

idn

E-Briefing Papers

Conferência Internacional:

“Ameaças Híbridas – Responder à Complexidade
num Mundo Interconectado”

Conference:

“Hybrid Threats – Responding to Complexity
in an Interconnected World”

Os *E-Briefing Papers* do Instituto da Defesa Nacional visam proporcionar o acompanhamento de temas e debates atuais nos planos da segurança internacional e das políticas de defesa nacional, incluindo resultados da investigação promovida pelo Instituto da Defesa Nacional, sobretudo na sua vertente aplicada e de apoio à decisão política, bem como contributos de outros analistas e investigadores associados do Instituto.

As opiniões livremente expressas nas publicações do IDN vinculam apenas os seus autores, não podendo ser entendidas como refletindo uma posição oficial do IDN ou do Ministério da Defesa Nacional de Portugal.

FICHA TÉCNICA

Diretora

Isabel Ferreira Nunes

Coordenação Científica

Isabel Ferreira Nunes

Editor

Luís Cunha

Centro Editorial

Filipa Teles

Design Editorial

Núcleo de Desenho do IDN - Paulo Jorge Pereira

Propriedade, Edição e Design Gráfico

Instituto da Defesa Nacional

Calçada das Necessidades, 5, 1399-017 Lisboa, Portugal

Tel. + (351)211 544 700

Email: idsn.publicacoes@defesa.pt

<http://www.idn.gov.pt>

ISSN: 2184-8246

Conferência Internacional: “Ameaças Híbridas – Responder à Complexidade num Mundo Interconectado”¹

International Conference: “Hybrid Threats – Responding to Complexity in an Interconnected World”²

Data: 23 de fevereiro de 2026

Date: February 23, 2026

Local: Auditório 1

Location: Auditorium 1

¹ Transcrição parcial da Conferência Internacional «Ameaças Híbridas – Responder à Complexidade num Mundo Interconectado» (23 de fevereiro de 2026). Transcrição realizada por Mariana Silva e Ryan Powers, no âmbito do programa de estágio no Instituto da Defesa Nacional. Moderadores da conferência Coronel: Jorge Costa Campos, Assessor de Estudos do Instituto da Defesa Nacional e Mestre Paula Pereira, Universidade Autónoma de Lisboa e Assessora do Instituto da Defesa Nacional

² Partial transcript of the International Conference: “Hybrid Threats – Responding to Complexity in an Interconnected World” (23 February 2026). Transcript by Mariana Silva and Ryan Powers, interns at the National Defence Institute. Moderation of the conference by Colonel Jorge Costa Campos, Advisor to the National Defence Institute and Paula Pereira (MSc), Autonomous University of Lisbon and Advisor to the National Defence Institute.

Índice

Programme	5
Opening address	6
Professor Isabel Ferreira Nunes, Director of the National Defence Institute (IDN)	6
Lieutenant General Rui Ferreira	9
Challenges of Governance Encountering Hybrid Threats	14
Evgenia Karatari	14
Emilie Berthelsen	19
Roderick Parkes	22



International Conference Hybrid Threats + Countering Complexity in an Interconnected World

National Defence Institute, 23 February 2026

idn
Conferences

50
anos
idn 1976 - 2026

In an era marked by profound geopolitical uncertainty and rapid technological change, security challenges have become increasingly complex, interconnected, and difficult to attribute. Hybrid threats blend military and non-military means, state and non-state actors, conventional and unconventional tools and target governmental structures, the armed forces and the cohesion of societies.

This conference brings together national and international experts to examine how hybrid activities are reshaping the contemporary security environment. Through a multidisciplinary lens, the conference will explore foreign interference, disinformation, governance challenges, and the protection of critical infrastructures, as well as the organizational and strategic adaptations required to enhance collective resilience.

PROGRAMME

14:35 Welcome Remarks

Isabel Ferreira Nunes, Director of the National Defence Institute

14:45 Keynote address delivered by

Lieutenant General Rui Ferreira, on behalf of the Chief of Staff of the Army, General Mendes Ferrão
Chair: Colonel Jorge Costa Campos, Advisor, National Defence Institute

15:15 Panel - Challenges of Governance in Countering Hybrid Threats European Governance and Hybrid Threats

Evgenia Karatari, Deputy Head of Division EU Situation Room, European External Action Service
Hybrid Threats and Critical Infrastructures: The Role of Strategic Intelligence
Representative of Portuguese SIED

Coffee Break

Hybrid Threats and Digital Frameworks

Representative of Portuguese SIS

Military adaptation, innovation and organisational change

Emilie Berthelsen, Technical University of Denmark
Chair: Paula Pereira, Advisor, National Defence Institute

17:15 Foreign Interference and Future Perspectives

Roderick Parkes, Researcher, NATO Defense College
Chair: Filipe Santos Costa, Non-Resident Researcher, National Defence Institute

Opening address

Professor Isabel Ferreira Nunes

Director of the National Defence Institute (IDN)

The National Defence Institute celebrates its 50th anniversary, and this conference is integrated into a commemorative cycle of conferences. In the coming months, five conferences, reflecting on defence and international security matters, will be organized. These events will address the challenges of digital transformation, examine the increasing needs for a comprehensive approach to the protection of critical infrastructures, debate the challenges of Europe's economic security, and discuss problems and opportunities of governance and security in Africa and in the Arctic. Today, four years after an unprovoked and unlawful decision was made by Russia to invade a sovereign country, the impact of hybrid threats in an interdependent and connected international environment as part of the global conflict with collective rest will be addressed. Hybrid threats are not a new theme in the security agenda; however, two main developments at the national level enable it to have wider expression. On the one hand, the greater geopolitical competition among international actors that characterizes the current security landscape generates new forms of struggle for power and influence among competitors, of which hybrid threats are a significant part. On the other hand, technological developments associated with the digital revolution and social media create a higher degree of connectivity that makes our governments, institutions, services, and citizens much more vulnerable to the effects of covert operations, foreign interference, and disinformation. Conceptual clarity is essential to identify, analyse, report, and mitigate this category of threats. A lack of response, due to a weakly defined nature and scope of hybrid threats, may affect the credibility and the legitimacy of States and organizations to act. In the European context, the emergence of heavy challenges not only has a political impact on how they are collectively addressed by security organizations and States, but it also has consequences on their institutional architecture, leading to important adaptations within the European Union (EU) and NATO. From the operational perspective, the EU Intelligence and Situation Centre and the establishment of a European hybrid fusion cell have been contributing to collecting information and intelligence, essential to the protection of Member States. The creation of the

European External Action Service, Strategic Communication Task Force, has been crucial in identifying and countering hostile narratives against the European Union, their guiding principles and policies. Likewise, centres of excellence, such as the European Centre of Excellence for Countering Hybrid Threats, are helping to develop a more structured approach to research, analysis, and awareness-raising. With respect to the alliance, hybrid threats are reshaping NATO's structure, leading to institutional adaptation through the creation of analytical units, such as the NATO hybrid analysis branch, designed to counter hybrid threats and reframe NATO's strategic doctrine by acknowledging hybrid actions as a threat that may trigger collective considerations. This has an impact on planning and response mechanisms while promoting civilian and military resilience, integration and cooperation with partners, and better interaction between military and non-military actors. These structural adjustments reflect the reconfiguration of both the European Union and the Alliance towards the mitigation of complex and multilayered security challenges that extend beyond traditional military confrontation. These have constituted important steps to enhance the capacity to identify, interpret, and react to hybrid challenges and threats. These institutional developments are meaningful from the Euro-Atlantic political and operational point of view, as well as from the perspective of cooperation with international partners. From a political perspective, it formally signals the way organizations and States perceive and assess the importance of hybrid threats and their disruptive potential. From the operational standpoint, it underlines the collective resolve and the capacity to protect and rapidly respond to the scale and the frequency of these threats. This new dimension of security has also strengthened European cooperation within NATO in the hybrid and cyber contexts, a cooperation that has been effective by combining European regulative and economic instruments with NATO's deterrent and digital vigilant military presence, able to counter foreign interference and revisionist foreign policies. However, hybrid threats pose challenges that cannot be easily addressed by democracies. Democratic systems rely on the observation of the rule of law, rights, and freedoms, making them prone to malicious effects of hostile narratives and acts, leading democracies to seem weak and inefficient as compared to totalitarian and authoritarian regimes, often portrayed as strong and efficient. In liberal democracies, because they are open and accountable political systems, the consequences of hybrid action may affect public trust in institutions and

public policies set to safeguard the security and safety of citizens. The disinformation campaigns that spread globally following the invasion of Crimea, the outbreak of COVID-19, the pandemics, and the Russian invasion of Ukraine in 2022, just to name a few, are good examples of this new reality. The most visible face of hybrid warfare comes in the form of cyberattacks, data manipulation, disinformation, service denial, and targeting of critical infrastructures, necessary to the normal functioning of States, societies, and businesses. The less visible, but far from being a less harmful dimension, comes under the form of influence operations, which may hinder the pursuit of foreign policy objectives of States or even the business continuity of public and private sectors and services. Hybrid threats require a whole-of-government approach, able to effectively connect the civilian and the military dimensions with the individual and State levels of security of these two, with the national and international strategic environment, where they operate. Regardless of the interpretation of security priorities, what is at stake is the future of whole-of-government systems, freedom, and prosperity in Europe, which we need to preserve in order to protect and defend our territorial integrity, our national security, and our collective and individual freedom, which we enjoy in the democratic societies we live in. States need better analytical instruments to detect and counter hybrid threats, proper legal frameworks to limit, criminalize, and punish them, and consistent strategies between governmental and non-governmental actors in order to mitigate hybrid threats and better resilience and awareness by both public and private actors.

Today's conference will analyse the conceptual and policy boundaries posed by hybrid threats and examine the challenges of military innovation and adaptation in countering hybrid threats. We will address the opportunities offered by closer dialogue and coordination within Europe and by better cooperation with partners and international organizations. The conference will conclude with a reflection on the future perspectives regarding the impact of hybrid threats.

The keynote address that follows has been delivered by Lieutenant General Rui Ferreira, Land Forces Commander, on behalf of the Chief of Staff of the Army, General Eduardo Mendes Ferrão.

Lieutenant General Rui Ferreira

This conference is dedicated to a subject that decisively shapes our time: hybrid threats and the profound transformation of the strategic environment.

Hybrid threats do not constitute an entirely new phenomenon. For strategic studies and international relations, even though their systematic conceptualization and exploitation of effects are relatively recent, historically, both State and non-State actors have always used a combination of a plethora of military and non-military instruments to achieve political objectives, simultaneously exploiting the military, economic, informational, and diplomatic dimensions of power. Thus, while the practices associated with hybrid threats have clear historical precedents, what is relatively new lies in their conceptual systematization and in the amplification provided by digital technologies, particularly the cyber and informational domains, and the growing institutionalization of the term in doctrinal documents and international security agendas. It is a concept that has gained centrality in academic and strategic debate over the past two decades. With cyberspace, social media, and digital networks, information ecosystems are becoming privileged domains for influence operations, and disinformation and sabotage are producing transnational impacts at a relatively low cost and with a high degree of ambiguity regarding attribution.

The result is a great, ambiguous, and contested space in which strategic competition unfolds permanently, through a combination of instruments that challenge traditional models of response. This concept can be examined through five distinct perspectives.

Firstly, the structural transformation of the security environment, the acceleration of geopolitical uncertainty fuelled by intensified competition among States, the emergence of this disruptive behaviour by major powers, the rise of new centres of power, and the contestation of the international order create a complex scenario that is further aggravated by a technological revolution that amplifies vulnerabilities and decentralizes the strategic use of information, and with it, the battle of narratives. Recent history shows us that major powers, as well as small actors, employ a broad range of instruments: diplomatic, informational, military, economic and cyber, operating in a coordinated and synchronized mode, below common perception. Their

objective is not to trigger open conflict, but rather to alter balances, condition political decision-making and undermine the internal cohesion of the States. Russian operations in Ukraine since 2014, and the manipulation of democratic processes are current paradigmatic examples of this approach. They reveal a strategic matrix in which perseverance, influence, disruption, and intimidation are combined, often without clear attribution or through plausible deniability, taking advantage of the inherent difficulty of attribution. This is the defining characteristic of hybrid threats.

Second perspective: hybrid threats and disasters as a disruption multiplier. From a conceptual standpoint, the ambiguity surrounding the term «hybrid» reflects precisely its nature, with conflict adapting to contests in which the political and military cost of a direct confrontation is excessively high. It is therefore essential to recognize that, within a broader security framework, hybridization is above all a strategy of competition. However, today we must also consider a new reality, which deserves particular attention, reflection, and discussion: the use of disasters as a multiplier of hybrid disruption. When a State faces devastating wildfires, severe floods, pandemics, large-scale energy blackouts, or cyberattacks, it is not merely confronting a civil emergency; it is also exposure to the possibility that hostile actors may exploit a vulnerability to amplify this disruption, manipulate perceptions, and undermine societal trust. In moments of profound crises, it becomes easier to manipulate narratives and spread automation, exploit fear and uncertainty, apply pressure on saturated logistical systems, infiltrate support or volunteer networks, disrupt supply chains, weaken social cohesion. In short, a natural disaster can rapidly become a strategic opportunity for those seeking to influence, divide, or destabilize the State, fostering the perception, real or fabricated, that the State is failing to fulfil its sovereign functions.

Third perspective: impacts on small and medium-sized States. Many States face additional challenges due to their size: economic exposure, external dependencies, social openness, and deep integration into global networks. These characteristics, which are essential assets for our prosperity, also make the country more permeable to influence campaigns, disinformation, economic pressure, espionage, or cyberattacks. Disinformation is a key aspect of this. Consequently, it is imperative to strengthen national resilience in all dimensions: political, social, economic, technological, and military, since no modern State can respond in isolation to hybrid threats, disregarding borders and exploiting combined vulnerabilities. Hence, in-

tegration within international alliances, like NATO, the European Union (EU), and multilateral coalitions, are vital; not merely out of solidarity but out of strategic necessity. This reality highlights the dialectic between solidarity and participation. Countries, such as Portugal, require the collective, political, military backing of alliances. In return, however, they must also assume their share of responsibility, contributing actively to shared security, investing in relevant capabilities, and participating in response alert and cooperation mechanisms through national plans that must be integrated at collective levels.

Fourth perspective: States' preparedness for hybrid threats and disasters is critical to emphasize that no modern State can address hybrid threats and large-scale disasters independently. Therefore, this will always be a multidimensional struggle. It requires an integrated approach, based on a whole-of-government and a whole-of-society perspective. It demands that ministries, armed forces, security forces, intelligence services, regulatory authorities, the private sector, academia, and civil society align around a shared understanding of the problem. This entails strengthening situational awareness, based on an integrated intelligence system, with strategic surveillance and the ability to detect patterns of influence, manipulation, or infiltration; reinforcing institutional resilience, by strengthening critical infrastructures, communication systems, supply chains, and decision making structures, ensuring that legal and political frameworks adapt to the ambiguity of threats, enabling rapid, proportional, and effective responses, and promoting a culture of security disseminated throughout public administration, business, and among citizens.

Preparation for the next crisis, whether natural, technological, or hybrid, begins long before it occurs. None of these elements can be improvised; anticipation requires political continuity, sustained investment, and permanent inter-ministerial coordination.

Finally, the fifth perspective: the role of the armed forces in a hybrid environment and disaster scenarios. In a strategic environment marked by the hybridization of threats, and by the increasing frequency and intensity of disasters, the armed forces unequivocally retain their partitions, ensuring the military defence of the state. This mission continues to rest upon the maintenance of spreadable, modern, and effective conventional military capabilities, capable of responding to high-intensity scenarios. Hybrid warfare

does not eliminate these requirements; on the contrary, it reinforces them. Deterrence ultimately continues to depend on the existence of robust, ready, and interoperable conventional forces. At the same time, however, the armed forces – and the army, in particular – are increasingly called upon to play an enhanced role in supporting society during crises, within the framework of military emergency support. This support should not be understood as supplementary or circumstantial, but as a structural component of national resilience, fully integrated into the emergency and civil protection system. This framework requires military emergency support to be resized in two fundamental levels: planning and intervention. Such resizing must be fully embedded with the doctrinal and legislative architecture of civil protection, particularly with the national plans, which must be strengthened to ensure clarity of responsibilities, rapid decision making, and flexibility of employment. The model should be based on scalable logic. In an initial phase of response, priority should be given to capabilities resident within the national civil protection structure, complemented by the selective use of certain military capabilities, particularly those that are specialized and absent from the civilian system. In a subsequent phase, when the scale, duration or complexity of the disaster so requires, the role of the armed forces becomes more robust and structuring, ensured not only by the quality but also by the quantity of resources deployed and by the broader employment of the differentiated military capabilities. In this context, it is important to highlight the structural advantage of the Portuguese army: its extensive territorial dispersion, its nationwide presence allows greater proximity to populations and more refined knowledge of the terrain; and, above all, a faster initial response is a decisive factor in emergencies. Added to this, it is the dual-use nature of many military capabilities, designed for combat but also fully employable in disaster scenarios, like engineers, logistics, transportation, communications, energy, health command and control, and cyber defence capabilities. In these contexts, this demonstrates significant strategic value, directly contributing to the protection of lives, the stabilization of the situation, and the restoration of normality. But what is foreseen as a reform, the framework described, makes it clear that we are facing a structural paradigm shift to respond credibly to hybrid threats and major disasters. The armed forces – and the army, in particular – will necessarily have to grow. They must grow, first and foremost, from a conventional perspective, within the scope of land forces 2025. The Army must continue to develop capabili-

ties compatible with the commitments assumed within NATO, particularly in meeting NATO capability targets, ensuring readiness, interoperability, and high-intensity combat capability. But they must also grow in terms of emergency support capabilities. Recent events have clearly demonstrated that these capabilities are not indispensable to State resilience and the protection of the population. This growth should be based on a scalable force employment model, enabling the army to be deployed progressively, adjusting the volume of resources and the type of capabilities to the severity of the situation. Such a model should rest on a dual-use concept of military capabilities, without compromising the core defence mission, while recognizing the need to maintain a set of dedicated and resident capabilities in this domain. It is within the framework that the importance of structure, specifically dedicated to military emergency support, such as the military emergency support regiment, becomes evident. These constitute a national strategic asset and must be preserved, consolidated, and strengthened. The way forward implies sustained investment in critical capabilities, reinforcing interoperability within NATO and the European Union (EU), deeper interagency cooperation mechanisms, and the full integration of the armed forces into the national civil protection structure. Above all, however, it requires recognizing that national cohesion is the first line of defence against hybrid defence. Trust in institutions, clarity of political objectives, the solidity of strategic culture, and social resilience are as decisive as any military capability.

In conclusion, hybrid threats are not a temporary phenomenon. They represent the contemporary expression of strategic competition and will continue to shape international security in the decades to come. The same applies to major disasters, which are occurring with increasing frequency and destructive scale, demanding a robust response and the entire emergency and civil protection system. Portugal, as an active member of Europe, the Euro- and the Atlantic alliances, has not only the duty but also the responsibility to prepare and contribute within its sphere of responsibility. The Portuguese army is committed to this mission to adapt, learn, cooperate, innovate, and defend, in all domains, the fundamental interests of the State and the security of the Portuguese people. A strong Portugal, a strong Europe, and a strong transatlantic community depend on our ability to understand and confront, with clarity and determination, the complexity of the world that lies ahead.

Challenges of Governance Encountering Hybrid Threat

Evgenia Karatari

This discussion outlines the cooperative framework while evaluating the foremost challenges confronting both the European Union and the broader international community.

Prior to the core analysis, this section introduces the division and delineates the strategic contribution of the situational room to addressing hybrid threats. This situational room, which is part of the class response centre at the European External Action Service, is the civilian 24/7 capability, working around the clock without any interruption. This has been the case since 2002, when the first nucleus of the situational room was created by the then High Representative, Javier Solana. Mr. Borrell attended the spot brief on the invasion of Ukraine by Russia and followed the first developments in this situation room.

The reason for Mr. Borrell, together with duty officers and military, to join the situation room, was to obtain what is called – and what is a basic part of addressing hybrid threats – situational awareness. So, Mr. Borrell got situational awareness instantly.

What are hybrid threats as a concept? This analysis adopts the definition established by the Centre of Excellence, the leading authority on countering these threats. This concept refers to coordinated and diplomatic actions that deliberately target the systemic vulnerabilities of democratic States and institutions. As a pertinent digression, what do the actors do? First, they identify the existing vulnerabilities, and they exploit the threshold of detection and attribution. So, they know that it is difficult to attribute the attack, because they really work in what is called «in the shadows» and blow most of the time in electronic measures and means that are not easy to identify to whom they simply belong.

What are their objectives? To sow doubt, divide societies, influence decision-making and achieve strategic goals without triggering military conflict, so these actors operate below the open warfare threshold. The actors are always coordinated and they aim at manipulating, targeting, or threatening to harm a target, being a state or an institution, while operating below the threshold for what has been known as traditional warfare. In the

current operational environment, one can see that the means employed are a combination of military and non-military. The target is to destabilize and undermine either States or institutions. So, they operate in a profound geopolitical ascendancy, but it goes to the advantage of these actors. The radical technological change is in their favour as well, so they exploit old chronological solutions quite efficiently. And, as they are difficult to attribute, one has to deal, in the military and non-military means, with State and non-State actors, with conventional and also unconventional tools targeting governmental structures, armed forces, and, most importantly, the cohesion of our societies. Overall, these are conventional and asymmetric methods of action. The current operational environment is the manifestation of cyberattacks, disinformation, attacks on critical infrastructure, economic pressure, legal coercion, and also weaponization of migration, but also attempts to undermine democratic institutions and cultural social cohesion; the main characteristics of these attacks are deliberate ambiguity, difficulty in attributing responsibility, and exploitation of democratic and open societies. Thanks to democratic openness, these actors find their way in.

How are these threats perceived at the European level? EU is multidimensional and cross-border, so they do not remain within the national borders of any given Member-State, or even within the borders of the European Union – they go across borders, always. Even if there is an attack on the soil of a specific Member-State, there are always repercussions for the other Member-States, and, in any case, any attack on a Member-State is an attack on the Union overall. They always require a collective response, so no one can do it on their own, and the EU needs to give emphasis also to interoperability, both from the side of the perpetration – if they use interoperable measures, the EU has to use interoperable measures in order to address –at this point, one needs to keep, as a key takeaway, that no country can address these threats alone.

To illustrate these threats, this section examines the entities that have demonstrated the highest levels of recent activity. Over the period of approximately seven years, the existing Russian activities across Europe involve different kinds of attacks: sabotage on critical infrastructure, sabotage, other attacks have to do with assassinations even, certain GPS jamming, spying, weaponizing migration and vandalism and terrorism, and I would say here the sky is the limit.

The new policy for addressing hybrid threats lies around four general lines of action. Situational awareness is crucial because Member States need to be aware of the challenges, informed on their decision-making, and, most of all, develop a common strategic culture. For this reason, they need to share the same level of information. Resilience encompasses the capacity to prevent, withstand, and recover from crises, including multifaceted hybrid attacks, which differ significantly in their nature. Most of the time, for example, an attack is always preceded by a cyberattack, combined simultaneously with other types of attacks, for example, the weaponization of migration. The European Union extends its support, beyond its Member States, to neighbouring nations, fostering internal resilience through the deployment of dedicated missions and operations. A specific project was developed by different academic institutions and funded by the United States, which aimed at building resilience in these specific countries. And finally, 4th cooperation, maybe the most important aspect. The European Union is committed to working on countering hybrid threats with international partners and organizations, as well as with stakeholders from civil society. Regarding the whole-of-society approach, this response cannot only be in the hands of the government or the military, but it must be in the hands of civil society. The same society organizations, even the private sector, for example, cyber companies, can be very decisive in how to counter hybrid threats. That it is not only important to make our own societies resilient and protected against hybrid threats, but also to those close to the EU's progress and beyond. And why? Because these have a cross-border effect.

Concerning the policy framework, since the EU works under specific legal policy frameworks, the 2016 «Joint Framework for Countering Hybrid Threats» and the 2018 «Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats» have been developed in Brussels. Through these frameworks, we understand that countering hybrid threats is primarily a national responsibility. However, the EU can facilitate member States cooperation, develop policies, and solutions, and encourage sharing the best practices. It was the strategic compass that had a structure for developing a hybrid toolbox for addressing the hybrid threats. This effective compass represents a strategic framework through which we counter hybrid threats. It is structured in four main axes: act, secure, invest, and partner; it introduces the operational logic, so it is not simply limited to policy and words: this strategic compass comes to operationalize the EU's po-

litical frameworks; it foresees to carrying out joint threat assessments and to reinforcing preparedness and prevention. The strategic compass has been, and still is, the basis of all operational planning.

And this represents the nutshell, the hybrid toolbox that was developed following the strategic compass adoption. This initiative represents a strategic effort to operationalize all available EU instruments: political, cultural, societal, legal, military, and defensive, and even spatial. Disinformation-related infrastructure intelligence, economy, and economic indicators suggest that these cycles will be happening even more in the future, depending on the adaptability shown to identify new areas where the EU will have to be more operational, in order to address a new nature of hybrid threats, because what is known today is what has already been mentioned, but tomorrow maybe unexpected security vulnerabilities will inevitably emerge, driven by technology, AI, as well as the creativity of State or non-State actors.

For instance, some concrete EU responses are the FIMI toolbox, foreign information manipulation, and interference. Consequently, the conceptual framework has expanded beyond mere disinformation to encompass broader, coordinated operations intentionally designed for foreign interference.

The cyber diplomacy toolbox and the assumptions

The EEAS has various tools and structures, some of which have already been mentioned. As tools, early warning is one of the basic activities of the EU situational room – working on a 24/7 basis – to be able to provide early warning to the EEAS. Although the EEAS receives early warnings, it lacks formal information-sharing with other EU bodies, focusing solely on situational awareness. Threat analysis and strategic communications are also shared with federal Member States; EU versus disinformation is a public website, where all the actions related to the effort against Russian disinformation are presented. This is a tool that has been developed by the strategic communications of the EEAS. It's very useful to use, and it's updated daily.

Regarding the public structures, an internal procedure has been developed for the crisis response mechanism. This procedure stipulates how the services have to proceed during a crisis. As an operational tool, the EU Situation Room serves as the hybrid fusion cell within the EU Intelligence and Situation Centre (EU INTCEN), the policy planning and strategic communications, so, the strategic communications are mainly responsible for addressing FIMI and receiving contributions from the situation room. There

is also a Hybrid Threats and Cyber Division; this is part of the Security and Defence Policy Directorate (SDPD). This division is responsible for preparing policy for preparedness and exposure, as well as dealing with international cooperation and partnerships. So, what is most relevant is that the EEAS possesses an information hub that has to do with hybrid threats and that cooperation within EU Member-States and international or regional organizations is part of the core business of SDPD.

Concerning cooperation with NATO, the main partner, we have a joint declaration of works, 16 and 18, respectively. It is important to be aware that 20 out of 74 common proposals for cooperation are related to countering hybrid threats, for enhancing resilience, for situational awareness, and countering disinformation. The organizations work and operate complementarily, and not competitively. This cooperation has been quite smooth, mainly through lessons learned, regular meetings, and the base exercises, where SDPD has been integrated as well.

In conclusion, the key takeaways are as follows: countering hybrid threats is a continuous process of adaptation and evolution, so it is not something that we have understood today, and the EU cannot be taking these measures for the next decade. Why? Because technology is not working to our advantage, but it can work, so on our side we need to use technology in an effective way, in order to counter hybrid threats. The EU needs to remain united, flexible, and cooperative, invest more in operational capabilities, and in its founding values. So, we need to maintain our freedom of speech, our democracy, and our democratic values, and in no way let those actors really undermine our societies in that respect. So, this reality in equation: collective action, plus prevention, plus resilience building, will ensure security, stability and democracy in Europe.

«Hybrid war does not announce itself. It does not wear a uniform. Clausewitz taught us that war is clouded by a fog of uncertainty. Hybrid war goes further: it deliberately creates and weaponizes that fog. It operates daily, quietly and persistently». This quote was written by a retired ambassador of Cyprus. This country happens to have the presidency of the Council of European Union, and it is very illustrative of what hybrid threats represent and how it operates.

Emilie Berthelsen

With this idea that hybrid activities are certainly reshaping the contemporary security environment, there must be a discussion about drones, based in Ukraine. While Ukraine is not a full-scale war, currently, as one of the most extreme examples of the need for resilience and adaptation, there is a lot to potentially learn from them. This analysis will focus specifically on this idea of continuous adaptation by adversaries. When one's vulnerabilities are exploited, they tend not to wait for someone to do it again; they try to fix it. That means that it is not a constant challenge being faced: the pressure is there, constantly, but the path it pursues changes over time. Additionally, deterrence by denial is not often as possible as one might prefer. When it comes to sort of unusual military activity, it often pushes the boundaries of imagination, and compounded by new technology, there are new challenges that may not have been predicted. Drones illustrate that dynamic. Consider Denmark, which has had a lot of trouble with drones recently. That goes in terms of drones over military installations, over commercial airports; however, that seems to be a European issue at this point. For example, Estonia, just a few weeks ago, and the UK, a few days ago; not only are drones a big issue nowadays but also Unmanned Surface Vehicles (USVs) and Unmanned Underwater Vehicles (UUVs) are also emerging as critical challenges. This is seen around critical infrastructures, in Denmark, with the maritime cables, for example, those have been in a bit of trouble in the Nord Stream line. Things are becoming vulnerable due to technology evolving. This creates new threats to the hybrid space: it lowers the barriers within the traditional conceptualization of war, committing immoral or illegal attacks, but it also risks actually contributing to arms race dynamics because it partially lowers the risk of attribution first, because there are no people on the ground necessarily, or if they are, they might be a bit away from the action; and the democratization of this technology means that more actors have opportunities to get involved. There are clear consequences of this, and whether this inflicts harm or just causes confusion, it undermines the belief in our institutions. This is a massive issue. Drones are part of the challenge of hybrid threats. However, they can also be part of the solution, but not in the way one might imagine. Of course, there is much more to hybrid warfare than the military; however, the military has a significant role here. When threats are not necessarily preventable, or they are not easily preventable or

predictable, then resilience and adaptability become very critical elements to have. That is, of course, a societal thing, but it also goes to the armed forces. When there are new challenges that evolve, that change over time as the adversary evolves, as they produce vulnerabilities, how does one then adapt to that? That is where there is something to potentially learn from Ukraine.

The reason Ukraine is a good illustration of this is that this can be summed up in a short quote: «A little Soviet army can't be beat by a big Soviet army». If you are playing the same game as someone who has an advantage over you, you are going to lose, so you need to play not on their rules. For the Ukrainians, that meant investing in something that was quick, scalable, and exploited Russian vulnerabilities – that was drones. The academic view of drones has traditionally been focused on this sort of surveillance role, moving to a more active battlefield weapon; now it's been re-conceptualized within the hybrid warfare world. What is important is this sort of rapid development and adaptation cycles that are being driven by software because it removes the need for humans to manufacture new military complex systems. A tank takes years to develop and to produce, whereas a drone takes weeks. The threat is evolving faster and, potentially, so is its counter. However, that relies on non-traditional innovation pathways that involve entire societies, both in the development, in the production and in the distribution; and one of the things that is traditionally overlooked in academia is the role of producers, of those that engage in the actual adaptation, that are outside the ministerial organization. In Ukraine they have been key to understanding the development of drones. There is a forward deployment of private engineers that go along with the armed forces, who respond directly to the operational challenges as they emerge. This is not to imply that adaptation, sort of wild in the field, is necessarily the solution to anything, but when the threat evolves faster, then one's conceptualization of it, the way to counter it, becomes an immediate response, and in Ukraine that has looked like engineers on the front lines.

Consider four to six weeks as the maximum time most unmanned systems are usable on the frontline in Ukraine. As soon as they come into contact with the adversary, they become outdated because the enemy adapts as well. That displays something about the need for change, it is not a one-and-done instance where the threat is countered. This is about investing in continuous development. However, this is not just seen on the front lines; so much of this happens behind the scenes: it happens in investments into

technology, it happens in getting the right people together. Research and development happen directly on the battlefield, but the system that facilitates that is seen behind. This creates a new role for the State. The State is no longer a sort of predictor of what happens, but, together with the military, finds new problems, operational problems, and puts them out into the world, asking, "How can we counter this?". This is when the question becomes how we get the right solutions to develop fast enough, get them to the right people, at the right time. This is one of the potential suggestions we're seeing emerge from Ukraine. Of course it is not just about developing it; in order to have it create effects on the ground, we need to get it out there. That means adapting the entire bureaucratic system behind it. The military procurement system is generally rather slow; however, in Ukraine, because the speed of change is so quick, there is an actual need to get new products out to the front within a week. How do they do that? By building an online website, that helps people lower down in the system diagnose their problems, request technology, and get it delivered. The average delivery time on one of these is 11 days, reportedly, at the moment. When you do not necessarily need to carry out the massive reform of your entire armed forces, but you need a quick response to a problem over here, these are some of the things that might help you do it.

In considering how military innovation is thought about, many often think of bureaucracy dictating what needs to happen. In wartime, some tend to think about it as these reactive, immediate adaptations to what is happening on the front. Rather, we need to look across. In order to facilitate that rapid response speed, it is about reforming the bureaucracy; it is about creating new institutional entities that can go in and actually take part in, not just initiating development, but can be sparring partners in developing it and then making sure it gets to the people who need it. This also ties to the definition of military innovation versus defence innovation, where we think in defence industrial policies, these need to be closely linked to what practitioners need. This is what has been evident in Ukraine. It is not a simple solution, but by getting civil society involved and creating a huge capability base that can be drawn from, and integrating that into collaboration with the military, provides new opportunities for previously unavailable responses.

In conclusion, looking to Ukraine, what has given them a competitive advantage, is not necessarily the technology itself, and it is not the particular

institutions or organizations they have created; it is the combination of this ecosystem of actors that create a system capable of constant evaluation and development. In consideration of hybrid threats, it is wise to try to bring closer military practitioners that are part of this response and the civilians, who have the capabilities to develop it.

Roderick Parkes

Strategic foresight is the practice of trying to map out future eventualities, trends, opportunities. There is good foresight, and there is bad foresight: bad foresight, on the whole, means admiring the problem. It means thinking of endless eventualities for how the future, in our case, threats might play out, but not linking them back to opportunities for action. Bad foresight means you can be quite accurate in your assessment of the future, but if you are not providing political options, then you are doing bad foresight. Good foresight is active; it is always linking to thinking of future options, and future eventualities. The way to do that is to build a sense of self-awareness in whoever you are providing foresight for. It is important to show people how, in their past decisions, their habits of mind, they are ruling out certain options, and they are creating certain risks. It is effortless to do bad foresight when it comes to hybrid threats. It would be very easy for someone to look into the future and say, "AI, disaster management, whatever it may be", but all they have done is added to your complexity. Doing good foresight for hybrid threats is tricky because it is opportunistic, it is low cost, and the adversary is constantly adapting. As soon as we make choices, the adversary adapts against us. Nevertheless, at the Defence College, we are being asked, increasingly, to think about how NATO can act in this field, and in particular, how our past choices have created the threat landscape today, because that is the easiest way to reduce our vulnerabilities. The College is asked how we are inviting hybrid threats, how we participate in certain dynamics with our adversaries that create these, how we miss signals and trends. The basic understanding is that the best way to combat hybrid threats is not to try to anticipate what the adversary is going to do, because the nature of the threat is that you cannot control; that is the point of hybrid threats, but it is to be honest about yourself, about your own posture, your own choices, and the way you are creating these vulnerabilities. There are three or four dynamics that NATO is becoming increasingly aware of that it wants to combat,

things that have made us vulnerable and continue to make us vulnerable. A lot of those go back to 1989 and the immediate post-Cold War era, decisions around defence spending or public education or whatever it may be, but this analysis is not the classic narrative that NATO has currently, of seemingly bashing society for becoming naïve. There is much greater self-awareness among political and military elites that we have contributed to these problems.

The first example is how, increasingly, we think about the future of disinformation and cognitive warfare. One would say, at the heart of that, of our vulnerability and of shaping the threat landscape, is society's ability to debate security issues in a mature way. It may be that many would look at the future and say, "The threat landscape is a worrying one, with AI, and so we will see a significant rise in disinformation and cognitive operations". However, many would probably reject the conventional response to that, which is greater education and inoculation of publics, fact-checking and pre-bunking attribution, and StratCom, or at least take it with a pinch of salt, because from our perspective, that is precisely the kind of top-down and prescriptive, rather technocratic, approach that has taken us here: with security elites treating publics as too irrational to deal with security affairs and debate them themselves, but sufficiently rational that if we tell them how to act or what the threat is, they will accept that. The elites have ceased to trust society, and that trust, or lack of trust, is reciprocated again. Looking back at the post-Cold War era and the shift there, many would reject the usual narrative around that, which is to say that our societies all became naïve, complacent, and believed in the end of history, in the end of ideological competition. With a little more self-awareness, we would say, "Our organizations, at that stage, lost the ability to make persuasive ideological arguments in favour of greater security, greater foreign policy, or greater investment". We preferred thinner arguments that are no alternatives or pointing to an enemy, rather than positive arguments; and at the same time, we asked technocrats to behave in a political way, so that they would provide us with the authoritative data, which would say there is only one choice and we do not need a public debate on this. So instead of pointing the finger at society and saying, "you have become naïve, and complacent, you believed in the «End of History», I think we have to self-scrutinize and say this is much more about laziness on the part of political and military elites, that we cease to try to persuade society of the benefits of investing in defence and

security. The populist response to that, which is to re-politicize the truth data choices, that are not really choices, we are looking for other ways to do that. I think you can see it in the way that NATO handled its latest nuclear exercise: instead of heavily classifying everything and keeping it out of the public domain, the choice was to put a lot into the public sphere so that people could debate these implications, and on the whole, the response has been a positive one. That is the first shift. We do accept that there will be a rise in disinformation, and cognitive warfare, but the response is not a top-down, educational, fact-checking one; it is much more leaning towards the ideas that we must trust society, stop over classifying information, and put that into the public sphere.

The second example is around the future of hybrid warfare, grey zone operations, and so on. There, again, we would look internally, rather than towards the external threat landscape, when thinking about the future, and say, “It all comes down to our societies’ will to fight and their acceptance of our military power as an instrument of power”. Our expectations, going into the future, are that we will see a rise of unconventional means used for military purposes, and we heard before about the exploitation, for example, of disasters; and we will also see an increase of military means, such as drones used under the thresholds – we shared the same expectations as anybody else. Again, where we diverge increasingly is in the usual response. So, not primarily a whole-of-government response, a sort of all-hazards resilience where we are just crouching and waiting for anything to hit us, and not even necessarily the shift from welfare to warfare, that we are saying our societies have become complacent and we need to shift from welfare spending to defence spending as a way to wake them up. Again, we would now look at that with the degree of self-knowledge and say that these are precisely the kinds of policies that would have made us vulnerable in the first place: that we have invested in military superiority, but we do not have the societal backing to use it. That invites this kind of unconventional warfare that our adversaries are inviting us to duck out of the fight, by being just under the threshold, or mixing military and civilian means. The old NATO narrative around this, going back to 1989, would be to say, “Society is post-heroic”; we are not having enough children to fight; we like welfare instead of warfare, etc. With the degree of self-knowledge, firstly, we would say that our response, back in the 1990s and 2000s, was to disguise warfare: we still ended wars in Iraq, Afghanistan, and so on, but we did it out of area, we pretended

it was bloodless, and we used drones and other sort of bloodless technologies like that. The response now is to bash society, which is mistrustful of us, and to say, “You’re post heroic, you don’t like fighting, and you need to buck up your ideas”. NATO is moving around this understanding of popular mistrust of the military that is partly a response to our past policies. We also see the populist response to that, which is to politicize and romanticize the military, similar to what you are seeing in the US, around returning to the warrior ethos and so on. It is an attempt to bring back the use of power and the status of the military. We do not think that is very helpful, so what we are looking for, is new means of engaging with society, and the shift there is towards total defence policies. For NATO, that does not mean trying to militarize society and turn ordinary citizens more into professional military; it is much more about having a whole-of-society military, that we are trying to change military structures where possible to adapt to society.

The third and final shift is looking at the future of sabotage of cables, industrial production, and connective infrastructure. There, again, we must look inwards and consider that we are creating our own vulnerabilities. Consider allies’ pursuit of European autonomy. We would connect our future vulnerabilities to the pursuit of European autonomy. The thing that is often perceived as the solution to our vulnerabilities would actually be the cause of them. The NATO expectation of sabotage and attack on infrastructures is that we probably expect them to become more brazen, and deadly, also more tit for tat – if we are doing certain things in Ukraine, certain things will happen in the Baltic. However, perhaps we would reject the classic response, which we are seeing on the EU side, which is to try to cut connections to the outside world, to push towards buying and making European, to reduce dependencies on the outside world, to build up an EU market on defence and investment. The sense, increasingly, is that we are creating greater connections internally at the expense of our connections outside, and that is making us more brittle and dependent on the outside world. Again, the classic narrative post-1989 is the one that we are revisiting. The classic narrative would be to say, “Europeans believed in globalization, and they went out and created many dependencies”. If you look back now, with the degree of self-awareness, you would say the EU created heavy internal vulnerabilities and connectivity but put up a protective wall around itself. The pursuit of European autonomy, in many ways, created today’s situation in terms of antagonizing the US and in terms of potentially worsening

the security situation in neighbours that depend on access to the European Union for its markets. Obviously, there is a NATO angle to this. It is very undesirable, with European autonomy, that Turkey, Norway, and the UK be excluded from European security; but there is a greater sense where the EU pursues autonomy, and it not only becomes more of a target, it also becomes less relevant globally, potentially, because it is cutting itself off. So, you will start to see sabotage acts that become much more about signalling rather than trying to disrupt, much more connected to other global theatres, rather than about Europe, and possibly focused more and more on neutral States in Europe, in a bid to say “the niceties of Europe matter less than they did because Europe matters less than it did”; and also forcing neutral States to take sides. The pursuit of autonomy carries those risks. Within NATO, we share a perception of hybrid threats but also know that we must move the EU less towards autonomy and more towards the idea of indispensability. That means that the EU is making a vital contribution either to security, as an ally, or to production, which means that attacking it carries those costs. I think increasingly we would say the response to all these negative dependencies that Europeans have is not to try to cut off these dependencies, but perhaps to replace them with indispensability, that both sides have an interest in holding them.

In conclusion, we see that NATO allies are becoming more active. We see a shift towards greater readiness for cost in position when it comes to hybrid attacks that we’re ready to deter by punishment. There is a shift, potentially, towards cumulative attributions, a «three strikes rule» that says, “We do not need to prove attribution each time; if we can say that you have been doing these things in the past, then we will react”. Additionally, at a national level, there is more of an offensive posture, particularly in the cyber realm. All these things point to NATO allies using their choices to shape the threat environment more actively. What is worrying is if that offensive posture, or that active posture, is not based on self-awareness of our own vulnerabilities and our habits of mind. At the heart of this it is not so much that society mistrusts politicians, business people, the military, but the other way around: the political business and military elites do not trust society. We look at voters and we say, “You are not mature enough to debate security; you have become complacent, naïve, etc.” Trust begets trust, and mistrust begets mistrust. The root of both, very often, is a distance from people and a lack of understanding of them. If you feel cut off from the people you depend

on, as you would in a wartime situation, or even today, in this tense security situation, you typically mistrust them and think the worst of them. The real story of the post-Cold War era, post-1989, is about elites becoming cut off from society; it is about politics becoming a profession in itself; it is about small technocracies in Brussels; it is also about military professionalization and shrinking the end of conscription, the creation of highly trained small militaries. All these things have created social distance between elites who sit on our military bases or in Brussels HQ, behind large walls, trying to understand the societies, which do not seem to understand us. Increasingly at the heart of NATO's rethink is the effort to reduce these barriers, to be out and about in society, to trust people with information: declassifying, putting things out in the public sphere, so that they can take informed decisions.

The goal of all this is to try to build up an allied security culture where our citizens are informed, they are vigilant, and they are active.

