

## Tech Summit – Edizione 2023: How technology is shaping the global power

### Report finale del progetto realizzato dall'Ufficio di Roma dello European Council on Foreign Relations

Il progetto è stato realizzato attraverso le seguenti attività:

- 1) Una conferenza a Torino, dal titolo **WAR, TECHNOLOGY AND POWER: The challenges to international security**, svoltasi il 19 e 20 aprile 2023, con 65 partecipanti a livello complessivo da Italia e Europa (lista dei partecipanti e agenda a seguire):
  - Una dinner discussion: **Technological Sovereignty and beyond: the EU and Great Powers competition** (19 aprile 2023)
  - Tre sessioni di lavoro *policy-oriented* (20 aprile 2023):
    - a. *Is this what “hybrid” really means? A reflection on the war in Ukraine between cyber space and conventional domains*
    - b. *The defence industry in the technological competition: Trends and challenges*
    - c. *“Invisible borders”: the cyber space fragmentation as a threat to democratic rights*
- 2) **Nota** finale dell'incontro (a seguire)

L'evento è stato organizzato dall'Ufficio di Roma di ECFR con il sostegno di Fondazione Compagnia di San Paolo e del Ministero degli Affari esteri e della Cooperazione internazionale, ed in collaborazione con il Comando per la Formazione e Scuola di Applicazione dell'Esercito - Centro Studi Post Conflict Operations.

Tra i partecipanti, 11 pan-European fellows ECFR-Fondazione Compagnia di San Paolo; i Consiglieri ECFR Giorgia Abeltino, Enzo Amendola, Valentino Valentini, Alejandro Romero, Alessandro Speciale, Fabrizio Tassinari; 11 esperti pan-europei di ECFR; Massimo Carnelos, Capo dell'Ufficio Innovazione, Ministero degli Affari esteri e della Cooperazione internazionale; Marco Saracco, Segretario di Legazione, Ministero degli Affari esteri e della Cooperazione internazionale e pan-European Fellow, ECFR-Fondazione Compagnia di San Paolo; Lorenzo Vai, Unità di analisi e Programmazione, Ministero degli Affari esteri e della Cooperazione internazionale, e pan-European Fellow, ECFR-Fondazione Compagnia di San Paolo; Claudio Catalano, Amministratore Delegato di Iveco Defence Vehicles; Alessandro Marrone, Responsabile del programma Difesa dello IAI; Alena Kudzko, Vice presidente del Globsec Policy Institute; Ruben-Erik Diaz-Plaja, Senior Policy Advisor dell'Ufficio del Segretario Generale della NATO; Dario Pagani, Head of Digital and Information Technology di ENI; Virginia Padovese, Managing editor di Newsguard.

## TECH AND FOREIGN POLICY SUMMIT- 2<sup>nd</sup> edition

### War, Technology and Power: The challenges to international security

---

Turin, 19-20 April 2023

After the successful first edition of the Tech Summit in 2022, the 2023 edition will continue the conversation on the challenges of technological competition for sovereignty in the current global order. The first edition, “Great Powers and Technological Competition: what role for the EU?”, focused mainly on the role of technology in the global competition and on the EU’s efforts in keeping pace. As a result of the two-days exchange, the conference set the basis for a productive reflection on the nature of the geopolitical competition in the technological field, ranging from the confrontation with the US, to the definition of tech sovereignty for the EU and for Italy to become a smart and cyber secure country.

The 2023 edition will focus on what the EU has done so far to fill the gap between the current scenario and the relevant geopolitical actor in the tech domain it is aiming to become. The impressive effort in making the Chips Act come true, and facing the semiconductor shortage, is certainly a positive sign in enhancing European technological sovereignty. But the supply chain fragility and the dependance from other foreign great powers is not the only threat in the digital world. The experience of the war in Ukraine has shown that interstate conflicts are still possible, even in the peaceful Europe: the technological power of states is therefore still something to be carefully taken into account when talking about international security, since technological development influences both the way wars are fought, and the domains involved in the clashes. Brussels has traditionally perceived technological development as a terrain to enhance the Single Market and an opportunity to increase services and people’s way of living. With the Von der Leyen Commission’s “Digital decade” as one of the six priorities, this aspect has become pivotal for the EU effort in the civilian domain. But what about the security and military dimension?

For this reason, the 2023 Tech Summit aims to stimulate the debate on the concept of “hybrid warfare” drawing some lessons from the experience in Ukraine. Technologically advanced weapons, like drones, and new tactics are in fact deployed alongside traditional ones, since the conventional domains are subjects to the attacks as well as the new domains. Attention will be therefore drawn on cyber security and the current debate on the topic: from its role in the new NATO Strategic Concept, to the possible EU effort in providing assistance to Eastern and Southern Partner countries. Secondly, the Summit will try to adopt the perspective of the defence industries in the technological competition and catch a glimpse of the current trends in this field. Eventually, cyber space will be again the protagonist, this time as the place where authoritarian regimes are now enhancing their repressive methods against people’s human rights.

The conversation will explore challenges and opportunities both for EU and Italian institutions to identify vulnerabilities and build on existing virtuous programs so that the geopolitical dimension will not be lost. In conclusion, the 2023 edition of the Tech Summit will build on the success of the previous one to expand the reflection the impact of technology in international relations and its security dimension.

## DAY 1 – April 19<sup>th</sup>, 2023

*Venue: Hotel NH Collection Torino Piazza Carlina, P.za Carlo Emanuele II, 15, 10123 Turin*

### 19:30 – 21:30 Dinner discussion: Technological Sovereignty and beyond: the EU and Great Powers competition

**Welcome remarks:** **Alberto Anfossi**, Secretary General, Fondazione Compagnia di San Paolo; **Alba Lamberti**, Deputy Director, ECFR

#### Speakers:

- **Giorgia Abeltino**, Director, Public Policy South Europe and Director External Relations Google Arts & Culture, Google; ECFR Council Member
- **Enzo Amendola**, Member of Parliament, Chamber of Deputies; former Minister for European Affairs, Italy; ECFR Council Member
- **Camille Grand**, Distinguished Policy Fellow, ECFR
- **Valentino Valentini**, Deputy Minister of Enterprises and Made in Italy; ECFR Council Member

**Chair:** **José Ignacio Torreblanca**, Head, Madrid Office and Senior Policy Fellow, ECFR

This dinner discussion will introduce the conference providing an overview on the EU efforts in improving the technological sovereignty and its role as a geopolitical actor in the digital and cyber space, more than one year after the Russian invasion of Ukraine started. The technological competition is higher than ever, and the EU is determined to keep the pace with the other main actors in this race, the US and China. As a matter of fact, the efforts to improve member states resilience in the digital field is certainly paramount in protecting the livelihood of European citizens. But as a geopolitical actor the EU recognizes the importance of ensuring a certain degree of resilience also in the neighbouring countries, since cyber space is way more volatile than the physical one, and the weaknesses of a partner can be exploited to harm the Union. For this reason, it is both an internal and an external effort to be carried out in the digital dimension. In particular, the speakers will try to offer a comprehensive view on the state of play in the Digital Decade, with a particular focus on what EU has done to improve the technological sovereignty, and to ensure its role as a geopolitical actor also in the field of cyber thought the projects developed by the External Action Service.

---

## DAY 2 – April 20<sup>th</sup>, 2023

*Venue: Circolo degli Ufficiali, Corso Vinzaglio, 6, 10121 Turin*

#### 9:00 Welcome remarks

- **Paolo Mazzuferi**, Col., Head of Study and Doctrine Department, Italian Army Post Conflict Operations Study Centre
- **Nicolò Russo Perez**, Head, International Affairs, Fondazione Compagnia di San Paolo; ECFR Council Member
- **Lorenzo Vai**, Policy Planning Unit, Italian Ministry for Foreign Affairs and International Cooperation
- **Arturo Varvelli**, Head, Rome Office and Senior Policy Fellow, ECFR

**09:30 – 10:45 PANEL 1: Is this what “hybrid” really means? A reflection on the war in Ukraine between cyber space and conventional domains**

**Speakers:**

- **Pietro Alighieri**, RDML, Senior Advisor, Secretariat General of Defence, National Armaments Directorate
- **Massimo Carnelos**, Head of Innovation, Italian Ministry for Foreign Affairs and International cooperation
- **Andrea Gilli**, Senior Researcher, NATO Defence College
- **Alena Kudzko**, Vice President for Policy and Programming, GLOBSEC Policy Institute; Schmidt Fellow
- **Josef Schroefl**, Deputy Director on Strategy and Defense, Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats

**Chair: Arturo Varvelli**, Head, Rome Office and Senior Policy Fellow, ECFR

The eruption of the conflict in Ukraine brought on the one hand to the return of conventional conflicts in Europe and on the other hand to the concretization of what theoretical and doctrinal experts have called “hybrid warfare” for years. As a consequence, since the beginning the debate around the war has been polarized in two main factions: the ones underlining the return to old fashioned tactics and weapons, and the others, highlighting the use of cyber warfare as the greatest possible game-changer in the conduction of the war. As some time has passed since February 2022, analysts can now prudently observe that the cyber dimension of this conflict was less predominant than expected, albeit essential in the Kremlin strategy. In this context, it is important to understand whether the offensive Russian capabilities have been overestimated or whether they were neutralized by the Ukrainian cyber defensive forces better than anticipated. In this case, it would be paramount to investigate the role of EU member states and NATO Allies in providing assistance: in front of a possible spillover of a cyber conflict, all states must be prepared to defend themselves, to defend the civilians, because the resilience of the overall system depends on the endurance of each member of the Alliance. At the same time, it would be unwise to forget the conventional aspects of the conflict and how technology has made relevant improvements in this, as well. The use of drones, for instance, which are not a new element per se, can still represent a way in for new applications of tactics implying further development of AI to be tested in an interstate conflict. To be prepared for the “future conflicts”, understanding the role of technologies and the possible use of it, will be paramount: this panel will therefore focus of the lessons to be learned so far and on possible improvements to be made, as European, as Italian, as part of NATO.

**10:45-11:15 Coffee break**

---

**11:15 – 12:30 PANEL 2: The defence industry in the technological competition: Trends and challenges**

**Speakers:**

- **Claudio Catalano**, CEO, Iveco Defence Vehicles
- **Ruben-Erik Diaz-Plaja**, Senior Policy Adviser, Policy Planning Unit, Office of the Secretary General, NATO
- **Alessandro Marrone**, Head of Defence Program, Istituto Affari Internazionali (IAI)

**Chair: Rafael Loss**, Coordinator for Pan-European Data Projects, ECFR

This panel will explore the current trends in technological development from the defence industry point of view, exploring the main field of investments by EU member States and by the global superpowers. Moreover,

there will be room for discussing how the various countries, from the smallest to the biggest, are now allocating the budget for R&D in the field of defence. The shocking event of the war in Ukraine has certainly played a role in shaping the most recent tendencies in the development of new weapons, that are compliant to the current strategic scenario. Alongside a return to conventional arms and weapons systems, it would be interesting to stimulate the debate on how the new technologies are being integrated with the traditional ones, as well as on the States investments in the different fields.

### 12:30 – 13:30 PANEL 3: “Invisible borders”: the cyber space fragmentation as a threat to democratic rights

#### Speakers:

- **Michelangelo Conoscenti**, Professor, University of Turin
- **Virginia Padovese**, Managing Editor & Vice President Partnerships, Europe, Australia and New Zealand, NewsGuard
- **Dario Pagani**, Head of Digital & Information Technology, ENI
- **Alejandro Romero**, Co-founder and COO, Constella Intelligence; ECFR Council Member

**Chair:** Julian Ringhof, Policy Fellow, ECFR

New technologies have brought new forms of democratic expression as well as new kinds of threats. Authoritarian regimes, in fact, can take advantage of surveillance technologies to control and to impose digital borders to their citizens. The days of the Arabs springs, when social networks were used as tools to spread ideas by the protesters, are now dead and gone, since many undemocratic governments have developed strategies to stop uprisings to be fueled by the virality of posts and videos online. If on the one hand the European countries have clearly stated their effort in defending democratic expression and human rights also in cyber space, many other States in the world have a slightly different vision on the topic, as it can be seen in the last Freedom House report “Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet”. This panel will therefore explore cyber space and the impact of a progressive fragmentation of the global network on the balance of power between authoritarian regimes and democratic states, in a context where people are more and more divided in cyber bubbles. Particularly, it would be interesting to analyse the EU efforts in this sense under the Global Gateway and the possible countermeasures to be taken at the international level, improving the regulation mechanisms or advocating alongside with civil society organization.

### 13:30 End of conference

---

13:40 – 14:30 Light lunch and departure of participants

# TECH AND FOREIGN POLICY SUMMIT

## 2<sup>nd</sup> edition

### WAR, TECHNOLOGY AND POWER

#### The challenges to international security

Turin, 19-20 April 2023

#### List of Participants

1. **Giorgia Abeltino**, Director, Public Policy South Europe and Director External Relations Google Arts & Culture, Google; ECFR Council Member
2. **Pietro Alighieri**, RDML, Senior Advisor, Secretariat General of Defence, National Armaments Directorates
3. **Vincenzo Amendola**, Member of Parliament, Chamber of Deputies; former Minister for European Affairs, Italy; ECFR Council Member
4. **Alberto Anfossi**, Secretary General, Fondazione Compagnia di San Paolo
5. **Alessandro Balossino**, Head, Research and Development, Argotech
6. **Luca Barana**, Researcher, Istituto Affari Internazionali (IAI); Pan-European Fellow, ECFR-Fondazione Compagnia di San Paolo
7. **Claudio Bertolotti**, Director and Head of Research, Start Insight
8. **Piero Boccardo**, Director, Ithaca; Full Professor, Politecnico di Torino
9. **Ettore Bompard**, Professor, Energy Department, Politecnico di Torino
10. **Flavio Brugnoli**, Director, Centro Studi sul Federalismo
11. **Federica Caciagli**, Public Affairs Department, Head of Associative Bodies Relations Development and Governance, ENI
12. **Mattia Caniglia**, Associate Director, Capacity Building at the Digital Forensic Research Lab, Atlantic Council; Affiliate Lecturer, University of Glasgow; Pan-European Fellow, ECFR-Fondazione Compagnia di San Paolo
13. **Tommaso Canonici**, Managing Director Europe, Opinno
14. **Massimo Carnelos**, Head of Innovation, Italian Ministry for Foreign Affairs and International Cooperation
15. **Gabriele Carrer**, Journalist, Formiche; Visiting Fellow, ECFR Rome
16. **Claudio Catalano**, CEO, Iveco Defence Vehicles
17. **Antonio Cavallo**, Capt., Staff Officer, Space Office, Italian army
18. **Lorraine Charbonnier**, PhD candidate, King's College; Pan-European Fellow, ECFR-Fondazione Compagnia di San Paolo
19. **Andrea Ciommi**, Institutional Relations & Sustainability, Head of International Business Support, Iveco Group N.V.
20. **Michelangelo Conoscenti**, Professor, University of Turin
21. **Teresa Coratella**, Program Manager, ECFR Rome
22. **Mauro D'Ubaldi**, Lt. Gen., Commander, Italian Army Training Command and School of Applied Military Studies
23. **Marco Di Liddo**, Director, Centro Studi Internazionali (CeSI)
24. **Ruben-Erik Diaz-Plaja**, Senior Advisor, Policy Planning Unit, Office of the Secretary General, NATO
25. **Daniele Frigeri**, Director, Centro Studi di Politica Internazionale (CeSPI)
26. **Maria Gargano**, Junior researcher, Egmont- Royal Institute for International Relations; Pan-European Fellow, ECFR-Fondazione Compagnia di San Paolo

27. **Mattia Giampaolo**, Research fellow, Centro Studi di Politica Internazionale (CeSPI); PhD Candidate, University La Sapienza; Pan-European Fellow, ECFR-Fondazione Compagnia di San Paolo
28. **Andrea Gilli**, Senior Researcher, NATO Defence College
29. **Camille Grand**, Distinguished Policy Fellow, ECFR
30. **Edoardo Greppi**, Professor, University of Turin
31. **Carla Hobbs**, Program Manager, ECFR Madrid
32. **Alena Kudzko**, Vice President for Policy and Programming, GLOBSEC; Schmidt Fellow
33. **Alba Lamberti**, Head, London Office and Deputy Director, ECFR
34. **Rafael Loss**, Coordinator for Pan-European data projects, ECFR
35. **Dario Malerba**, Manager & Mobility Lead, Opinno Torino
36. **Alessandro Marrone**, Head of Defence Program and Editor Documenti IAI, Istituto Affari Internazionali (IAI)
37. **Lorena Stella Martini**, Office Assistant, ECFR Rome
38. **Paolo Mazzuferi**, Col., Head of Study and Doctrine Department, Italian Army Post Conflict Operations Study Centre
39. **Alberto Miglio**, Researcher, University of Turin
40. **Antonio Missiroli**, Professor of European Security, Sciences Po; Former NATO Assistant Secretary-General for Emerging Security Challenges
41. **Karolina Muti**, Senior Fellow, Istituto Affari Internazionali (IAI); Pan-European Fellow, ECFR-Fondazione Compagnia di San Paolo
42. **Thibault Muzergues**, Resident Program Director, International Republican Institute
43. **Jonathan Nelson**, Director, Risk Intelligence, Constella
44. **Virginia Padovese**, Managing Editor & Vice President Partnerships, Europe, Australia and New Zealand, NewsGuard
45. **Dario Pagani**, Head of Digital & Information Technology, ENI
46. **Julian Ringhof**, Policy Fellow, ECFR
47. **Alberto Rizzi**, Associate Researcher and Pan-European Fellow, ECFR-Fondazione Compagnia di San Paolo
48. **Alejandro Romero**, Co-founder and COO, Constella Intelligence; ECFR Council Member
49. **Nicolò Russo Perez**, Head of International Affairs, Fondazione Compagnia di San Paolo; ECFR Council Member
50. **Stefano Ruzza**, Associate Professor of Political Science, University of Turin
51. **Stefano Sacchi**, Professor, Politecnico di Torino
52. **Silvia Samorè**, Pan-European Fellow, ECFR-Fondazione Compagnia di San Paolo
53. **Marco Saracco**, Legation Secretary, Italian Ministry for Foreign Affairs and International Cooperation; Pan-European Fellow, ECFR-Fondazione Compagnia di San Paolo
54. **Joseph Schroefl**, Deputy Director on Strategy and Defense, Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats
55. **Natia Seskuria**, Founder and Executive Director, Regional Institute for Security Studies; Schmidt Fellow
56. **Alessandro Speciale**, Head of Rome Office, Bloomberg; ECFR Council Member
57. **Eleonora Tafuro**, Senior Research Fellow, Istituto per gli Studi di Politica Internazionale (ISPI)
58. **Fabrizio Tassinari**, Executive Director, School of Transnational Governance, European University Institute (EUI); ECFR Council Member
59. **Loredana Teodorescu**, Head of EU and International Affairs, Istituto Luigi Sturzo; President, Women in International Security Italy (WIIS Italy)
60. **José Ignacio Torreblanca**, Head, Madrid Office and Senior Policy Fellow, ECFR
61. **Lorenzo Vai**, Policy Planning Unit, Italian Ministry for Foreign Affairs and International Cooperation; Pan-European Fellow, ECFR-Fondazione Compagnia di San Paolo
62. **Valentino Valentini**, Deputy Minister of Enterprises and Made in Italy; ECFR Council Member






63. **Giuseppe Valentino**, Vice President Product Management Backbone and Infrastructure Solutions, Sparkle
64. **Arturo Varvelli**, Head, Rome Office and Senior Policy Fellow, ECFR
65. **Michele Vellano**, Professor, University of Turin



Ministero degli Affari Esteri  
e della Cooperazione Internazionale

*With thanks to*

*for kindly supporting this initiative; in partnership with*  **ESERCITO**



# TECH AND FOREIGN POLICY SUMMIT

## 2<sup>nd</sup> edition

### WAR, TECHNOLOGY AND POWER

#### The challenges to international security

Turin, 19-20 April 2023

#### Report of the event

#### **The technological competition and the superpower competition among the EU, US, and China as a defining feature of the international system**

The troubled times we are living are challenging policymakers, researchers, and managers from the private sector to distillate clarity from complexity. This is particularly evident in the digital sector, whose influence has reached almost all aspects of economy and society and now more than ever is experiencing rapid changes. More than a year after the war in Ukraine broke out, some clear patterns concerning the impact of technology in modern warfare are emerging, while the dynamics of digital competition in the international system suggest how important it is for science and technology practitioners to cooperate with policy makers.

Far from having emerged from scratch, these dynamics are rooted in previous events. In fact, if the world is currently witnessing the pervasiveness of cyber-attacks and if everyone's life is affected by cyber vulnerabilities, it is also because during the pandemic governments, private companies and civil society had to cooperate to improve their degree of digitalization to overcome isolation. The war in Ukraine, in addition, was a catalyst for many similar, already ongoing phenomena.

Moreover, the geopolitical competition on technology, besides the digital domain, is higher than ever. Dealing with China is a dilemma: appeasement might not be the right strategy but, on the other hand, a close-door policy might strengthen the already existing alliance between China and Russia. Complexity increases when taking into account that for Beijing keeping the whole West focused on managing the conflict in Ukraine and its possible spill overs could be a strategic advantage to advance its internal and external interests in other parts of the world. For this reason, for Brussels the relationship with Washington remains the most important, at least in the European perspective; yet this alliance must acknowledge the fact that the West is shrinking. In the current scenario the West is not only against "the Rest", but against "the South" and "the Rest": Western countries have failed them and must now understand how to regain their trust.

#### **The war in Ukraine as a wake-up call and an endless source of lessons**

The Russian invasion of Ukraine has been difficult to read since its very beginning. After more than a year, it is now possible to identify several wars being fought at the same time: on the one hand, the world was caught by surprise by the massive use of space assets in this conflict. At the same time, it is possible to observe, as expected, a massive use of new technologies beside the deployment of traditional means of warfare in the

same battlefield. From what we seize from this war, the conventional domains are now in a sense supported by the space domain for a great deal. But the digital era has brought both the possibility to use space assets as enablers, and the capacity, the means and the ability to collapse the “fourth domain”. Since conventional and new battlefields are now inextricably interlinked, it is necessary to adopt the perspective of “joint domains”.

Moreover, digitalisation has proved that it is now impossible to separate the civil and the military, in terms of objectives, infrastructures and capabilities. We are becoming increasingly aware of how everything can become a weapon – and this is indeed the deepest meaning of “hybrid warfare”. This leads to several dilemmas to be solved: if a NATO country suffered from a cyber-attack to a health infrastructure, how would the Allies consider that? Shall they invoke article 5 as suggested by the new Strategic Concept?

Looking at the future, the European Union and NATO countries will need a range of capabilities that encompasses both traditional means of warfare and new digital instruments. Since conventional conflicts have proved to still represent a possible threat to our security, it is paramount to maintain superiority in the conventional domains. This would only be possible through a real and fruitful cooperation between NATO and the EU. Yet, all this will not be sufficient anymore.

The war in Ukraine, in fact, is much more than a high intensity conflict, and while it is still ongoing it might be impossible to catch the real impact of the underlying war fought in the cyberspace. What is it possible to observe for now are the impressive results achieved by the Ukrainians, who have managed to digitalise the battlefield to compress the time for decision making and improve precision. To do so, they have exploited in the best way the access to big data also provided by Western countries’ intelligence, developing the right software in order to improve their situational awareness and decision-making capacity. This proved that time still does matter: the hard military power is still needed, but in addition to that, States have to implement capabilities to multiply their impact and to protect them.

Cyber threats are part of the broader concept of hybrid threats, which also encompasses economic sanction, asymmetric warfare and disinformation, together with other phenomena. In the context of Ukraine, Western analysts have probably underestimated Ukraine’s resilience, considering that the element of cyber warfare was huge, but still the Ukrainian cyber domain was not destroyed. At the same time, telecommunication companies decided not to suspend any account running out of credit. This allowed thousands of refugees to still communicate. Ukrainian cyber capabilities were also improved thanks to the essential support from Western countries and neighbouring countries (Israel, Poland, Baltic Countries).

From previous intelligence insight, Russia is known to have developed a very impressive cyber disinformation machine, but for now there is no sign of Russian superiority in the cyber space. Yet Western countries should be wondering whether they are still missing something about Russian capabilities. Some possible hypotheses have been formulated by the analysts: first, there is the possibility that this kind of machine is not actually deployable in the battlefield. Another option is that Russian military forces are currently focusing on the conventional elements, which is why the cyber element is less decisive. On the other hand, it could also be the opposite: Russians might have invested more on cyber, and this is why they are struggling on the ground. This would probably mean that analysts could have completely misunderstood the nature of the attack, that might

be ongoing without the EU being aware of that. In the current uncertainty, what is happening in the cyber domain remains crucial for both military and civilian stakeholders.

Another very interesting trend emerging from this conflict is the role played by non-state actors, that for instance were very active also in conducting cyber-attacks campaigns. This is something essential to be acknowledged for the future. Moreover, digital and new economy have brought into the conflict an unlikely kind of non-state actors, like Elon Musk, the CEO of Starlink, a private company that can operate in space and provide a strategic advantage as well as a deadly threat to all the terrestrial activities relying on space assets. Paradoxically, the private sector has the resources and the capabilities to keep the pace with the development of new disruptive technologies and this is something policy makers should consider when working on the implementation of strategic sovereignty. For instance, quantum computing can now read a cryptographic key in a couple of minutes and if these technologies become accessible, as it has happened with drones within a few years, States will have to face this new threat. For this reason, it is important to maintain supremacy also in the technological competition, as well as in the traditional hard military domain.

The use of drones has proved to be another game changer, especially considering the way Ukrainians are using both military and expensive drones, as well as commercial and cheaper ones, to do things they were not projected to do. All this was possible also in great part thanks to the involvement of the private sector, and namely of tech giants. Yet a great deal of credit should be paid to the Ukrainians, who have proved to own a great digital expertise, showing that human IT experts are an asset they can rely on. Since 2014, Ukraine has implemented a high level of decentralization and encouraged experimentation by local leaders, thus improving the level of local leadership. Moreover, and as a consequence of the above-mentioned fusion of civilian and military sector, after February 24<sup>th</sup>, 2022, the whole society stepped in. This has also helped in the collection of data, and it is providing Ukraine with a concrete chance to win the war. Nevertheless, for the future we still need to learn some lessons: while the war in Ukraine shows that results on the ground can still be reached even with cheaper means, this should not be an alibi for European defence industries not to invest in research and development of competitive technologies.

### **The European defence industry dealing with the return of conventional conflicts**

For the defence sector, what has been happening in the last couple of years can be absolutely defined as a “wake-up call”. The current defence conversation is particularly aware that this is an unprecedented strategic moment, since after the Russian invasion of Ukraine, there would probably be no coming back. NATO and the EU should be prepared to face this moment with the right attitude, even though not all EU Member States necessary grasp the extent of what is happening on the battlefield, despite the massive number of casualties on both fronts – but especially on the Russian one. The first lesson to be learned is that high intensity conflicts are again a possibility. But the real challenge for the EU Member States is represented by the fact that we are facing three kinds of warfare at the same time: massive use of space, massive use of new technologies and traditional means of warfare. The EU is torn between the challenge to produce enough ammunition for the internal need and to support Ukraine, but it is also aware of the degree of the technological competition that includes both the US and China.

As the defence industry is heavily influenced by the geopolitical turn, the major tension that policymakers and private companies are facing is the need to conciliate contrasting objectives: on the one hand, the

conventional aspect of this war has led to the return of a strong focus on the land domain and on platform that had been almost abandoned for years; on the other hand, the above mentioned new disruptive technologies are posing a threat to which the West should react by investing in innovation.

Military technological industries had to be quite responsive and for many of them the return to conventional warfare has entailed the reactivation of whole supply chains. Also, they need to conciliate the imperatives of military platforms with the constraints of EU legislation, particularly the ESG. Thinking about strategic autonomy in this context has a lot to do with policymakers' understanding of the challenge private companies are facing in the provision of the right products, in accordance with the needs of the various national armed forces. Several non-material barriers to weapon systems import and export are in fact partially responsible for the difficulties in creating a real European industrial cooperation in the military field. Other crucial dilemmas in this area regard the current need to increase the industrial capabilities to keep the pace with the Ukrainian requests and the national defence imperatives.

But quantity, that would allow to rely on a critical mass to increase the sustainability of costs, is not the only element to be taken into account, as the quality of the military equipment is also crucial for the purpose of deterrence. For instance, the West is on the edge of a quantum leap concerning helicopters as a platform, but the kind of platform that will be developed might not be the right one for certain kind of missions and might not be interoperable with other platforms, such as war ships. These kinds of dilemmas are telling of the complexity of the defence planning process.

The future scenarios in this field will also be extremely influenced by the development of the security and geopolitical situation in the Indo-Pacific, as well as by the progressive necessities of the energy transition that might affect tech military industries. These stakeholders, moreover, will be particularly crucial in their role to transform demand of military needs into suitable outputs, provided that political elites will be able to clearly define the real necessities in this field. The continuation of the war in Ukraine is certainly a challenging factor for the EU and the West, that must be able to navigate the complexity of the current technological competition, while remaining steadfast in their support to Kyiv, preventing future threats through an increased deterrence capacity.

If on the one hand, military industries will have to balance between different constraints linked to the ESG criteria and the sustainability of the supply chains, on the other governments will be asked to clearly define strategies for the medium-long term, in order to allow for the implementation of the necessary technological progress against disruptive technologies. In this, NATO and Project DIANA (Defence Innovation Accelerator for the North Atlantic) could certainly provide the right support in keeping the pace with the fast-approaching future. This innovation hub, based in Turin, will certainly encourage innovation from the private sector and bring new solution to the threats coming from disruptive technologies. Concerning European Member States, the unsolved knot remains how to improve the common procurement given the different perception and sense of urgency for military industries to be enhanced among the different European countries. A pragmatic approach by the EU would be needed, in the guiding framework provided by the EU-NATO cooperation, working beyond rivalry and strengthening the Western posture against Russia.

## Cyber space: a beacon for democracy colonised by disinformation campaigns

Since it was invented, the internet was thought to be the true instrument for democracy as well as a beacon for democratization. This is an assumption that cannot be made anymore, for several reasons, including the Chinese will to fragmentate the internet, starting from the underlying protocols of network communication. The digital domain brings challenges on multiple levels, from the infrastructure and the physical layers to the logical and content that are conveyed online. While involving all aspects of human lives, digital transformation has created other forms of asymmetry that include the increasing inequality between people that have access to the resources and the necessary skills to navigate the complexity and those who do not. Moreover, the distinction between virtual and real has faded, and this might lead to a loss of centrality for the human dimension.

As democracies are built on their population and the consent that is created around policies and parties, internet as a mean of communication represents a strategic battlefield where the war is already being fought. Since the eruption of Covid-19, and even before, the digital space has been colonised by the spread of conflicting narratives, disinformation and misinformation campaigns that have gained the size of real hybrid warfare tools. These campaigns are characterised by a deliberate distortion of reality to create a model public opinion through media and internet, based on feelings instead of facts. Hanna Arendt would argue that “the inability to distinguish between fact and fiction as the key to totalitarianism”, which is why disinformation and conspiracy theories are indeed a threat to our democracies. They have no borders, they move across countries, languages, and formats, poisoning the trust between government and citizens and hampering the inner principles of democracies. This is what has been observed for instance with the group QAnon in the US, whose calls to action are based on the spread of disinformation and conspiracy theories. Just in the first weeks of the Covid pandemic in 2020, UK telecommunication towers were burnt, and other incidents connected with infrastructures were observed and connected to QAnon theories.

Several actors and stakeholders are developing instruments to fight against disinformation, to secure Western information space and to avoid weaponization of data and information, that include for instance digital tools to rate the information sources. Some experiments are done using AI as well, but human action is needed and cannot be replaced to contrast disinformation. A people centric approach, taking into account ethics and the human factor behind technology seems to be key in facing the threats coming from the digital dimension. In this framework, it is not a case that the CEO of Google has called for a greater involvement of social scientists and philosophers to address the ethical effects of AI. If on the one hand the real effort for governments should be to improve communication and fight disinformation through digital literacy and education initiatives, on the other hand the cyber domain remains a critical vulnerability for the security of Western democracies.

The digital ecosystem as we know it was not designed to defend itself from malignity: it was crafted to allow communication and free flows of information, being created and engineered in a time and under the belief that malignity would not conquer the internet. Nevertheless, as disinformation and cyber-attacks demonstrate, this not the case anymore. But the internet was never meant to be controlled, and this is both an advantage and a challenge. This intrinsic nature is more challenging for Russia, that is more interconnected with the global network, while it is less problematic for China, which started soon to impose restrictions on internet freedom, but still needs to be connected to the rest of the world for economic reasons. Possibly, this

means the world will not see a full fragmentation of the internet, but only its disentanglement, as it is happening with trade. The difficulty for democracy to control what is happening online is of course particularly relevant as a terrain where hybrid warfare through disinformation and cyber-attacks will continue to be carried out.

### **To strategic competitiveness and beyond**

In front of all these challenges emerging both from the digital domain and from the analogic world, EU Member States need to act cohesively and improve their degree of cooperation. The EU single market represents the only way the EU can still be relevant in the global competition. The efforts of the current European Commission are evidently in line with the necessity to keep the pace with other superpowers. Both the Digital Decade and the Chips Act, as well the Strategic Compass, are providing not only guidance but also resources and practical tools for the EU to be more autonomous. Especially in the cyber defence field, the use of Defence Funds was crucial to upgrade the EU cyber resilience capabilities.

Still, there are a lot of issues the EU must be ready to address. New technologies rely mostly on chips and software: unfortunately, the EU is weak both in manufacturing chips and in digital development. Innovation in the EU is hampered by complex bureaucracy, risk-averse cultural approaches and difficulties in collecting funds. Concerning drones used in Ukraine, most of them come from Chinese manufacturing enterprises. While the giant tech private companies that are engaged in the conflict at the moment are mostly coming from the US, one is left to wonder whether the EU will ever have the same capacity. In the battle of innovation, the private sector is in fact much more important than governments are.

In this technological war, as in any conventional one, adversaries are always going to strike where the other is weaker. This means that it is highly likely for Russia to continue using hybrid means – such as disinformation and strikes against infrastructures – and probably this will apply to China as well. It still remains to define whether disruptive technologies favour the attack or the defence, but it would be unwise for the EU not to compete for primacy in terms of research and development of both defensive and offensive capabilities.

The EU should shift the focus from strategic sovereignty and autonomy to strategic competitiveness, acknowledging the topical moment we are living in and responding to the wake-up call on the variety of different threats the present is bringing. All EU Member States will benefit from the increase of industrial defence and cyber capabilities, also with the aim of protecting democracy in the World Wide Web, and this implies investing in innovation and taking the necessary risks to achieve this goal. For a long time, the EU has fought to preserve the “European way of life”, calling for inclusion and connections as the basis of peace and prosperity. This dream is scattered but not lost. The digital world has been weaponized, but inclusion, as a mean for people’s empowerment, still represents the key for the internet to have a positive outcome in the European society.