Istituto Affari Internazionali

The Future of EU Defence: A European Space, Data and Cyber Agency?

by Jean-Pierre Darnis

Sovereignty has always been a tricky issue for EU Defence policy. When it comes to the use of military forces, it is difficult to bypass the views of member states. This is not only a legal issue related to the prerogatives of individual member states versus those of the communitarian Union, but rather an issue of democratic control: the use of force is deeply rooted in the political constituencies of EU member states.

Two kinds of risks emerge when seeking to find a common denominator in terms of military affairs in Europe. The first, is to go along with countries pushing for a full spectrum use of force, such as France, which might be too ambitious for most EU member states. The second, is to limit EU defence capabilities and exposure to a minimum, an approach that seems somewhat unsatisfactory in terms of operational capabilities.

Recent progress on European defence includes both a step-by-step approach, led by High Representative Federica Mogherini from the drafting of the EU Global Strategy to the European Defence Action Plan (EDAP), and more direct political action by individual member states, such as President's Macron recent speech in favour of an autonomous EU defence force.

The establishment of a Military Planning and Conduct Capacity (MPCC) within the EU military staff is evidence for this push: the creation of a small cell working as an EU defence command is a remarkable novelty but still far from the autonomous EU defence force envisioned by Macron.

The involvement of the European Commission in research and development (R&D) for the defence sector represents another historic step, breaking a barrier that had thus far forced the Commission to strictly focus on the civilian side. The launching of the Defence Action Plan is the first sign of an emerging supra-national logic in the defence field, with the Commission

Jean-Pierre Darnis is Head of the Security, Defence and Space Programme at the Istituto Affari Internazionali (IAI).

IAI COMMENTARIES 17 | 21 - OCTOBER 2017 ISSN 22532-6570

emerging as a key enabler through funding approbations.

Different factors are driving this evolution. The perception of growing threats coming from North and South has increased a common strategic awareness among EU states, a key step to shape common responses to crises. It is also important to highlight the evolution of new technologies, which are strategic and apply indifferently to the civilian or military sector. Space technologies, data gathering, data transmission and cyber capabilities represent a growing set of information technology applications which also tend to disrupt classic defence paradigms.

Space, for example, is considered a key defence asset for its navigation, observation and data transmission capabilities. As far as navigation is concerned, the European Union has invested in the Galileo system, which includes a Public Regulated Service (PRS) signal to be used by defence organizations. In data transmission, the GovSatcom programme defines the first step of a European public capability that is also for defence users. Earth observation has always been a tricky field for military cooperation, mainly because EU states are extremely reluctant to share intelligence. Still, Copernicus security applications – which support border surveillance and EU external action with geospatial data – are opening the way for a growing role of the European Union Satellite Centre (SatCen) based in Torrejon, Spain. One may also recall the Space Surveillance Awareness (SSA) programme developed by SatCen, which builds up capabilities to detect space objects, from debris to satellites.

The space sector provides important lessons: when member states cannot independently fulfil their needs, both in terms of technological capabilities and investments, they are more open to revisit concepts of sovereignty and allow the EU to develop and supply a common set of technologies and services. The increasing needs of data transmission capabilities, including remotely piloted aircraft systems (RPAS), are driving the development of EU capabilities such as satellite-based services like GovSatcom. Data transmission needs also teach a very interesting lesson in terms of ownership and control of data: there is no real technical problem with sharing capacities while keeping control over data flows, as the issue can be resolved via encryption.

Furthermore, the political acceptance of an EU data transmission capability provided to EU states for defence purposes seems very high as the EU could make virtual "pipelines" available without a specific deployment and without facing a veto from member states. Space data gathering – i.e. spy satellites – has, until now, been difficult to share partly due to the low number of EU systems, implying the need to control the targeting of intelligence. This problem could disappear if a growing number of sensors provided worldwide monitoring and continuous data flows which would then be dispatched among EU states' defence systems. One might advocate an ambitious development of a Copernicus defence and security system, for example. Existing member state capabilities are quite limited, and there is room for some kind of EU observation system able to provide more data that would be beneficial to all.

Cyber defence represents another opportunity to develop an operational European capacity. The EU has wisely chosen to define a cyber-security strategy, including cyber defence. The recent EDAP addresses skills gaps in the cyber defence domain and fosters training. These initiatives might be too limited however, in light of the pace of technological progress and the current political momentum conducive to joint action.

The European Commission is already addressing the issue of cyber security through its space policy, as shown by the contract given to Leonardo for the definition of Galileo's cyber security technology. The fusion between data gathering, transmission and processing, including the use of artificial intelligence, has already occurred and raises numerous issues. For example, the question of cyber weapons proliferation sees important information technology (IT) companies such as Microsoft looking for a dialogue with EU authorities. The EDAP capability window might be an opportunity to add further technologies to EU defence capabilities.

Converging policy trends in defence might also be an opportunity to further define an operational step by developing both autonomous and integrated capabilities with member states in order to boost the level of response and resilience. Some key states such as France, Germany or Italy are already developing cyber defence organizations. There is, however, a risk of a nationalization of defence systems in Europe which, given its technological nature would instead require a common and global effort to face threats and competition on a worldwide basis. The French Minister of Defence, Florence Parly, has recently excluded cyber defence from the topics for potential EU cooperation, in itself a worrying sign.

Industry also needs to be taken into consideration. The main IT companies are based in the US where the so-called GAFAM companies – short for Google, Apple, Facebook, Amazon, Microsoft – concentrates an impressive level of data processing and gathering capabilities. Europe does not have such global IT companies which is both a problem and an opportunity. It creates the need to permanently catch up with technological developments with no real integrator, and raises a number of questions in terms of control of information and sovereignty.

Yet, this is also an opportunity because no member states can claim an autonomous capacity, leaving space for EU initiatives which are, in a way, expected by the very same IT companies aiming to provide their services at the EU level. A new defence data and IT paradigm also fits with the need for EU level integration versus wasting time and energy on artificially raising national fences around a pervasive and holistic technology.

Space, data and cyber technological and political trends define areas of opportunity for the EU. On the technical side, a strong case can be made for an EU level approach based on the common nature of technologies applied to both civilian and defence domains, their very pervasive character at the global level which calls for a transnational approach and the need for a critical mass of investments, difficult if not impossible to fulfil at the level of member states.

On the political side, one can sum up what is at stake by focusing on the strategic issue of information technology chain control. This is already taken into consideration by the EU but could also support the development of a "space, data and cyber defence agency". This would be consistent with the project of an autonomous European defence force and give the EU, not only a tool to strategically and operationally face those issues, but also a way to transform and project its defence effort beyond the needs of tomorrow.

18 October 2017

Istituto Affari Internazionali (IAI)
Founded by Altiero Spinelli in 1965, IAI does research in the fields of foreign policy, political economy and international security. A non-profit organisation, the IAI aims to further and disseminate knowledge through research studies, conferences and publications. To that end, it cooperates with other research institutes, universities and foundations in Italy and abroad and is a member of various international networks. More specifically, the main research sectors are: European institutions and policies; Italian foreign policy; trends in the global economy and internationalisation processes in Italy; the Mediterranean and the Middle East; defence economy and policy; and transatlantic relations. The IAI publishes an English-language quarterly (The International Spectator), an online webzine (Affarinternazionali), two series of research papers (Quaderni IAI and IAI Research Papers) and other papers' series related to IAI research projects (Documenti IAI, IAI Working Papers, etc.).

Via Angelo Brunetti, 9 - I-00186 Rome, Italy
T +39 06 3224360
F + 39 06 3224363
iai@iai.it
www.iai.it

Latest COMMENTARIES IAI

17 | 21 Jean-Pierre Darnis, *The Future of EU Defence: A European Space, Data and Cyber Agency?*

17 | 20 Aldo Liga, *The "Israel Factor" and the Iraqi-Kurdish Quest for Independence*

17 | 19 Davide Cancarini, *Like a Bull in a China Shop: Uzbekistan Traces a New Foreign Policy Direction*

17 | 18 Guillaume Lasconjarias and Lukáš Dyčka, *Dealing with the Russian Bear: Improving NATO's Response to Moscow's Military Exercise Zapad 2017*

17 | 17 Francesco Michele and Dario Rossi D'Ambrosio, *The Challenge of Long-Term Development in the Occupied West Bank: Voices from the Field*

17 | 16 Riccardo Perissich, *Juncker's Last Hurrah*

17 | 15 Carlo Trezza, *The UN Nuclear Ban Treaty and the NPT: Challenges for Nuclear Disarmament*

17 | 14 Adriano Iaria, *International Humanitarian Law and the UN Nuclear Ban Treaty*

17 | 13 Sinan Ekim, *Eyeing Elections, Erdoğan Doubles Down on Critics: Will the Strategy Backfire?*

17 | 12 Giuseppe Spatafora, *EU-Malaysia Trade Talks: No End in Sight*

ISSN 2532-6570