Young Aspen Leaders

A Comprehensive New European Architecture: technology, democracy and security

by Gerardina Corona

Gerardina Corona is a Lieutenant Colonel, Chief of the Press Office-External Relations, Carabinieri Corps Headquarters, Rome; Alumna Aspen Institute Italy.

Since 2020, events that have affected the entire world have impacted people's daily lives setting new priorities and creating a "new normality". The first major event of this changing season was the Covid-19 pandemic.

To address it, each Government searched for the right tools to deal with and manage the disease: oxygen cylinders, masks, ventilators and vaccines have been crucial, especially as the prime example of international cooperation. In this historic phase, the exchange of information and data management has gained strategic importance for the security of nations, so discoveries that could help end the pandemic were to be fostered promptly.

The second major recent event that shook the global balance was the invasion of Ukraine by the Russian Federation. Here, too, the management of data and information has had a fundamental impact on the course of events in a multitude of levels.

Information is widely used as an indirect weapon in projecting soft power: targeted propaganda campaigns, dissemination of fake news and systematic censorship of information sources associated with the perceived enemy.

Furthermore, data and information are at the center of a real digital battle - the cyber warfare. It is not just people who are susceptible to IT attacks; on the contrary, in most cases the objectives are the IT systems of infrastructures and strategic companies, with the intention of damaging,

cancelling or requisitioning access to data, interrupting business continuity and the efficient delivery of services.

It is in this context of crisis that the concepts of “European technological sovereignty” and “strategic autonomy” have emerged. This should not be perceivedas a bypass to NATO, it actually strengthens the alliance, given its interdependency with the EU.

The EU needs to develop a serious technology plan and worthy of its economic magnitude, considering that the Union is the most important economic platform in the world, and the European members of NATO have four times the population of Russia and 12 times its GDP. The growth path of European technological and digital sovereignty must be built by constantly maintaining the combination of technological investments and regulation[1].

In addition, we have seen in recent years the instrumentalization of migrants, the privatization of armies and the politicization of the control of complex technologies. Add to this the dynamics of state failures, the retreat of democratic freedoms, as well as the attacks on the “global commons” of cyber space, the high seas and outer-space, and the conclusion is clear: the defence of Europe requires a comprehensive concept of security. We see conflicts, military build-ups and aggressions, and sources of instability increasing in our neighborhood and beyond, leading to severe humanitarian suffering and displacement. Hybrid threats grow both in frequency and in impact. Interdependence is increasingly conflictual and soft power weaponized: vaccines, data and technology standards are all instruments of political competition[2].

As such, given the both the number and the multiple (hybrid) forms of threats,, strengthening civil and military cooperation has become essential.

The EU’s civilian CSDP missions, provide an essential contribution to rule of law, civil administration, police and security sector reform in crisis areas. They are also crucial in the EU’s wider response by non-military means to security challenges, including those linked to irregular migration, hybrid threats, terrorism, organised crime, radicalisation and violent extremism.

---

[1] Speech by Commissioner Gentiloni at the Peterson Institute for International Economics: Transatlantic economic policy in times of war. 21st April 2022Washington, DC.
[2] A Strategic Compass for Security and Defense - For a European Union that protects its citizens, values and interests and contributes to international peace and security, Council of the European Union, 21 March 2022.

The EU also needs to remain strongly committed to promoting and advancing human security and the respect of and the compliance with International Humanitarian and Human Rights Law and the protection of civilians, including humanitarian personnel, in all conflict situationsfurther developing due diligence policy in this regard.

Hybrid threats and connectivity

State and non-state actors are using hybrid strategies that include cyberattacks, disinformation campaigns, direct interference in elections and political processes, economic coercion and the instrumentalisation of irregular migration flows. Russia and China are not shying away from using emerging and disruptive technologies to take strategic advantages and to increase the effectiveness of their hybrid campaigns. In the Cyber domain, our forces need to operate in a coordinated, informed and efficient manner. We will therefore develop and make intensive use of new technologies, notably quantum computing, Artificial Intelligence and Big Data, in order to achieve comparative advantage in cyber responsive operations and information superiority. Cyber defence is paramount to ensure that Enhanced Military Mobility unfolds its full potential as essential enabler.

At the same time, free and safe access to global strategic domains is more and more contested. Cyberspace has become a field for strategic competition, at a time of growing dependence on digital technologies. We are increasingly facing more sophisticated cyberattacks. It is essential to maintain an open, free, stable and secure cyberspace. Notwithstanding the principle of the peaceful use of outer space, competition in this domain has strong security and defence implications. It is key for observation, monitoring, navigation and communication capabilities, yet it is a congested and contested domain.

Maritime security in the Baltic Sea, the Black Sea, the Mediterranean and the North Sea, as well as of the Arctic waters, the Atlantic Ocean and the outermost regions is important for the EU's security, our economic development, free trade, transport and energy security. Maritime zones, critical sea lanes of communication and several maritime chokepoints as well as seabeds, are increasingly contested.

The recent explosions at the North Stream pipeline raised the level of attention to the safety of these vital infrastructures, and have also turned the spotlight on what would happen if such an attack was carried out against submarine cables for Internet connections.

In fact, geopolitical competition is evolving more and more from the “war for the territory” to the “war for connectivity”, that is a constant tug of war between states for their supremacy over global supply chains, energy markets, industrial production and on the very precious financial, technological and knowledge flows. In this context, therefore, attacking the submarine cables responsible for managing the Internet traffic of large portions of state territories, or even entire continents through the so-called “bottlenecks”, would significantly weaken the actors thus affected.

The threat is real, as are its material consequences. This is mainly due to both the lack of security around this type of infrastructure, and the willingness of authoritarian regimes to increasingly attack non-military targets, using hybrid warfare techniques. Submarine cables are highly important for the functioning of the Internet network and, implicitly, of the services that depend on it: - they enable 97% of Internet traffic, and about 10 billions dollars in financial transactions every year),

Imagining the Internet as something “ethereal” and intangible is a naivete we cannot afford, as we risk underestimate the threats to the primary technological infrastructures on which the Internet has always been based.

A common European security architecture will have to be put in place above all through strengthening the security of information and communication technologies, as approved by the EU member states during the European Council held in Brussels on 20 and 21 October.

Looking at technological developments with a view to a new security architecture, Europe will certainly not be able to neglect the theme of AI (Artificial Intelligence) in the military field, developed in consideration of shared and ethical values. In the absence of a common European Army, the condition sine qua non for expanding interoperability between the Armed Forces of member countries is investing in shared defence systems, with technological ones playing an increasingly important role.

The digital world and democratic principles

It is precisely on this last aspect that an in-depth study is necessary, in order to avoid that the development and technological progress, used to enhance European security, takes a path not compatible with ethical and democratic principles. The relationship between digital technology and democracy will therefore have to redesign the boundaries of freedom and the extension of power, but at the same time the implementation of these new technological tools will have to be applied with caution, always taking into account the strength of the democratic fabric[1].

First , as outlined in the study prepared by a European task force on the subject of democratic artificial intelligence[2], such a revolutionary and certainly invasive technological development needs to be essentially based on principles such as justice and autonomy.

The importance that ethics should remain at the heart of any use of technologies, especially where they are entrusted to institutions as a new means of security architecture, was at the heart of the EU-funded initiative in 2012, RISE (Rising pan-European and international awareness of biometrics and security ethics), in which an important debate was launched regarding the case of biometric techniques capable of allowing the collection of enormous amounts of data on people. In this case, the use of information and biometric technologies, conceived as democratic forms of control and respectful of citizens' rights, can be tools capable, among many objectives, of reducing illegal immigration and facilitating the fight against terrorism and to organized crime. However, the delicate aspect of these tools is that the technologies that make use of biometric identification (e.g. facial recognition) are considered by the European Union to be intrusive systems because “they evoke a feeling of constant surveillance and indirectly dissuade from exercising the freedom of assembly and other fundamental rights”[3].

A report of the European Council on Foreign Relations entitled “The Geopolitics of technology: how the EU can become a global player”[4], highlights the following recommendations for the purpose of a democratic use of technologies:

---

[3] *“Democracies and Power of data”, A. Soro.*
[4] *AI4 PEOPLE project.*
[5] *Press release, European Commission, 21 April 2021, Europe ready for the digital era.*
[6] *https://ecfr.eu/publication/the-geopolitics-of-technology-how-the-eu-can-become-a-global-player*

» the creation of a global fund to protect democracies, with the aim of protecting democratic elections from potential foreign interference operations and cyber-attacks;

» creation of a fund to facilitate global regulatory convergence on digital rights, to ensure the security of electronic communications and an ethics of artificial intelligence;

» lead the establishment of a global alliance on democratic governance and the ethics of technology (this fundamental) by facilitating the creation of committees on the democratic use of technology;

» ensure, at the same time, a rapid and effective application of technological sanctions.

Investing in innovation and making better use of civilian technology in defence is key to enhancing our technological sovereignty, reducing strategic dependencies and preserving intellectual property in the EU. It is also necessary to foster synergies between civilian, defence and space research and innovation, and invest in critical and emerging technologies and innovation for security and defence. Strengthening the resilience of our supply chains and industries' access to private funding will be necessary for the European Defence Technological and Industrial Base. The European Investment Bank should also use all its tools to contribute to that effort. It is equally important to ensure that horizontal EU policies, such as initiatives on sustainable finance, remain consistent with the European Union efforts to facilitate the European defence industry's sufficient access to public and private finance and investment[1].

The management of the enormous amount of data available today (Data Governance), the definition of the new relationship between human beings and Artificial Intelligence (Human Automomy Teaming), the use of Autonomous Systems to support or replace the military, the regulation of the new domain Space, the strategic impact of the hypersonic threat, the new potential of quantum technology and the application of biotechnologies to the civil and military context are just some of the issues developed that require specific in-depth analysis in terms of implications for defence and international security.

[7] *A Strategic Compass for Security and Defense - For a European Union that protects its citizens, values and interests and contributes to international peace and security, Council of the European Union, 21 March 2022*

The challenge of Artificial Intelligence and the EU's response

In the light of a new revolution and technological transformation, a profound cultural change therefore appears inevitable, which will certainly require new priorities, courage and determination, speed and adaptation to new levels of risk, investments and an ever-greater search for concrete and effective synergies.

Progress and technological innovation entail multiple challenges and offer great opportunities. Society, economy, politics and the military world are modified and influenced by the pervasiveness of new technologies, without however fully understanding the real change or the extent of the consequences. Not all inventions have brought about the desired advantages and transformations but, on the contrary, some have given rise to instability, criticality and generated new and heterogeneous forms of threat. The reality is that humans, in their ability to progress and innovate, must necessarily increase their ability to adapt, and focus on predicting the effects of their actions.

The evolution of technologies (innovative, emerging or disruptive that they are) changes at a surprising speed and the main challenge, especially for future generations, will be to operate with speed, in a predictive mode and, unfortunately, living with a potential degree of indeterminacy, insecurity and increasing risk. It is therefore essential to identify and study those indicators which, if caught and intercepted in good time, will make it possible to anticipate the changes underway, and those that will probably manifest themselves in the medium and long-term future. It is therefore essential to support a concrete cultural and cognitive transformation that leads us to develop a real "Culture of Innovation".

Technological innovations, which have contributed to the improvement of living conditions, are the result of the evolutionary development and the work of human. In consideration of the disruptive strength inherent in "emerging and disruptive technologies" , we are called upon to better govern and manage their development and future use.

A revolution that, in reality, also embraces the training sector, the employment of personnel and leadership, transforming itself into a substantial and important mindset change.

In this vain, the application of artificial intelligence to military defence raises a number of ethical and regulatory issues, some of which appear particularly relevant: first, the correct dosage of AI, or the balance between its non- and excessive use.

Human organizations often pose unjustified obstacles and strong “internal” resistance to the use of innovative and transformative technologies. This is an example of underutilization often seen in public administration sectors such as health, justice and education; yet, not even the business world is immune, although it is known that AI is primarily what gives today's companies their competitive advantage.

On the other hand, the growing presence and relevance of Artificial Intelligence systems in contemporary societies has implications that transcend the technological aspect and possess a profound transformative potential, yet raising questions of an ethical, legal, organizational and moral nature. In fact, all these applications are undoubtedly revolutionary in scope and open scenarios full of further potential, but at the same time they involve various risks, often inherent in ethical, legal and social acceptance issues, whose interpretation is not univocal, nor is the way to approach it.

Among the most debated issues , is that of the responsibility for any damage caused by devices that make use of AI (of the manufacturer? of the owner? of the algorithm programmer?). Numerous approaches have been proposed, all depending on the degree of autonomy and the application context (among these there is one that suggests the establishment of an “electronic personality”).

Another concern is on the values to be used as a reference for the ethical evaluation of AI (a possible answer could be to use the Charter of Fundamental Rights of the European Union) and the ethics of the use of robots in the military, highly divisive issues with persuasive arguments on all sides.

Furthermore, the processing of personal data through facial recognition and very detailed profiling of individuals, in order to understand interests and propensities to purchase products, can lead to biases determined by the type of data that have been used to train the AI algorithms.

It is no coincidence that the issue of the unconscious re-proposition of discriminatory prejudices deriving from cognitive biases has assumed considerable importance in

the debate on new technologies which, reflecting in the type of data entered and, therefore, in the algorithms, would effectively nullify the supposed impartiality of AI systems. These conditions include a plurality of human characteristics such as ethnicity, age, gender, sexual and / or religious orientation. Basically, since the functioning of the algorithms is based on the entry of "historical" data, the risk that these data reflect historically established prejudices and social distortions is very high.

The analysis of future scenarios (2040+) indicates an increasingly decisive and pervasive role of emerging and disruptive technologies that will substantially change society, the economy, politics and the dimension of national and international security and defence. Technological development, characterized by an exponential trend, proceeds so rapidly that it does not give the opportunity to understand the change, let alone the related consequences. A proactive and shared approach is therefore necessary between institutional actors, the academic environment, the industrial world and research to bridge the conflict between the life cycle of technologies and development and procurement times. The ability to develop and implement these technologies then focuses on the essential issues of the independence of a state as a fundamental tool to support its level of strategic ambition with respect to its main competitors.

It is clear that efforts to intercept technological development in a predictive key must be supported by a "new" attitude that takes into consideration other factors at play such as training and the legal component. Leadership, and not only, must become aware of changing their mindset in terms of managing complexity. Accepting to invest in multiple projects, taking into account that, even if considered promising, only a few of them will give the desired result. Therefore, establish a selection process that brings out only the best performing ideas. In addition, attention must be paid to the legal component that is slowly becoming a real multiplier lever, or even an active tool, in redefining the equilibrium also in terms of technology. In the context of the comparison with the major competitors, it should not be underestimated that the counterparty could use the ethical-legal corpus, which characterizes Western companies, to its own advantage and in a malevolent way (relativization of law and ethics) in order to exploit its vulnerabilities (so-called lawfare).

Another legal ethical aspect also emerges from the evident contrast even in the digital field between the rigidity of the rules imposed on citizens and the freedom of action of cyber-criminals. An obvious example is the provision of data that citizens perform when using software or visiting the web: the recent European regulations implemented by individual states (see the GDPR) require citizens to express numerous consents, which often are more of a burden than a protection, also because companies tend to make possible dissent complicated. On the other hand, those who act in a gray area are very easily able to illegally collect user data, for example through apparently harmless and playful apps and programs. It would therefore be necessary to better balance the protection of personal data and the procedures for providing them, which is more for the real protection of the user citizen, just as it is necessary to harmonize these regulations at an international level, also guaranteeing the necessary legal and technical instruments for international police cooperation. to effectively combat the misappropriation of personal data for the purposes of cyber-crime.

In the near future, a leadership model characterized by a flexible approach aimed at managing, promoting and guiding change marked by increasingly complex challenges and the speed of decision-making processes will prove successful. The combination of these two factors will mark the flywheel for a new paradigm characterized by an e-leader with less and less technical skills (without eliminating them) and more and more transversal skills (“soft skills”) who is inclined to experiment by putting aside “biases” cognitive.

The dynamics of technological sovereignty, accelerated - let us remember - by the Covid-19 crisis, constitutes in many ways a leap forward in technological modernization. It outlines a promising future for a Europe that can review its priorities and its tools to definitively project itself as a pole of global technological democracy.