HYBRID COE

Hybrid CoE Working Paper 12

OCTOBER 2021

Calibrating the compass: Hybrid threats and the EU's Strategic Compass

RASMUS HINDRÉN

Hybrid CoE

Hybrid CoE Working Paper 12

Calibrating the compass: Hybrid threats and the EU's Strategic Compass

RASMUS HINDRÉN

Hybrid CoE Working Papers cover work in progress: they develop and share ideas on Hybrid CoE's ongoing research/ workstrand themes or analyze actors, events or concepts that are relevant from the point of view of hybrid threats. They cover a wide range of topics related to the constantly evolving security environment.

The European Centre of Excellence for Countering Hybrid Threats tel. +358 400 253800 www.hybridcoe.fi

ISBN (web) 978-952-7472-00-2
ISBN (print) 978-952-7472-01-9
ISSN 2670-160X

October 2021

Hybrid CoE is an international hub for practitioners and experts, building Participating States' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats, located in Helsinki, Finland.

Contents

Introduction

The EU has embarked on a strategic reflection process which should result in a document called the Strategic Compass. It aims to update elements of the EU Global Strategy from 2016, while retaining a more focused and operational tilt. The Compass should clarify the EU's assessment of the security environment, define the level of ambition in security and defence matters, and offer concrete tools and proposals to achieve that level of ambition.[1] The Compass is set to be finalized during the French presidency of the EU Council in 2022.

As always, expectations will need to be managed, not least because security and defence issues remain contentious within the EU. Some member states value their neutrality, non-alignment or similar status,[2] others pin their hopes on and put their trust in the transatlantic relationship, while still others try to advance a European defence union.[3] Added to this strategic imbalance is the portrayal of the EU as a peace project and a post-modern actor that transcends the classical security dilemmas. This thinking has been enshrined in the treaties and while the Maastricht and Lisbon Treaties have done much to enable the evolution of the EU's defence dimension, the treaties continue to be a limiting factor for the EU in understanding and coping with the threat environment.

One particularly pernicious side effect of the treaties and the EU's strategic self-image has been the strict dividing line between the Union's foreign and security policy and internal security policies. While in the previous century this kind of division might have arguably been possible, today's threats cut across state lines, government sectors, competencies and authorities. The situation has been further blurred by the expansion of hybrid threats. The malign actors deliberately target the gaps and seams between democratic countries, government sectors and EU institutions, and exploit their relative inability to respond flexibly or control escalation. The current security environment is best described as constant competition. It is not war, but neither is it strictly speaking peace.[4]

The threat environment requires adaptation from all actors involved. For the EU, the Strategic Compass is a chance to give guidance for operating in a new threat environment and with a view of the future trends, not least the rapid pace of technological development and the opportunities and threats that it presents. The Strategic Compass also offers an opportunity to establish common strategic situational awareness. It will not lead to a harmonization of member states' interests, but it should lead to a better understanding of those interests and to the conclusion that the EU needs to be more capable of protecting those interests.

Oftentimes, the EU is mainly in the role of a facilitator of member states' efforts. Sometimes the EU must act, wielding the considerable tools it has in its toolbox. Some of the changes in the threat environment are rather well suited to the EU's modus operandi and structural strengths, and some are less so. In any case, as the threat picture is more complex than before and as situations requiring an EU response might arise at short or no notice, a new approach is needed.

This approach will be explicated in this Working Paper in three steps. The first step consists of a look at the development of the EU's security and defence dimension until now, and an analysis of the threat environment and the concept of hybrid threats. The second step entails the introduction of the concept of deterrence in the EU strategies, in a way that is compatible with national approaches, and which harnesses the EU's tools in the most effective manner.

Finally, the third part looks at ways of improving the EU's responses. Applying the concept of hybrid

1 See for instance Biscop, 'From Global Strategy to Strategic Compass'.
2 Cramer & Franke (eds.), *Ambiguous alliance*.
3 Engberg, 'A European Defence Union by 2025?'.
4 See for instance Torossian et al., 'Hybrid Conflict, Neither War nor Peace'.

threats and the deterrence model allows us to see that in order to be effective the EU must be better at bridging the gaps between the various actors: the member states and the council bodies, the Commission as well as the Parliament. This can be framed as an integrated approach, based on better information sharing, agile and comprehensive decision-making mechanisms, and through exercises.

While in many ways the analysis seeks to be applicable to the EU as a whole, the emphasis is on domains and policies that could realistically be covered by the Strategic Compass. This approach is chosen to make it as relevant as possible for the ongoing deliberations within the EU context. At the same time, it is intended to give planners and decision-makers a perspective that extends beyond the traditional security and defence policy realm.

The development of the security and defence dimensions of the EU

In the early days, in tune with the threat environment of the 1990s and the early 2000s, the focus of the European Security and Defence Policy (ESDP, renamed Common Security and Defence Policy, or CSDP, after the Lisbon Treaty) was on crisis management and developing the capabilities necessary to conduct crisis management operations. The focus on external action meant that the debate rarely touched on the key competencies of the Commission. At the time, there was also very little overlap with the Justice and Home Affairs (JHA) area.[5] This meant that the Commission largely stayed out of the defence policy discussions in the Council. When it started to enter the defence debates, it happened in the context of industrial policy instead of foreign policy.[6] The "defence package" that included two defence-related directives came into force in 2009.[7] This was complemented by various member state-led initiatives established during and after the fallout from the financial crisis. The crisis put defence budgets under severe strain, forcing more cooperation and a better leveraging of the EU instruments.

The precedent established by the directives, and the dawning defence cooperation led by economic imperatives, paved the way for a more thorough rethink about the relationship between the policies completely or partially within the Community competence, and the policies within the member states' competence, such as foreign and security policy. This reflection process culminated in the December 2013 European Council, which, in the words of the president of the European Council, Herman van Rompuy, looked at the "state of defence in Europe".[8] The meeting was a watershed moment. It managed to raise the topic to the level of the Heads of State and Government, but it also managed to bring the various aspects of defence, from capability development to operations, together to form a comprehensive package. This was unprecedented as it broke several taboos. First, it allowed the agenda to be expanded beyond the CSDP paradigm, which in its strict interpretation covers only external action. Second, the European Council preparations were divided between the External Action Service (EEAS), the European Defence Agency (EDA) and the Commission, assigning each a significant role. Third, it was decided that the Commission would start to fund defence-related research for the first time, in the context of the Preparatory Action on Defence Research (PADR) to begin with.

While not leading to major immediate successes, the process and the European Council decisions that followed broke important psychological and institutional barriers. Those were the crucial intermediate steps before new ones could be taken. While the 2013 process could largely be seen as a response to internal factors, the process since 2014 has been more due to external factors. The first external factor was the invasion of Crimea by Russia, and the second was the election of Donald Trump as the president of the United States. Ukraine brought a sense of urgency and an understanding that crises can still erupt at the borders of the Union and, just as crucially, that new strategies of malign influencing combining different methods can affect the member states themselves under the threshold of an open conflict. The threat environment became clearer and muddier at the same time. It necessitated a renewed focus on territorial defence while at the same time requiring a better understanding of the other societal and non-kinetic threats and means to counter them.

5 As the JHA has risen on the political agenda, its overlap with external and security policies has increased. See for instance Trauner & Ripoll Servent, 'Justice and Home Affairs in the European Union'.
6 Arteaga, 'Strategic autonomy and European defence'.
7 Defence Procurement Directive 2009/81/EC and the Intra-Community Transfers Directive 2009/43/EC.
8 Van Rompuy, *Defence in Europe: pragmatically forward.*

While several useful initiatives have been undertaken, progress thus far has been characteristically uneven. The member states' views continue to differ with regard to security and defence policy-related objectives. The threat assessments vary, as do the solutions. Countries that are sceptical of the EU taking on a bigger role in security and defence justify their views by either underlining their overall reluctance to have more integration, pointing to the spotty record of the EU so far, or on the need to sustain the transatlantic relationship, referring essentially to the security umbrella that the United States provides. Therefore, the United States possesses a major possibility to influence further progress in the EU defence dimension.[9]

The point that needs to be underlined is that even if the US decides to lend more weight to its support and if the European capitals become more united in their will to deliver on previous decisions, the internal and institutional challenges remain. They relate to the nexus of internal and external security and the delineation of responsibilities between the Union and the member states, namely how the strategic priorities should be set and when the EU should act. Before looking into these questions in more detail, a common situational assessment is needed, and a look at where the Strategic Compass can and should deliver.

9 Bergmann et al., 'The Case for EU Defense'.

Trends in the threat environment

When defining the threat environment, the EU will draw upon the Global Strategy[10] and the more recent threat analyses. There are two notions that would merit a closer look in framing the current environment, namely competition and hybrid threats.

In the United States, perhaps the most important legacy of the Trump era is the laser-like focus on strategic great power competition. The focus started during the Obama era but gained a greater sense of urgency later. The role of great powers in the competition has been analyzed thoroughly, but attention should also be paid to the term competition. While competition might not fully capture the current nature of the political environment, it serves as a useful conceptual intermediate space between conflict and peace.[11] The clearest signs of a threat environment characterized by competition are the constant probing of adversaries and potential adversaries, priming them for further actions, and operating in the "grey zone", a legally and politically dubious area where norms are challenged by hybrid actors and yet these deeds often go undetected or unpunished. Therefore, a successful way of competing must involve a lot more than just deterring war.[12]

Hence, the EU could do worse than take great power competition as a starting point. In the context of the Strategic Compass, perhaps strategic competition could be an even better term as it takes the agency of smaller and medium-sized powers into account as well. Most importantly, the focus should be on competition, as opposed to a strict and artificial division between conflict and peace, or war and peace. Furthermore, the rise of competition in the international arena should not be seen as a counterpoint for globalization, but rather as an extension of globalization by other means.

Competition in international affairs has two major characteristics that ought to be reflected in the debates around the Strategic Compass: it is more or less constant and it takes place mostly under the threshold of open conflict.[13] The fact that it is constant should require a rethink on how the West perceives the logic of conflict and escalation, and how it has structured its defences in terms of preparedness and decision-making. The reality of competition means that there is unlikely to be any "Pearl Harbor" moment when a clear threshold has been breached, setting in motion the decision-making processes, response actions and escalation management protocols. The reality more closely resembles another cliché, that of the proverbial frog in boiling water. It implies that we are already constantly experiencing hybrid influencing, including but not limited to cyberattacks, but as the attacks lead to relatively small effects, we remain oblivious or unable to muster a sense of urgency for responding. The attacks stay mostly below the thresholds of detection or attribution. Equally worrying is the fact that EU countries lack mechanisms for an effective and meaningful response.

Besides the rise and intensification of competition, the threat environment is also changing due to other trends. In addition to great power competition, a democratization of warfare is also taking place, exemplified for instance by cyberattack capabilities or drone technology becoming more available to smaller states, non-state actors and even individuals. This democratization trend reflects another broader trend: the rapid pace of technological change, especially in the context of emerging and disruptive technologies (EDTs). While, historically, talk of a revolution in the security environment has often been hyperbolic,

10 European External Action Service, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy.*
11 Friedman, 'The New Concept Everyone in Washington Is Talking About'.
12 Sisson, 'A Strategy for Competition'.
13 For a discussion on the meaning of strategic competition, see Mazarr et al., 'Understanding the Emerging Era of International Competition, Theoretical and Historical Perspectives'.

in the current situation it is warranted to talk about EDTs as a game-changer. Finally, there is a cognitive element involved. Most of the battles take place in our heads, as we try to make sense of the wealth of information and, too often, misinformation and disinformation available to us. The competition in the information sphere also reflects the differences between democratic and authoritarian regimes, introducing an ideological component to the competition.

Most of the trends discussed here can be understood under the concept of hybrid threats, which has entered the broader lexicon in the last ten years.[14] The 'hybrid' in hybrid threats refers to the way that malign actors combine and utilize different tools at their disposal. The tools target various domains from information, social and culture to space, cyber, and military domains. As the combinations of these tools are practically endless, the preparedness for hybrid threats should not exclude any of them.[15] Furthermore, the technological trends suggest that the portfolio of hybrid threat tools will expand.[16]

Besides the characteristics of the threat, the actors themselves need to be considered. Hybrid activities, up to the level of hybrid warfare, sometimes constitute a strategy on their own. However, they often support an existing strategy or policy in the eventuality that the strategy or policy is viewed as unsuccessful or failing. This means that traditional tools of international influencing like diplomacy, economic deals, and legal agreements alone do not allow the actor to reach its strategic goals. Usually the military-centric approach is excluded or may not apply and there is interest in minimizing the risk of open escalation or conflict.[17]

The EU has addressed hybrid threats in various Council meetings since 2014. The 2016 *Joint Framework on countering hybrid threats*[18] provided a nascent common understanding of the threats and a first blueprint for the EU's response. The concept has since been refined, including in the report *The landscape of Hybrid Threats: A conceptual model* by the EU's Joint Research Centre (JRC) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).[19] Currently, there is a relatively wide understanding of the term and concept within the EU. Unlike during the preparations of the EU Global Strategy, it would now be possible to use it as one of the anchors in the description of the threat environment, and of the EU responses in the Strategic Compass.

14 The concept has been accompanied by a wide-ranging and persistent debate, focusing on its analytical utility and the perceived tendency to overuse it (see for instance Raitasalo, 'Hybrid warfare: where's the beef?'; Wigell, 'Hybrid Interference as a Wedge Strategy'; Hoffman, *Conflict in the 21st Century*). One of the arguments within the debate is that the concept is so broad that it is effectively rendered devoid of meaning. It is certainly true that the most often used definitions cover a broad spectrum of threats. They are also intentionally flexible, allowing responsiveness to the ever-evolving nature of hybrid threats (see Hindrén & Smith, 'Understanding and Countering Hybrid Threats Through a Comprehensive and Multinational Approach').
15 Ibid.
16 See for instance Thiele, 'Hybrid Warfare'; Thiele & Schmid, 'Hybrid Warfare – Orchestrating the Technology Revolution'.
17 Hindrén & Smith, 'Understanding and Countering Hybrid Threats Through a Comprehensive and Multinational Approach'.
18 European Commission, Joint Framework on countering hybrid threats, a European Union response.
19 Giannopoulos, G. et al., 'The Landscape of Hybrid Threats'.

Countering hybrid threats by building deterrence

When assessing the EU's policy tools in countering hybrid threats, the list is long and growing. Gaps exist, but perhaps more importantly, an overall framework for organizing the tools is lacking. The question is essentially twofold: how do the EU and its member states build their resilience to withstand external threats, and how do they respond when threats actualize? Here the concept of deterrence is helpful as it enables actors to define the threat environment and their potential responses. While not entirely absent,[20] it has long been a concept with relatively little usage in EU circles. A coherent and explicit deterrence policy has been missing, not least because of the connotations pointing to the realm of nuclear weapons, traditionally the dominion of individual member states and NATO. The term still encounters opposition within the EU, including from the Union's only nuclear power, France, which has a very specific understanding of the term. Additionally, some of the member states see the term as a precursor of a creeping militarization, both in semantics and in substance.

Yet deterrence could now take on a new meaning in the context of the hybrid threat environment. The classical deterrence model still has value but should be complemented with a deterrence against hybrid threats.[21] Classical deterrence, while effective in its field, might also give a false sense of security because the adversaries are playing in other fields as well.

Hence, building on the classical models of deterrence, deterring hybrid threats requires a strategic approach that must blend "resilience and crisis response with the ability to impose cost on hostile actors". This is a crucial starting point that should not be lost in the broader discussions, which often tend to separate resilience from the foreign and security policy tools to be activated in times of crisis. The key lies in a combination of these elements, the "deterrence by denial" and "deterrence by punishment" of the classical deterrence theories. These elements can be complemented by other factors, including deterrence by diplomacy or deterrence by entanglement.[22] Another promising concept is "democratic deterrence", which is constructed primarily with the countering of hybrid threats in mind.[23]

Future threats will require a more flexible and more proactive approach that will not supersede the classical deterrence, but complement it instead. Thus, the application of a deterrence terminology and mindset is an opportunity for the EU to update its understanding of the security environment but, more importantly, to harness the power of its own capabilities and tools more systematically and more proactively.[24] The threat environment, as outlined above, requires exactly the kinds of tools that the EU seemingly has in abundance: the capability to regulate industries, to fund innovations and joint solutions, and to take a whole-of-society approach to security. It does not require the EU to actively forget the military-centric approach to security and defence because it never had the chance to learn it in the first place.

The two sides of deterrence are resilience and countermeasures. They are interrelated and must be understood as forming one deterrence package. In the EU context, resilience is by far the more advanced and politically feasible part of the package. It relates more to passive defences instead of active or politically riskier actions, and it is based on whole-of-society thinking.[25] Considering the relative "softness" of resilience,

20 See for instance European Commission, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*.
21 Taylor, 'From Strategy to Task'.
22 Kersanskas, 'Deterrence: Proposing a more strategic approach to countering hybrid threats'.
23 Wigell, 'Democratic Deterrence: How to dissuade hybrid interference'.
24 The primary responsibility for countering hybrid threats is at the national level. The argument presented here does not entail or recommend a shift of powers from the member states to the EU, but rather underlines the need to clarify the responsibilities, and aims to activate the member states to utilize the Union better in terms of capability development, situational awareness and countermeasures.
25 For a more detailed discussion of resilience in the context of countering hybrid threats, see Savolainen, 'Hybrid Threats and Vulnerabilities of Modern Critical National Infrastructure'.

it is only surprisingly recently that the EU has put it at the centre of its actions.[26] Part of the challenge has involved the inadequate conception of security, which has tended to separate internal preparedness for disasters and other crises from the foreign and security policy of the Union. Resilience has been enhanced without an updated and collated understanding of the threat environment and the malign actors using hybrid strategies. All of this can be remedied in the Strategic Compass and, to an extent, it already has been in the context of the threat assessment that was prepared in 2020.

On the other hand, it would be unfair to say that the EU hasn't been paying attention to resilience. It has initiated a number of ambitious projects that all support building resilience in the member states and throughout the Union. These projects include the Security Union Strategy of 2020[27] and its implementation, but also the Critical Entities Resilience directive, the NIS2 directive, Digital Services Act (DSA), EU Cybersecurity Strategy and its implementation, 5G guidelines, updated FDI screening rules, the Cyber Diplomacy Toolbox, the European Democratic Action Plan (EDAP), the European Defence Fund (EDF), Permanent Structured Cooperation (PESCO), and so on. Yet the EU hasn't consistently underlined the fact that all of these initiatives are in fact enhancing the resilience of the Union and its member states. The Security Union Strategy was a step in the right direction as it sought to specifically tackle resilience questions[28] with a view to establishing sectoral resilience baseline requirements.[29] Nevertheless, these approaches are destined to fall short as long as they cover only those aspects of resilience directly related to the Commission, without a thorough discussion of the strategic foreign and security policy environment and without setting the objectives for the sectors under the Council lead as well.

Countermeasures should also receive sufficient attention. The discussion about countermeasures in crisis situations is politically difficult and suffers from a lack of clarity about the responsibilities when there is a need to react to an influencing attempt or other type of external aggression. In most cases, the primary responsibility lies with the member states themselves. But what if the target is an EU structure, such as the European Parliament or the Galileo satellites? There are existing procedures for these cases, but if an adversary tests those procedures by deliberately probing for the gaps and seams in the EU response mechanisms, some vulnerabilities are bound to be found.

Deterrence is a relative term. The credibility of the EU's deterrence will not be decided by any of its strategies or even its capabilities. Instead, it will be decided in the minds of the adversaries, as they ponder the benefits and risks of engaging in a certain action. The EU cybersecurity strategy rightly points out that an "effective deterrence means putting in place a framework of measures that are both credible and dissuasive for would-be cyber criminals and attackers. As long as the perpetrators of cyber-attacks – both non-state and state – have nothing to fear besides failure, they will have little incentive to stop trying".[30]

Besides the issue of credibility, the comprehensivess of the concept also merits further analysis. Originally, it was focused on nuclear strategy and the need to prevent the escalation of any crises to the level of nuclear exchanges. During the Cold War, this was mainly achieved by the mutually assured destruction doctrine. The concept has been extended to conventional warfare as well, with the aim of managing the escalation of conflicts or preventing them from flaring up in the first place. Part of the reason that certain states have scaled up their hybrid probing and influencing activities lies in the fact that classical deterrence models have proved their usefulness. If countries and the EU focus on deterring hybrid threats, they will still need to ensure that deterrence is upheld in the nuclear and conventional sphere.

26 See for instance European Commission, *Communication from the Commission on the EU Security Union Strategy.*
27 Ibid.
28 See also Wigell et al., *Best Practices in the whole-of-society approach in countering hybrid threats.*
29 The Commission is currently working on a review of the existing regulation designed to enhance resilience. Depending on further guidance, the next steps could include identifying resilience gaps, developing EU resilience guidelines in line with the existing NATO guidelines, and leveraging the EU instruments to support implementation.
30 European Commission, *The EU's Cybersecurity Strategy for the Digital Decade.*

An integrated approach to preparedness and crisis response

By outlining the complexities of the security environment and showcasing the potential of the EU to tackle several of the emerging threats, the previous chapters sought to underline the need for an integrated approach. The EU has acquired valuable experiences from a comprehensive approach in its external action in general and crisis management in particular.[31] The experiences should be put to good use when devising the new approach, but it must be understood that the new threat environment puts a lot more pressure on the Union and its decision-making as it encompasses both the Council and the Commission competencies.

A greater level of integration must be achieved across several different axes. The first and perhaps the most important of these relates to the nexus between internal and external security. Reflecting on the 2016 EU Global Strategy, Real Elcano Institute Senior Analyst Felix Arteaga argues that the strategy "reiterates the need to connect the internal and external dimensions of EU policies" but it "does not try to resolve the discontinuity between the two dimensions".[32] On the other hand, many national security strategies "address the nexus from both directions, recognising that what happens in the internal sphere also affects their external action".[33] This would provide important guidance for the development of the Strategic Compass. While the Compass is narrower in its scope than the EU Global Strategy, it cannot ignore the fact that the line between external and internal is porous, and that the faultline is likely to be exploited by adversaries.

The trick lies in making the Council and the Commission work seamlessly together without any changes to the treaties or competencies. While difficult, it should not be impossible. Everything hinges on a relatively common threat assessment and a shared sense of urgency. Hybrid threats cut across key mechanisms aimed at sustainment of our societies, our democracies and our way of life. Sometimes this gets forgotten in the daily Brussels processes, which sometimes tend to be heavy on the bureaucratic side and too often driven by narrow national interests. In the Commission, it is also a matter of instituting a "strategic culture". In this context, it would mean increasing the understanding of security and defence- related issues, which has not been a Commission forte. It would also mean strengthening the interaction with the Council on security policy, and even losing some turf battles in order to achieve the common strategic objectives. In practice, it requires conducting a considerable number of exercises, especially when it comes to the hard parts. These include situations where there is a lack of clarity about the responsibilities, where less used treaty articles are involved, such as the relationship between Art. 42.7 (the mutual assistance clause) and Art. 222 (the solidarity clause), or when a given threat evolves and crosses the line between internal and external security.

A related aspect of integration concerns the relationship between the member states and the EU institutions and agencies. When is something a member state responsibility and when an EU responsibility? The Strategic Compass will be a member state-driven process, which distinguishes it from the Global Strategy, which turned out to have less than full endorsement from the member states. Having a full member state endorsement is critical and should be sought even when it means endless negotiations and watering down the level of ambition. Part of this process should be an effort to clarify instances where a multilateral – namely EU – approach is preferable to a national approach. This clarification should be made at two levels: preparedness and crisis response.

31 Fiott (ed.), 'The CSDP in 2020, The EU's legacy and ambition in security and defence'.
32 Arteaga, 'European defence between the Global Strategy and its implementation'.
33 Ibid.

Conclusions

The competition between world powers, together with technological changes, are driving a threat environment that is more complex, more unstable and more interdependent. There are several ways of trying to make sense of this and many countries are currently adjusting their security strategies to better reflect this new environment. The Strategic Compass should do this too but, in a way, it must fulfil an even stricter set of criteria: it must be politically digestible for all member states and it should, of course, be realistically implementable. To achieve this, the Compass should draw on a common understanding of the threat environment and make the best use of the EU's strengths.

The EU has already come a long way in developing its security and defence dimension. There has also been great opposition to this process, particularly where military matters and means have been concerned. Now there is an emerging understanding that developing the defence side has helped "normalize" defence issues as a part of the Union policies. Furthermore, the defence pillar has started to grow alongside all the other pillars relevant for countering hybrid threats. The recent trends have also underlined that defence does not take place in a vacuum but as a part of whole-of-society preparedness and responses. The interdependencies between security and other policy areas have increased dramatically. In theory, all of this plays to the strengths of the EU, which lie in its ability to muster a comprehensive approach, combining various actors and policy sectors. Yet it provides a unique challenge for the Strategic Compass, which should remain focused on security and defence to give the clarity and the strategic guidance required.

The Compass should start with the recent threat assessment, which underlines the complexity of the threat environment and the pervasiveness and evolutionary nature of hybrid threats. It must acknowledge the interdependencies of our societies and the various actors within them. Crucially, it should treat hybrid threats as a horizontal factor. Once this has been established, the Compass should turn to objectives. The primary objective should be deterrence as argued in this paper. Deterrence against hybrid threats consists of resilience and responses, and the EU could play an even greater role in assisting the member states to strengthen their ability to be both resilient and capable of responding to aggressions, while strengthening the institutions' own capabilities. Institutions, including the European Parliament, are not exempted from these dynamics.

As discussed earlier, there are several critically important resilience-building initiatives on the Commission side. Could the Strategic Compass be the vehicle for bringing all of the relevant aspects and projects together, and helping to ensure that they support the strategic objectives as the member states see them? At first, it seems to be putting overdue emphasis on resilience since it is one of the main baskets, alongside crisis management, capabilities and partnerships.[34] However, to provide the much-needed strategic guidance, resilience ought to be understood horizontally in the context of both internal and external security, and as cutting across the other baskets of the Compass. It would also be advisable to link resilience more closely to countermeasures as it sometimes entails the same capabilities that might be used to prevent adversaries from achieving their objectives, and to punish them. This is true in cyberspace, for instance, where the lines between defence and offence are increasingly blurry.

Enhancing the countermeasures is as important as it is difficult. In the context of the EU Foreign and Security Policy, active engagement is historically defined mostly in terms of diplomacy and the use of diplomatic tools, and, in the narrower sense of security and defence, in terms of crisis management. There has been evolution in this regard, as argued before, to include a better understanding of the interrelatedness of the external and inter-

34 See eu2020.de, 'Strategic Compass: Developing Strategic Principles'.

nal policies, and the need to leverage the instruments better, including in the context of defending Europe. The EU has also been honing its sanctions toolbox, which it has been using with some success.[35] Yet the Strategic Compass should bring the countermeasures into clearer focus, understanding them in the context of the new and dynamic deterrence against hybrid threats and leveraging the member states' tools and the Commission's tools. Sanctions can and likely will play a large role in the Union approaches as a whole, but the overall toolbox must be more comprehensive than that. Diplomatic tools are not sufficient either. There must be real kinetic capabilities, which do not need to be owned or operated by the EU, but which must be integrated into the overall EU approach. Consequently, the EU must be resolute in its communications. Language in the Compass can remain strategically ambiguous with regard to thresholds and the exact nature of responses, but it should be clear enough and, importantly, it must be backed up by real capabilities and a collective willingness to follow through.

All of the above is underlining the fact that the EU responses need to be horizontal in nature, across the dividing line between external and internal security and across policy sectors. Economic policy, technology policy and information policy all have security policy implications. The EU needs an educated workforce that understands these connections and looks for integrated responses. Strategic culture will need to continue being built. When insufficient or overlapping competencies become an issue, the European Council should consider these questions from a holistic perspective and provide strategic guidance.

In the same vein, the relationship between the member states and the EU must be further clarified. The member states should see the possibilities that the EU can bring in both enhancing resilience and supplementing the crisis response toolbox. They should insist on a deep relationship between the internal security and external security policies. Consequently, the Strategic Compass should have a direct connection to the Security Union Strategy and its implementation, including in the context of resilience and setting the baseline requirements for the member states and institutions alike. Finally, a window of opportunity exists in the EU-NATO relationship. Managing all of these interdependencies and taking a holistic, integrated approach to countering hybrid and other threats requires a clear articulation and a common view. The Strategic Compass could be the vehicle for achieving this objective.

35 Russell, 'EU sanctions: A key foreign and security policy instrument'.

Author
Mr Rasmus Hindrén works as Head of International Relations at the European Centre of Excellence for Countering Hybrid Threats.

Sources

Books, articles and reports

Arteaga, Felix. 'European defence between the Global Strategy and its implementation'. Real Instituto Elcano Working Paper 4/2017, http://www.realinstitutoelcano.org/wps/wcm/connect/1e698ba2-2ff0-4a6a-8b5f-0fad2dc0d122/WP4-2017-Arteaga-European-defence-between-Global-Strategy-implementation.pdf?MOD=AJPERES&CACHEID=1e698ba2-2ff0-4a6a-8b5f-0fad2dc0d122. [Unless otherwise indicated, all links were last accessed on 15 September 2021.]

Arteaga, Felix. 'Strategic autonomy and European defence'. ARI 102/2017, http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari102-2017-arteaga-strategic-autonomy-european-defence.

Baron, Kevin. 'Mattis: Pentagon Shifting Focus to Great Power Competition — "Not Terrorism"'. Defense One 2018, https://www.defenseone.com/policy/2018/01/mattis-declares-pentagon-will-shift-focus-great-power-competition-not-terrorism/145305/.

Bergmann, Max; Lamond, James; Cicarelli, Siena. 'The Case for EU Defense; A New Way Forward for Trans-Atlantic Security Relations'. 2021, https://www.americanprogress.org/issues/security/reports/2021/06/01/500099/case-eu-defense/.

Biscop, Sven. 'From Global Strategy to Strategic Compass: Where Is the EU Heading?', Research Report, Egmont Institute 2019, https://www.jstor.org/stable/resrep21401?seq=4#metadata_info_tab_contents.

Cramer, Clara Sophie & Franke, Ulrike (eds.). *Ambiguous alliance: Neutrality, opt-outs, and European defence*. ECFR Essay Collection, June 2021, https://ecfr.eu/publication/ambiguous-alliance-neutrality-opt-outs-and-european-defence/.

Engberg, Katarina. 'A European Defence Union by 2025? Work in progress'. SIEPS 2021, https://www.sieps.se/globalassets/publikationer/temasidor/european_defence_union_policy_overview.pdf.

eu2020.de. 'Strategic Compass: Developing Strategic Principles', 25 August 2020, https://www.eu2020.de/eu2020-en/news/article/eu-defense-strategic-compass-foreign-policy/2377030.

Fiott, Daniel (ed.). 'The CSDP in 2020, The EU's legacy and ambition in security and defence', 2020, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CSDP%20in%202020_0.pdf.

Friedman, Uri. 'The New Concept Everyone in Washington Is Talking About', *The Atlantic* 2019, https://www.theatlantic.com/politics/archive/2019/08/what-genesis-great-power-competition/595405/.

Giannopoulos, G.; Smith, H.; Theocharidou, M. 'The Landscape of Hybrid Threats: A conceptual model'. Publications Office of the European Union, Luxembourg, 2021, https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/.

Hindrén, Rasmus & Smith, Hanna. 'Understanding and Countering Hybrid Threats Through a Comprehensive and Multinational Approach: The Role of Intelligence' (unpublished 2021).

Hoffman, Frank. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, Virginia: Potomac Institute for Policy Studies, 2007.

Karabell, Zachary. 'Will the Coronavirus Bring the End of Globalization? Don't Count on It'. *Wall Street Journal*, 20 March 2020, https://www.wsj.com/articles/will-the-coronavirus-bring-the-end-of-globalization-dont-count-on-it-11584716305.

Kersanskas, Vytautas. 'Deterrence: Proposing a more strategic approach to countering hybrid threats'. Hybrid CoE Paper 2, 2020, https://www.hybridcoe.fi/publications/hybrid-coe-paper-2-deterrence-proposing-a-more-strategic-approach-to-countering-hybrid-threats/.

Koenig, Nicole. 'A European Defence Union: In the Name of the People?'. Policy paper 214, Jacques Delors Institute, 2017, https://institutdelors.eu/en/publications/a-european-defence-union-in-the-name-of-the-people/.

Mazarr, Michael; Blake, Jonathan S.; Casey, Abigail; McDonald, Tim; Pezard, Stephanie & Spirtas, Michael. 'Understanding the Emerging Era of International Competition, Theoretical and Historical Perspectives'. RAND Corporation Research Report, 2018, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2726/RAND_RR2726.pdf.

McInnis, Kathleen J. & Starling, Clementine. 'The case for a Comprehensive Approach 2.0: How NATO can combat Chinese and Russian political warfare'. In-Depth Research & Reports, Atlantic Council 2021, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/comprehensive-approach-how-nato-can-combat-chinese-and-russian-political-warfare/.

Raitasalo, Jyri. 'Hybrid warfare: where's the beef?'. War On The Rocks, April 2015, https://warontherocks.com/2015/04/hybrid-warfare-wheres-the-beef/.

Real Instituto Elcano & EUISS. 'A Strategic Compass for EU defence: What implications for the European defence industry?'. 2021, https://www.iss.europa.eu/sites/default/files/EUISSFiles/ES-EUISS-Elcano%20-%20Strategic%20Compass%20-%20Report.pdf.

Russell, Martin. 'EU sanctions: A key foreign and security policy instrument'. European Parliamentary Research Service Briefing, 2018, https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/621870/EPRS_BRI(2018)621870_EN.pdf.

Rühle, Michael & Roberts, Clare. 'Enlarging NATO's toolbox to counter hybrid threats'. *NATO Review*, 2021, https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html.

Savolainen, Jukka. 'Hybrid Threats and Vulnerabilities of Modern Critical National Infrastructure'. Hybrid CoE Working Paper 4, 2019, https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-4-hybrid-threats-and-vulnerabilities-of-modern-critical-infrastructure-weapons-of-mass-disturbance-wmdi/.

Schmid, Johann. 'Konfliktfeld Ukraine: Hybride Schattenkriegführung und das "Center of Gravity" der Entscheidung', in *Krieg im 21. Jahrhundert*, ed. Hans-Georg Ehrhart (Baden-Baden: Nomos Verlag, 2017), 141–162.

Sisson, Melanie W. 'A Strategy for Competition'. CNAS Commentary, 2020, https://www.cnas.org/publications/commentary/a-strategy-for-competition.

Taylor, Nicholas. 'From Strategy to Task: Development of hybrid deterrence activities'. Hybrid CoE Limited Release Paper 1, 2021.

Thiele, Ralph. 'Hybrid Warfare: Future & Technologies Inspiration Paper No. 2' (updated). Hybrid Warfare – Future & Technologies Horizon Scan & Assessment, 2019.

Thiele, Ralph & Schmid, Johann. 'Hybrid Warfare – Orchestrating the Technology Revolution', ISPSW Strategy Series: Focus on Defense and International Security, Issue No. 663, January 2020, https://www.ispsw.com/wp-content/uploads/2020/01/663_Thiele_Schmid.pdf.

Torossian, Bianca; Fagliano, Lucas & Görder, Tara. 'Hybrid Conflict, Neither War nor Peace'. The Hague Centre of Security Studies, January 2020, https://hcss.nl/report/hybrid-conflict-neither-war-nor-peace/.

Trauner, Florian & Ripoll Servent, Ariadna. 'Justice and Home Affairs in the European Union', in *Oxford Bibliographies in Social Work* (Oxford University Press, 2019), https://www.researchgate.net/publication/331383924_Justice_and_Home_Affairs_in_the_European_Union.

Van Rompuy, Herman. *Defence in Europe: pragmatically forward*. Speech by President of the European Council Herman Van Rompuy at the annual conference of the European Defence Agency "European Defence Matters". Brussels, 21 March 2013, https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/136394.pdf.

Wigell, Mikael. 'Democratic Deterrence: How to dissuade hybrid interference'. FIIA Working Paper 110, 2019, https://www.fiia.fi/en/publication/democratic-deterrence.

Wigell, Mikael. 'Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy'. *International Affairs*, Volume 95, Issue 2 (2019): 255–275. https://doi.org/10.1093/ia/iiz018.

Wigell, Mikael; Mikkola, Harri & Juntunen, Tapio. *Best Practices in the whole-of-society approach in countering hybrid threats*. European Parliament Directorate-General for External Policies study, 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf.

EU documents

European Commission. *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy*. COM/2020/605 final, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&from=EN.

European Commission. *Joint communication to the European Parliament and the Council. Joint Framework on countering hybrid threats, a European Union response*. JOIN/2016/018 final, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016JC0018&from=EN.

European Commission. *Joint communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*. JOIN/2017/0450 final, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017JC0450&from=en.

European Commission. *Joint communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade*. JOIN(2020)18 final, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0018&from=EN.

European External Action Service. *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign And Security Policy*. 2016, https://eeas.europa.eu/topics/eu-global-strategy/17304/global-strategy-european-unions-foreign-and-security-policy_en.


Hybrid CoE