to violence to resolve their political disputes. Many international and domestic crises are interrelated, either because they share the same protagonists or because of their mutual impact.

Since Russia's deliberate attack on Ukraine in February 2022, the threats lurking at Europe's door have become more menacing, not least with the current changes in the geopolitical order in the Middle East and the ejection of French and European military forces from the Sahel now under the control of authoritarian powers. That said, the threat of terrorism which so excessively obsessed the western powers before the Russian invasion has not gone away. Western democracies are also threatened from within, by outside interference in their elections and manipulation of public opinion that have undermined the population's confidence in the institutions and led it to distrust its politicians.

In an international context marked by massive upheaval, Europe appears as a weak and amorphous mass, incapable of defending its own interests, of exerting an influence on events, at the mercy of the decisions of other powers. But the planet's predators are always quick to spot weaknesses, which they find provocative, and are happy to challenge who we are as Europeans by attacking, often surreptitiously, the things we care about the most. This is, in fact, the principle behind today's hybrid strategies, which tend to remain below the detection threshold yet constitute attacks that are difficult identify and harder still to trace back to their source.

How can European democracies rise to the major challenge of hybrid threats?

First of all, by analysing the changes in the nature of warfare and the historical and technological background that have culminated in these threats.

Then, by identifying the specific hybrid threats affecting the EU, in particular the never-ending cognitive warfare with which we are assailed, in order to obtain a better grasp of what is afoot.

Lastly, by making proposals to enable the EU to build up its arsenal of countermeasures to parry these hybrid threats and regain its former powerhouse status.

The changing nature of conflict

The concept of a hybrid approach is nothing new. 2,500 years ago, in his famous treatise on the "Art of War", Sun Tzu described several of the principles that underlie today's hybrid strategies. He emphasised the importance of cunning and psychological warfare, the ability to seize opportunities and turn the enemy's resources against it, all typical features of hybrid strategies. For Sun Tzu, "the supreme art of war is to subdue the enemy without fighting". Whence the value he attaches to the strategic value of using patience to wear down the enemy and avoid direct conflict, keeping the enemy on the back foot, combining unconventional and indirect methods to sap the enemy and chip away at its resistance.

But we need at this point to focus on more contemporary history to understand how we have come to find ourselves in the situation in which we are today.

Following the end of the Cold War, the United States military demonstrated its absolute supremacy during the first Gulf War in 1991. It was, however, after the American defeat in Vietnam that the world was stupefied to discover the results of the "Revolution in military affairs" spearheaded by the US Department of Defense: widespread use of internet and space for observation purposes, telecommunications, precise positioning and navigation by means of GPS, and implementation of the air-land battle concept, the precursor to joint combat operations. The international coalition with a 500,000 strong force from 35 countries under US command was able to free Kuwait in 42 days from Saddam Hussein's invading Iraqi troops, at the time ranked 4th among the world's armed forces[1]. The operation, codenamed *Desert Storm*, began with a sustained five-week air campaign and ended with a 100-hour long land battle.

In the face of this striking demonstration of "US hyper power" [2], the Europeans thought that the final chapter had been signed, "the end of history" to use the words of Francis Fukuyama, namely that the western model had proved its ultimate superiority, under the umbrella of *Pax Americana*.

While the western powers were complacently reliant on their technological superiority in managing crises in asymmetrical conflicts, in which their expeditionary forces were able to operate in relatively permissive environments, their enemies were covertly observing them.

This is particularly true of the Chinese who, back in 1999, were already theorising about ways of outwitting the western military powers in a famous publication entitled "Unrestricted Warfare". For the authors of this treatise, Qiao Liang and Wang Xiangsui, two colonels in the People's Liberation Army, the "battlefield is everywhere". They explain how, with the advent of technology, the limits between physical and virtual domains have disappeared paving the way for widespread use of non-military (financial, economic, legal and technological) means

[1] 1 million soldiers, 5,500 tanks, 700 combat aircraft, etc.

[2] In the words of Hubert Vedrine, a former French Minister of Foreign Affairs

to gain the upper hand over the United States, in particular, and the western powers in general.

This new battlefield is the result of widespread access to technological innovation, notably digital information technologies, which are by nature dual purpose in that they can be used both for civilian and for military purposes.

At the beginning of the 21st century, easier access to technological innovation had two vital consequences. Firstly, it signalled the end of the technological advantage enjoyed by the western powers, secondly, it created new domains of warfare, for example outer space, cyberspace, the seabed, the electromagnetic spectrum or the field of information.

As we have become increasingly dependent on these new technologies and need to defend our interests and resources on these fronts, the area of potential conflict has inevitably expanded beyond the traditional land, air and sea battlefields.

The theory of the modern hybrid warfare concept began to take shape more specifically in 2005 in the United States, when General James Mattis and Franck G. Hoffmann published "Future Wars*"*, followed in 2007 by another seminal work *"*Conflict in the 21st Century: The Rise of Hybrid Wars".

It was during the wars in Iraq and Afghanistan that the rebels or the Taliban began to combine conventional warfare (armed ambushes, etc.) with more unconventional techniques (improvised explosive devices, psychological warfare or information campaigns).

Mattis and Hoffman were well aware that future conflicts would be fought more via cyberattacks, disinformation, economic coercion and other hybrid means of weakening the enemy without declaring outright war.

The role played by the "little green men"[3] in these two Ukrainian provinces is attributed to the strategic vision of Valery Gerasimov, Chief of the General Staff of the Russian Armed Forces, although he has never officially claimed to be behind this doctrine. It was an article[4] published in February 2013 on changes in modern warfare, in which Gerasimov analysed what he perceived as western interference in eastern Europe, not least Ukraine, during the 2004 Colour Revolutions that was the source of this confusion. In response to this interference, he described a Russian approach to hybrid and unconventional warfare, in which the boundaries

[3] Russian soldiers disguised in unmarked green military fatigues and organising insurrection against the legitimate government.

[4] Valeri Guerassimov, "The value of science is in the forethought", *Voyenno-Promyshlenny Kuryer* (Military-Industrial Kurier), February 2013.

between war and peace were less defined and where non-military weapons played a major part in achieving strategic targets.

In Europe, the concepts of hybrid strategies and threats started to become a major issue from 2014 with Russia’s annexation of Crimea. NATO formally recognised the existence of such strategies at its 2014 Summit in Wales. The EU, for its part, officially adopted the expression “hybrid threats” in its documents in 2015, in response to Russia’s use of such strategies in Ukraine.

In April 2016, the EU approved the “Joint framework on countering hybrid threats”, in which it used the term of “hybrid threats” to describe the combination of disinformation, cyberattacks, economic coercion and discrete military operations.

These new domains of warfare, for which there exist little or no regulations, no clear legal or political framework, have become **grey areas**, where neither outright war nor complete peace prevail. In these grey areas, our enemies have the ability to adopt hybrid strategies below the threshold of open warfare but which include hostile action very difficult to trace back to its perpetrator.

HYBRID THREATS AGAINST THE EU

Hybrid confrontation is indicative of **the shift in battlefields** with the advent of new forms of action that lower the bar of legality.

For a more **operational definition** of hybrid strategy, we only need to refer to that of the joint concepts, doctrines and experiments centre of the General Staff of the French Armed Forces, namely “the strategy of a protagonist, whether or not a state actor, the purpose of which is to circumvent or weaken another power, diminish its influence, legitimacy and opposing designs by resorting to a combination of military and non-military tactics, licit or illicit, often subversive, ambiguous and hard to trace back to their author, in order to create paralysis, while remaining discrete enough to avoid riposte or open conflict, potentially with the intention of ramping up this aggression to another level”.

By way of summary, it may be said that hybrid strategies are played out below **three different types of threshold**, namely those of detection, comprehension and reaction.

For a more accurate idea of the nature of the new hybrid threats menacing the EU, it is worth looking more closely at the Russian approach to the **transformation of modern warfare** described by Gerasimov.

As an example, he explains that modern warfare no longer takes place exclusively using military resources on the traditional battlefields. Today war is waged using a **mixture of military and non-military weapons** combined into an overall strategy. He insists on the fact that the boundaries between war and peace are becoming blurred and that warfare now extends to new and often indirect methods.

According to Gerasimov, non-military methods such as disinformation, cyberattacks, economic coercion and clandestine political action can be as efficient, if not more so, than conventional military measures.

He is of the opinion that, in modern warfare, the resources earmarked for these non-military methods should be around four times higher than those afforded to conventional military methods.

Gerasimov places emphasis on the importance of using a combination of conventional means (regular armed forces) and the new non-conventional means:

- Local paramilitary and militia groups (as in Crimea or eastern Ukraine with the pro-Russian separatists, or the Wagner Group in Ukraine and Africa, rebaptised the Africa Corps since the death of the group's historic leader Yevgeny Prigozhin)
- Cyberattacks to disrupt critical infrastructure
- Disinformation and propaganda to destabilise the enemy and influence public opinion
- Economic coercion and targeted sanctions.

These are all methods that may be used to **weaken another State without ever officially declaring war**.

Gerasimov highlights the crucial role of information warfare, pointing out that propaganda and psychological warfare are vital in influencing public opinion and throwing the enemy into confusion.

He emphasises the need for **Russia to take preventive action by turning latent conflicts to its advantage** or by becoming involved in crises before they reach a critical stage.

This is exactly what is happening in Europe or in parts of the world where the Europeans have vested interests. In **Africa**, the French and European armed forces were forced to pull out of the Sahel in spring 2024, as a result of Russian anti-French propaganda. Elsewhere, the social and political tensions rife in French **overseas territories** have been fuelled by foreign interference, resulting in violent protests against the authority of the French State in New Caledonia and Martinique.

Similarly, the Russians are currently using a number of different tactics in an attempt to **lessen European support for Ukraine**: by stepping up their psychological warfare and their spying activities on the social networks, by weaponising pacifism, mobilising nationalism, exploiting existing divisions, turning people against refugees and migrants and by targeting diaspora communities.

In another register, **more technical areas** are also being targeted by hybrid strategies.

Access to **space** is no longer reserved for major nations and nuclear powers. With the advent of New Space, the price of orbiting satellites has dramatically fallen, going from over 10,000 euros to some 2,000 euros per kilo over the last decade, **giving access** to a variety of protagonists, States or not. By way of example, the Montpellier University Space Centre is now producing nanosatellites with extraordinary technical capabilities from 10^3 cm CubeSat units and launching them into orbit at reasonable cost for scientific research applications.

It is also now easier to escape the deterministic laws of orbital mechanics by manoeuvring in space. As a result, enemy **patroller satellites** can close in on a non-cooperative satellite to spy on it or stop it from operating by jamming or kinetic action. This type of manoeuvre is hard to detect, making it equally hard to apportion blame. For example, a Russian *Luch Olymp* satellite closed in on the Franco-Italian *Athena-Fidus* satellite in the geostationary orbit in 2018, and another Russian satellite demonstrated its **manoeuvrability in low earth orbit** in 2024.

An increasing number of services are reliant on space infrastructure, which is ever expanding with the arrival of the giant satellite constellations. In the early 2000s, there were some 1,000 satellites in orbit whereas, today, there are nearly 10,000. Growth is exponential, which is certainly going to raise sustainability issues given the ballooning risks of in-orbit debris. At a time when we have never been so **dependent** on the space sector, with European citizens each using an average of 47 satellites[5] in their everyday lives, it has become absolutely essential to defend our interests in the space domain.

Similarly, where **cyberspace** is concerned, there are possibilities for hybrid attacks on all three layers. The first so-called physical layer consists of the infrastructure hardware that is the networks, servers and computers used to power the internet. The second layer is the logic and application layer that includes software and generates and transmits information. The third is the cognitive and semantic layer and is the term used to describe websurfer thought processes. In view of our growing dependency on internet and networks, we urgently need to

[5] French National Assembly, « Rapport d'information déposé par la commission des affaires européennes sur la politique spatiale européenne », n°1438, 21 November 2018, https://www.assemblee-nationale.fr/dyn/15/rapports/due/l15b1438_rapport-information

defend our resources and our activities throughout cyberspace against those deliberately seeking to do us harm.

A large part of the infrastructure used for internet lies in the **seabed**, which is hard to reach and to monitor. Submarine cables often embedded at depths of up to several kilometres beneath the ocean floor contain the optical fibres through which transit **95% of the world's internet communications**. Enemy foreign powers are quite capable of damaging these cables to disrupt the flow of data or of establishing discrete connections with these cables to divert or spy on data. It is a known fact that Russia is fully capable of such acts and is suspected of having used them to isolate Crimea or, in the Baltic Sea, to disrupt connectivity on NATO's northern facade.

Among the hybrid threats, the **most dangerous are undoubtedly those that concern information interference**, in other words deliberate manipulation, influencing public opinion and interfering in elections, which is what happened in 2016 in the USA when Donald Trump was first elected and in the United Kingdom at the time of the Brexit referendum. Other examples are the 2017 election of Emmanuel Macron as President of France (MacronLeaks) and, more recently, during the general elections in Romania. In this latter case, the Far-Right pro-Russian candidate **Călin Georgescu** was virtually unknown until one month before the elections and, at the time, was credited with 1% of the votes. In the last two weeks before the elections, he suddenly became the 9th most visible person on Tik-Tok through a combination of a cyberattack and information manipulation devised by the Russians and uncovered by the Romanian intelligence agencies, a fact subsequently confirmed, at least in part, by Tik-Tok. As a result, Georgescu came out on top of the poll, with more than 23% of the votes recorded, much to the general surprise. His victory was, however, short-lived since it was soon irrefutably and technically demonstrated that the result was ascribable to "outside" interference and the Romanian Constitutional Court was able to invalidate the election.

Information is now weaponised. It is, in fact, a powerful and effective tool in a society that makes massive use of the digital technologies that have exploded over the past decade. New communications technologies have had the effect of **multiplying the possibilities** for manipulating information.

In an **ultra-connected, digital environment** producing huge volumes of information, it would be dangerous only to think in terms of the technical aspects of the above-mentioned fields and to ignore the human and societal dimensions. In addition to cyberwarfare, which consists of using digital resources to control, alter or destroy information, there is a new form of warfare that consists of playing with the human brain to change the way in which it processes information.

Referred to as "**cognitive warfare**", this unconventional battle technique consists of using information technologies to exploit the cognitive bias of a group of people to plant a false image of the world in their minds and, by doing so, change their way of thinking, break down their inhibitions or even divide communities.

The unbridled impact of the social media, the press and television, disinformation or even propaganda on the general public is a clear illustration of how information technologies and psychological warfare can be combined to transform the **human brain into a new battlefield**.

Cognitive warfare lies at the interface between cyberwarfare and information warfare and constitutes the most sophisticated technique used to manipulate the behaviour of a group of individuals. **The general public has become a new target for this type of combat**.

In order better to understand the mechanisms at work, there are several factors to bear in mind:

Firstly, **cognitive bias** is a common error based on two key biological principles:

- A preference for the simplest reasoning to expend minimum time and energy (natural intellectual laziness)
- The strong constraint of adopting a way of thinking other than one's first reaction.

Secondly, the **hyper-personalisation algorithms** that are responsible for the growing polarisation of public opinion. The social media make it easier for people to broadcast "*surprising and negative*" messages and are a breeding ground for emotional instability and extremism. The most unlikely and usually fake news items are 70% more likely to be retweeted[6].

Sound and images carry a strong emotional charge, and emotion often supplants reasoning and logic. It is for this reason that media content increasingly **generated by AI** (deep fakes) is so dangerous and so effective.

[6] According to Guy-Philippe Goldstein, researcher into cognitive warfare and polarisation of the Cold War version 2.0.

POSSIBLE EU RESPONSE: RE-ENGAGING WITH POWER PLAY

Europe is under attack from all sides, from authoritarian regimes challenging the international order established by the western powers in the wake of World War II and feeling threatened by the appeal of liberal democracies for their citizens.

But Europe is also vulnerable because its refusal to play the power game has made it into a **rich, weak and ageing prey** for all the geopolitical predators. Since the 5th century, almost every generation of Europe's population has experienced warfare, despite the continent's world domination between the 15th and 20th centuries via its colonial empires. The last two World Wars were a bloodbath of horror and self-destruction in Europe, with a total of some 65 million civilian and military victims.

Europe was able to rebuild after WWII thanks to American protection which enabled the NATO European and EU nations to enjoy the **longest period of peace** since the days of the Roman Empire, 80 years, which is more than two generations.

With the United States' declared intention of disengaging from Europe and its "pivot" towards Asia and the Pacific as its new strategic priority, the EU must now take its **strategic responsibilities** more seriously, defending its interests and its values against increasingly assertive strategic rivals.

Under these conditions, **what can Europe do** to be better prepared to manage these hybrid threats and defend its own interests?

First and foremost, it must make its citizens **more aware** of the nature and existence of the threats and associated dangers. We may not be engaged in open warfare but we are not at peace, in particular in the virtual domains of cyberspace and information, where our companies, our organisations and our populations are constantly under attack from our strategic rivals on a daily basis. It is therefore vital to spread the word on this subject as widely as possible.

We need to educate and train our younger generations to develop their **critical thinking** capabilities. Users need to better understand the mechanisms behind the social media algorithms so that they can ask themselves the right questions, for example: Why have I received this message? What is the sender's motivation? If we can develop reflexes of this sort, we will be better placed to act less emotionally and avoid inadvertently passing on unsuitable content.

That said, it is virtually impossible to convince people to change their minds once they have been taken in by fake news, in particular if those concerned are firm believers in conspiracy theory. The best way to call fake news into question is to **teach people to use online digital tools** based on AI to produce their own deep fakes and to create a *chatbot* to drive traffic on the social media. Once they are familiar with the techniques for falsifying information, they are likely to be less credulous.

Similarly, we need to make our fellow European citizens more aware of the **importance of defence issues and cultivate the development of a defence mindset**. While Europe may favour pacifism on historical grounds, it is still surprising to see the extent to which some of its nationals are defeatist and convinced that we would be unable to defend ourselves without American aid in NATO. You only have to look at Ukraine to see that the ability to defend oneself is first and foremost a state of mind and a burning desire to fight to defend the things we hold dear.

This is why it is so important to break free of our stultifying dependency on the United States for our defence and to consolidate **NATO's European pillar** together with the other CSDP instruments[227] to endow the European allies with greater strategic responsibility. In truth, Europeans often fondly believe that NATO is an American organisation in which Europe is involved, whereas it is, in fact, a European organisation that the Americans manage at our behest. In reality, America's defence organisation is much bigger than NATO and has a truly worldwide dimension[8].

Seen from outside Europe, the differences of opinion among the European allies are trifling. However, to develop a **common strategic European culture,** it will be necessary to step up the higher military education delivered by Europe's war and staff colleges. A project to this effect was set in train by the French War College in 2022, adopting a progressive approach[9]. The idea was that of establishing the conditions in time and space to enable European military officials and civil servants not only to learn with each other but also to learn from each other. This would enable them to acquire a better knowledge of each other's history, geography, politics and military culture and, by extension, better understand the political stance or strategic

[7] EU Common Security & Defence Policy.

[8] Jean-Marc Vigilant, "Europeanising NATO: a pipe dream or an obvious necessity for Europeans?", *IRIS*, 16 May 2024, https://www.iris-france.org/europeaniser-lotan-une-utopie-ou-une-evidente-necessite-pour-les-europeens/

[9] Jean-Marc Vigilant, « A European war college, an opportunity for European Defence? », *The European Security Defence Union,* vol 37 (4/2020), 18 December 2020, https://issuu.com/esdu/docs/esdu_2020_vol37/s/11509967 ; Hartmut Bühl, « Strategic leadership in the European Union », *The European Security Defence Union,* vol 43 (2/2022), 29 July 2022, https://issuu.com/esdu/docs/esdu_2022_2/s/16474712

visions of their neighbours. They should thus be more able to see where their countries' common interests lie.

It is equally important to build up the **resilience** of our societies from all points of view, in other words the ability to take a fall but to pick oneself up and start all over again. The Common Framework for Countering Hybrid Threats referred to later in this article makes this patently clear. Yet, **internal cohesion** will be vital to fight against cognitive warfare, which tends to play on the tensions or divisions existing in society, to exacerbate them and create mistrust within communities or between the people and their government.

The main challenge for a State that is under attack from hybrid warfare is that of **detecting** the attack, **identifying** the people responsible, and then **counterattacking**. The State under attack is then faced with a double dilemma, namely that of interpreting the aggression of which it is the target despite the ambiguous nature of threat and of responding to this attack in accountable and sufficient controlled fashion to prevent escalation.

Given the difficulties in obtaining evidence that could stand up in court to counter this type of attack, without compromising the methods and sources of the intelligence agencies or threaten operational security, **naming and shaming can only be a political decision**.

One of the challenges facing democracies plagued by hybrid attacks is that of finding a way of punishing the perpetuator without stepping outside the confines of the law.

There do exist specific instruments to assist them, such as the Centre of Excellence (CoE) for Countering Hybrid Threats in Finland. This centre was created in 2017 following Russia's incursions into Ukraine and Crimea. It analyses threats, develops doctrines and promotes best practices in the interest of NATO and the EU.

At a recent hearing with French politicians, Dr. Teija Tiilikainen, Finnish Director of the CoE for Countering Hybrid threats in Helsinki, stated that the two countries that were the best prepared to counter hybrid threats were Sweden and France.

This would tend to suggest that some of the countermeasures put in place by France could usefully inspire other European countries in their efforts to build up their resilience:

- A fully interministerial approach[10] spearheaded by **General Secretariat for Defence and National Security** towards analysing the threats, identifying the attacks and

[10] « Lutte contre les influences étrangères malveillantes. Pour une mobilisation de toute la Nation face à la néo-guerre froide – Rapport », n°739 (2023-2024), *La Galaxie Sénat*, 23 July 2024, https://www.senat.fr/rap/r23-739-1/r23-739-1.html

preparing a response in five priority areas: cyber (ANSSI[11]), information (VIGINUM[12]), economic security (SISSE[13]), legal standards and operations (General Staff).

- In **French military doctrine**, hybrid warfare can only be countered by means of a multidimensional defence and riposte strategy using not only all forms of military power (army, navy, air force, cyber, space), but also the whole arsenal of civil instruments of power (diplomacy, media, economics) to respond to insidious, multifaceted threats. It is perhaps here that could lie the EU's added value in ensuring coordinated use of these levers to supplement military action.
- It would also be possible to consider EU action along these lines as part of a **"reverse" Berlin Plus[14]** agreement in support of NATO, given that NATO is a strictly military organisation and only able to respond legitimately to hybrid attacks that have a direct impact on its ability to engage in military operations. By providing non-military support, the EU could have a **multiplying effect on resilience** by reinforcing the civil, economic and digital capabilities of NATO Member States to respond more effectively to complex, multidimensional hybrid attacks.
- Moreover, even if the term "hybrid strategy" may have negative connotations and tends to be used in relation to an enemy, we also need to **be proactive,** not only reactive. This explains why, in addition to the five strategic functions set out in the French White Paper (knowledge-anticipation, dissuasion, prevention, protection and intervention) France has proposed a sixth to cater, at least in part, to the problem of hybrid threats, namely **influence** for which the MEFA[15] and the MAF[16] have joint responsibility. The aim of this function is to foster positive attitudes to our interests outside national territory, while remaining fully answerable and within the law.

Last but not least, the **Common Framework for Countering Hybrid Threats** developed by the EU in 2016 still has a part to play in building up cooperation and capabilities among Member States in the face of hybrid threats. This framework is underpinned by a common vision of the challenges we face because of hybrid threats and sets out guidelines for reinforcing our detection, prevention and response capabilities to counter the new menace.

[11] French National Agency for the Security of Information Systems
[12] Agency for vigilance and protection against foreign digital interference
[13] Department for strategic information and economic security
[14] The Berlin Plus agreements of 14 March 2003, setting the bases for NATO-EU cooperation by giving the EU access to NATO's planning and command capabilities for operations spearheaded by the EU to which NATO as a whole is not party.
[15] French Ministry for Europe and Foreign Affairs
[16] French Ministry of Armed Forces

The main objectives of the **Common Framework** are:

- To enhance coordination between the institutions and States belonging to the EU and to NATO
- To arrive at a common understanding of what constitutes hybrid threats
- To improve our prevention and detection capabilities
- To guarantee a fast and effective response as part of a global approach
- To boost the resilience of critical infrastructure
- To encourage cooperation with outside partners

There are already a large number of initiatives in the different Member States aimed at countering hybrid threats and still further proposals could usefully be explored to build up general EU capabilities in this area.

CONCLUSION

General André Beaufre, one of prime movers behind French nuclear deterrent policies, developed a theory with regard to the three stages culminating in war: **competition, dispute, confrontation**.

Today, in the complex globalised world in which we are living, these three stages can take place simultaneously, depending on the issues at stake, the area concerned and the protagonists, in particular by applying hybrid strategies that remain just on the right side of outright confrontation. Two countries can be partners in one area and opponents in another. One thing, however, never changes: **anything unprotected is a target for spoliation and anything spoliated is disputed**.

It is therefore high time that Europe realised that it needs to **re-engage in power play**, to accept the power balance forced upon it by its strategic rivals and recognise the necessity of fighting to defend its values and its interests on all fronts and against all threats, irrespective of their source.

But to rise to this challenge, Europe must cast off the defeatism currently rife in the continent, perhaps even as a result of manipulation by foreign powers, according to which without the Americans, the Europeans would be unable to defend themselves. **The EU is the world's number two economic power** with a population of 450 million inhabitants and a GDP of 20,300 billion euros[17]. It combined defence budgets amount to 279 billion euros for a total of 1.3 million armed personnel. Obviously, the EU needs to increase and improve its efforts in

[17] International Monetary Fund estimation in 2023.

this field but it should not be afraid of Russia, which is languishing in 9th position in the world with a nominal GDP of 2,200 billion euros[18] i.e. not as rich as Italy, for a population of 142 billion inhabitants. Its annual defence budget stood at 113 billion euros[19] in 2024 and its armed forces comprised 1.1 million soldiers.

The EU must have confidence in itself and must reaffirm its determination to defend itself using whatever means it takes, including military force, to turn the tables on those who are trying to frighten us and instil fear in them instead. But for the EU to become more credible, it will be necessary for Member States to prepare themselves mentally and materially to really assume their strategic responsibility. It is only in this way that they will be able to keep the peace and defend the freedom and values that they hold dear.

"Life is not about waiting for the storm to pass...It's about learning to dance in the rain.", Vivian Greene

[18] World Bank estimation in 2023.

[19] According to Military Balance 2024.

Strategic expertise with total independance

PROGRAMME
EUROPE, STRATEGY & SECURITY

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

2 bis, rue Mercœur - 75011 PARIS / France
+ 33 (0) 1 53 27 60 60
contact@iris-france.org

iris-france.org

IRIS, a public utility association, is one of the main French think tank specialized on geopolitical and strategic issues. It distinguishes itself by its unique ability to bring together a research center and a school (IRIS Sup') which delivers diplomas.
This model contributes to its national and international attractiveness. IRIS is organized around four activity units: research, publication, organization of events and training.