REPRÉSENTATION PERMANENTE
DE LA FRANCE AUPRÈS DU
COMITÉ POLITIQUE
ET DE SÉCURITÉ
DE L'UNION EUROPÉENNE
Liberté
Égalité
Fraternité

European Union Institute for Security Studies

Contested global commons: a multidimensional issue for the Strategic Compass

EVENT REPORT

The **EU Institute for Security Studies** and the **French Permanent Representation to the EU** co-organised a high-level conference on the contested global commons and the EU Strategic Compass on 12 March 2021. The conference benefitted from an experienced speaker line-up including high-ranking civilian and military officials from Estonia, Finland, France and Portugal, the European Commission, the European External Action Service and the European Parliament, plus think tank analysts and academics.

The conference focused on concrete ways in which **the Union can strengthen its ability to uphold its freedom of access in the maritime, air, outer space and cyber domains**. These strategic spaces (maritime, air, outer space and cyber) are **vital for the global economy and international security**. The flow of data as well as the transit of goods and people requires these **global commons** to remain **free, safe and open**. The EU has a major interest in enhancing the Europeans' ability to **access and use the global *commons* in a responsible way**, while also upholding the multilateral rules-based order.

However, these global commons are becoming new fields of power competition and their access is being challenged by a growing disregard for norms, irresponsible and destabilising use and practices and unsupported territorial claims. The conference led to a comprehensive reflection on the nature of these **challenges** and a discussion on the risks associated with them. To a large extent, these challenges and risks are fuelled by **the development of new tools, capabilities and strategies by the EU's main competitors**. As a result, **these strategic commons are less regulated, less permissive and increasingly militarised,** prompting escalatory dynamics which could potentially lead to perilous arms races, new confrontations and/or miscalculation.

The conference resulted in **concrete policy recommendations** that are relevant to each of the Compass' four baskets on crisis management, resilience, capabilities and partnerships. The discussions emphasised that **the EU and its Member States can mobilise a wide range of assets** through its experience of maritime operations, its air power, its space ecosystem, its digital and technological capabilities and its normative power. By connecting these dots, the EU has the ability to better support a rules-based international order, effectively **protecting its own territory and citizens** and **projecting security towards its partners**, while shaping international rules or standards that fit its values. The event conclusions can **directly inform the Strategic Compass process** before it is adopted in March 2022.

THE MARITIME DOMAIN

"a need for urgent and rapid EU action on maritime security"

Globalisation has only increased the EU's longstanding and cross-cutting reliance on the maritime domain, and the Union has a major stake in **protecting the global maritime rules-based order**, which is vital for its economic, food, energy, resource and digital security.

Given the absence or limitations of direct State control on the maritime domain, criminal activities are still disrupting security in many areas of the world. New threats like terrorism at sea have also emerged, while great power competition, through highly destabilising hybrid tactics as well as traditional confrontation between navies, has increased in recent years in the context of a new global maritime military build-up in many regions of the world.

Overall, the norms and rules that have underpinned the peaceful and free use of oceans and seas and allowed global trade **are now being tested and sometimes successfully dismantled**. Strategic sea lanes of communication and critical infrastructure are put at risk by new adversarial dynamics and even directly targeted.

The rise of **China** has accelerated this trend and brought many of these issues to the fore. In the vicinity of the South China Sea, Beijing's strategy illustrates new confrontational strategies at sea, with attempts at creating a de facto **exclusive maritime zone** through the use of non-military hybrid tactics.

In this environment, the most pressing challenges facing the EU are to **bolster its capacity to uphold freedom of navigation and to avoid the risks of being denied from accessing choke points and constrained by hybrid maritime threats** that combine **legal warfare, *faits accomplis*, cyber and other 'grey zones' activities**. The EU simultaneously needs to confront re-emerging challenges such as piracy and arms and illicit material trafficking, especially in the Gulf regions of West Africa and the Middle East.

The Strategic Compass is an opportunity to **set a strategic and integrated approach for the EU's maritime security,** to match the changing character of maritime threats and challenges, while ensuring that the EU can act as a global maritime security provider. The EU already engages in maritime security and can build on the experience of two CSDP naval operations, *Irini* and *Atalanta.*

The EU needs to focus its efforts by identifying maritime areas of interest and strategic sea lines of communication, in the framework of an implementation of the EU maritime security strategy (EUMSS). Moreover, the EU should also step up its political and operational responses to **maritime hybrid threats and risks to maritime infrastructure and freedom of navigation**. To this end, reflections on future maritime security operations should take into account European *ad hoc* mechanisms outside of the CSDP framework. Finally, there is a need for the EU to ensure strategic coherence between its maritime security efforts and its international ocean governance policies. This requires much closer cooperation between relevant EU institutions and bodies.

An important task ahead will be to ensure coherence among all of the existing and future maritime-related strategies of the Union on connectivity, the Indo-Pacific, ocean governance and maritime security.

Finally, the EU Member States' ability to **coordinate their naval forces** will be a key test. Be it for humanitarian and disaster relief, freedom of navigation or evacuation operations, securing synergies among European navies is likely to be a decisive force multiplier and thus a major political enabler. Coordination among national naval assets of the EU Member States must rest on an adequate all-purposes maritime information sharing mechanism between all the relevant European actors. Building on the pilot case in the Gulf of Guinea, the CMP concept can serve as a useful experience to feed into the Strategic Compass process, as a way of enhancing the EU's **maritime surveillance in critical zones**, especially in order to deal with maritime criminality, hybrid threats and the protection of logistics hubs and supply routes.

THE AIR DOMAIN

Europe is one of the most congested air traffic zones in the world. Many international **flight paths traverse conflict zones** and crisis hotspots in Eurasia and the Middle East. Flight routes are being used as political leverage by certain countries failing to respect freedom of flight passages. Furthermore, **increasingly aggressive aerial postures** that rely on both defensive and offensive capabilities and the technological arms race in this domain constitute a major threat for EU security and prosperity. In Ukraine, hundreds of civilian lives were lost to the irresponsible use of such technologies and capabilities. The rise of anti-access/area denial (A2/AD) 'bubbles' used by Russia, China and regional powers also threatens **the EU's access and aims to dissuade military action**.

"continued freedom of access to air spaces is a core element of the EU's resilience"

Airpower is **critical for European security and the protection of Europe**. It confers the ability to project force in a flexible, mobile and rapid way, which supports decisive political action. Continued freedom of access of air forces to European and foreign spaces is a core element of the Union's ability to intervene when required. For the Union to maintain its strategic access to airspaces, it needs to **enhance information sharing, training and exercises** between the EU Member States. Mastering cutting-edge technologies is also necessary to guarantee a safe European air space and secured access to the international air space.

Hedging against A2/AD bubbles requires a need to **secure both permanent and temporary air access points**, especially in the Mediterranean, the Middle East as well as the Indo-Pacific. Joint deployments, as well as air policing operations by the EU, should be conducted in coordination with NATO. Second, the EU should strive to **conduct coordinated strategic campaigns in the air domain** to ensure Europe's persistent engagement. A first step could be, for willing military authorities, to share periodical information on their national air deployments in areas of strategic interest for the EU. Furthermore, **the EU could also make better use of air capabilities in its CSDP missions and operations**: air surveillance missions, support to other operations with transportation, increased cooperation with the European Air Transport Command.

Multinational training involving fighter aircraft, strategic transportation and other enablers can strengthen interoperability among European and NATO allies, as well as with other partners. In addition to these combined joint exercises and training, strategic partnerships between EU and non-EU states could help **facilitate logistics lines between overseas bases**.

"a need to ensure the interoperability of civil and military air users"

Furthermore, there is a need for the EU to **continue to invest in aerospace technologies**. European air forces should **develop new doctrines and tactics in order to penetrate and operate in A2/AD areas**, even for short periods. Overall, this means that the Union's efforts should facilitate investments in capacities to delete enemy air defence.

Despite efforts under the Single European Sky initiative, more can be done to **enhance interoperability and coordination between military and all European civil air operators.** The modernisation and **digitalisation of flight navigation systems** is a key challenge and opportunity for the EU. The task is to ensure safety against cyber risks and to overcome the fragmentation of information sharing between national civil and military authorities, as well as between EU countries. EU co-funding could be used in this respect.

THE OUTER SPACE DOMAIN

Space should be conceived as a strategic enabler, and the Union has already achieved a great deal of autonomy in this domain. Space is vital for the Union's prosperity, societal security and defence. Moreover, space is essential for Europeans' military activities in different theatres of operation. However, it is a rapidly evolving domain with greater militarisation and growing use by commercial actors. This evolution is partly due to the strategies and behaviour of major powers, which are increasingly resorting to ambiguous and destabilising actions such as anti-satellite launches, proximity manoeuvres and various pre-eminence strategies. These strategies increase the risk of misunderstanding and escalation.

"space is critical for the Union's economic functioning, societal security and defence"

Another core challenge is the **congestion in orbit and the dangers linked with space debris**, which leads to the higher possibility of collisions. Other factors are also a challenge for the EU, including space weather events, cybersecurity of space systems, threats from jamming and spoofing technologies, and extraterritorial norms and regulations, which may challenge the Union's industrial competitiveness in the space sector. Therefore, continued EU engagement in the genuine development of pragmatic and non-binding voluntary norms of responsible behaviour and regulations is required. So too is enhancing the Union's technological sovereignty in the space sector.

The EU is already focused on space on multiple fronts. From a diplomatic perspective, the EU 'Space Task Force' continues to engage partners and other stakeholders. It works to promote **multilateral solutions to space use and security**. The EU can also benefit from the **geospatial intelligence** services provided by the EU Satellite Centre. Projects developed under Permanent Structured Cooperation (PESCO) seek to enhance the EU's space situational awareness. Under the EU Space Programme, investments will focus on **modernising Galileo and Copernicus** as well as developing new flagships projects such as satellite constellations. In addition, the future use of Galileo's **Public Regulated Service** and EU **Government Satellite Communications** should positively contribute to EU security and defence through the integration of defence requirements.

"there is a need for a common perception of space and defence at the EU level"

The Strategic Compass is an opportunity to take stock of the risks and challenges in space **and outline an EU space defence strategy** that provides guidance and raises political awareness. **Electronic warfare and cyber threats** challenge the functioning of EU space capacities, as evidenced by the increasing use of anti-satellite weapons (i.e. space-to-space and ground-to-space). The Compass should underline the need to **invest in space technologies** that help protect the EU's space assets and terrestrial infrastructure and develop its capabilities in situational awareness.

The EU's ability to **track and anticipate space risks** – through robust space imaging, surveillance, tracing, communication, positioning and navigation capabilities – is also a core need. Still, it is necessary for the EU to address **critical supply security** in the space industry. In coordination with the European Commission, this could be done by blending funds from the European Defence Fund (EDF), Horizon Europe, the EU Space Programme, Invest EU Fund and the European Investment Bank. The Strategic Compass should also foster strategic unity between the Member States on **space and defence** matters. It could contribute to a **common perception** between national capitals on the strategic relevance of space and the risks and challenges in this domain.

THE CYBER DOMAIN

The EU has an interest in **ensuring a free, open, secure and stable cyberspace**. This is a contested domain in which malicious activities constitute a threat to EU institutions and the Member States' critical infrastructures and networks, but also to European citizens and private companies. The numerous risks are not simply emanating from terrorist organisations and criminal networks. The internet is increasingly used for national security purposes by certain states, a phenomenon coupled with the proliferation of offensive cyber tools. Cyber-attacks are complex to apprehend, anticipate and react to since they are often situated in a 'grey zone' **below the threshold of an armed attack**. They can produce potentially significant harm or damage, and they are difficult to attribute. Finally, **the Covid-19 pandemic has revealed further cyber vulnerabilities** and a sharp rise in cyber criminality, increasing pressure on individuals, companies and infrastructures as essential as those of the health sector.

The growing trend towards fragmentation and **State control of cyberspace hits at the core of democracy, liberty, the multilateral rules-based order and the historic multi-stakeholder governance of the internet**. This order is marked by challenges related to juridical control, extraterritorial governance models and strategic dependence on cyber technologies. Cyberspace is also characterised by a concentration of private actors that manage cyber platforms and large amounts of personal data. This **concentration into the hands of a few major companies** raises questions for the EU. Firstly, private firms in cyberspace are increasingly becoming political actors and, secondly, the exploitation of their vulnerabilities can produce systemic effects and damage. The EU has a role to play to preserve multi-stakeholder governance of the internet and a decentralised cyberspace.

"Covid-19 has revealed further cyber vulnerabilities and an evolution in cybercrime"

Fully aware of this changing reality, the Member States of the EU are coming together, for the first time, to work on a common assessment and understanding of the factors shaping our geopolitical context. The Strategic Compass and the first-ever threat analysis done at the EU level has provided, regarding cyber, a clearer view over the wide range of pressing challenges and risks the Union is confronted with.

The EU has already come some way in developing tools that reinforce cyber cooperation between the Member States. Increasingly, the EU has understood that **a 'whole of government' approach** is required to ensure cyber resilience and that we should invest more in innovation, research and education. Furthermore, the 2020 EU Cybersecurity Strategy places emphasis on the need to invest in **prevention, discouragement and response** to cyber threats, calling for enhanced exchanges of information and convergence of analysis between the Member States. Finally, legislation such as the EU Directive on security of network and information systems (NIS) and cyber defence capabilities being developed under the EDF and PESCO are evidence of the EU's steps forward in cybersecurity.

Additionally, the **EU promotes cyber norms** in relevant international bodies, such as the United Nations, International Telecommunication Union (ITU) or Organisation of Security and Cooperation in Europe (OSCE), and is committed to working with partners.

Despite these efforts, the EU can do more to ensure its cybersecurity and **assert European digital sovereignty**. The overall aim should be to **build up cyber deterrence** to discourage its rivals from acting maliciously against its interests. In this regard, the EU's **cyberdiplomacy toolbox** provides a framework to better face and respond to threats. It should be strengthened, both in its coercive dimension (e.g. sanctions) and its collaborative one (e.g. strategic dialogues, capacity building). The EU is a crucial platform to ensure interoperability and coordination between the Member States when developing political responses, technologies and innovation. The EU should also ensure the **security of its institutions**, which requires investing more broadly in secure communications systems within the EU. Defence networks and communications links need to be reinforced at the EU and the Member State levels as they are a direct target for adversaries. The ongoing revision of the NIS directive and the adoption of common binding rules, and the establishment of clear governance for all EU institutions, bodies and agencies will be paramount.

Ensuring **cyber resilience and solidarity in the context of Article 42(7) TEU** and Article 222 TFEU are also important, especially regarding the potential mutual assistance responses that could benefit from a European management framework. The EU and its Member States have a collective role to play in multilateral *fora*, such as the UN or OSCE. They should also partner with States and international and regional organisations that are willing and able to actively contribute to the Union's external efforts. Besides, the Union must continue to explore ways of reinforcing EU-NATO cooperation in cybersecurity, by highlighting the Cooperative Cyber Defence Centre of Excellence in Tallinn or through joint exercises. The Strategic Compass could lead to enhanced **cyber exercises and cyber hygiene** for civilian and military CSDP actors. Finally, there is potentially scope to build upon the civilian CSDP 'mini concepts' in the area of cybersecurity capacity building.