Marco Mayer (in collaboration with Francesco Gabrielli)

Next generation Eu: The digital transition's policy dilemmas

NEXT GENERATION EU: THE DIGITAL TRANSITION'S POLICY DILEMMAS

In the Nineties it was exceedingly clear that «cyberspace» had become a new artificial domain of power in international politics in addition to the four previously identified domains (land, air, maritime, and space). As to warfare, this new dimension implies a network-centred and information-sharing approach both between the army, the navy, the air force, the space and within the different military forces, including the use of Artificial intelligence. This multi dimensional domain affects human societies in a profound way and already deeply influences not only everyday life, but also human behaviour, finance, trade, and international politics in all the previous four domains combined. This is why we have suggested using the definition «digital society» instead of the term «cyberspace» which appears to us – although technically correct – too limited. The European Union decided that the «digital transformation» would be one of the two priorities (together with the green transition) of Next Generation Eu, whose strategy is intended to benefit European citizens, businesses and the environment. This can be achieved only if the Eu's approach is based on thorough understanding of the criticalities of the digital transition. The Ict revolution together with globalisation created deep and consistent interconnections and interdependencies between the major world powers in the global political and economic arenas, and even in the most resilient democracies new digital technologies – and relevant networks – can challenge the central values of an «open society». On the external dimension, cyberattacks and disinformation coming from state-sponsored groups in countries like China, Iran and Russia are mounting, making the Eu-Us digital and Ict cooperation a renewed priority. The Us and Eu's common goals should indeed aim at fighting ransomwares, disinformation and finalising a common approach to cloud computing and Ai, both at civil and military level, not only to better ensure the safety and privacy of citizens' data, but primarily to safeguard civil, religious, and political liberties, the rule of law and the effective functioning of democratic institutions.

KEYWORDS *Digital Transition, European Union, United States, International Politics, Digital Authoritarianism, Totalitarianism, China, Cybersecurity.*

Marco Mayer, Luiss Guido Carli – Via di Villa Emiliani, 14 (Segreteria Master Cybersecurity) – 00197 Roma, email: mayerkos@yahoo.it.

Francesco Gabrielli, Scuola di Scienze Politiche "Cesare Alfieri" – Università degli Studi di Firenze – Via delle Pandette, 32 – 50127 Firenze, email: francesco.gabrielli1@stud.unifi.it.

ISSN 2785-0072

1. Introduction

Since the end of World War II, 78 years ago, there has arisen a consensus among the world's political science, international relations, military doctrine elite that four, interdependent domains define the strategic spheres of power throughout the globe. These are: land, air, maritime, and space. Since the early Nineties it became exceedingly clear that a fifth domain of crucial significance had emerged in the world, and at the very least, the academic community at a multi-disciplinary level (political, social, strategic and computer sciences) has given that fifth domain a name: «cyberspace». The term arose in popular culture through science fiction and the arts, and to date there is no official definition of it. In fact dozens of academic and military definitions of cyberspace can easily be found (Clark 2010; Mayer *et al.* 2014). The term cyber-ecosystem is also widely used in the scientific literature and has the same meaning[1]. But there is no denial that, whatever its name, the Information communication technology (Ict) revolution has created a new artificial domain of power throughout the world that slices through all of the four natural domains.

As for warfare, one of the most visible outcomes of the Ict revolution is the widespread use of drones as the current Ukraine war clearly shows, but more importantly the digital technologies have created an organisational revolution in the whole chain of Command, control and communication system (C3). This implies a network-centred and information-sharing approach both among the army, the navy, the air force, the space and within the different military forces, especially in the Us new military policies, including the use of Artificial intelligence (Ai) (Rusi 2022; Schiavi 2022; Hambling 2022; Vergun 2022). In June 2022, officials of the Us Defense department discussed the importance of digital transformation and Ai in enabling warfighters to maintain a battlefield advantage, even as China and Russia develop their own Ai for military purposes (Us Army 2021; Vergun 2022).

The new domain will affect every human and all societies in a profound way and already deeply influences not only everyday life, but also human behaviour, finance and trade and, last but not least, international politics in all the previous four domains combined. Thus it can be argued that terms such as «cyberspace» and «cyber-ecosystem», while correct, are not sufficient to analyse the pervasive impact of the technological revolution in the contemporary world. In order to fully understand the implications of the so-called «digital transition» – which is one of the main goals of the Next generation eu (Lilyanova 2022) – we need a wider and deeper definition of what is actually

[1] See «ecosystems» https://niccs.cisa.gov/cybersecurity-career-resources/glossary#C.

at stake in Europe and worldwide. The Eu's digital strategy will benefit European citizens, businesses and the environment only if it is based on thorough understanding of the criticalities of the digital transition. As stated by George Westerman, principal research scientist with the Mit Sloan initiative on the digital economy, «when digital transformation is done right, it is like a caterpillar turning into a butterfly, but when done wrong, all you have is a really fast caterpillar» (quoted in Mit Sloan Executive Education 2014).

Therefore, after addressing the impact of the digital revolution on the consolidation of authoritarian power in already non-democratic societies (section 1), the second section of this article encompasses both economic and political aspects of international relations in the digital era, emphasising the role of technology-driven interdependencies. Given the rise of these new challenges, the third section features an analysis of the most recent developments in the Eu-Us digital cooperation, while the fourth section questions whether there is room for full-fledged democracy in digital societies, with a focus on market power and press freedom during the digital revolution. Finally, the fifth and the sixth sections deal respectively with the Eu's digital ambitions, enshrined in Next generation eu and the Digital compass, and with the related challenges linked to the Italian recovery and resilience plan.

2. Heading towards digital totalitarianism?

Given the pervasiveness of digital technology, a broader and more encompassing conception of the current circumstance may be captured by the expression «digital society» or even better «digital societies», as the digital revolution has a different impact in various countries and in the diverse political, economic, social, religious and cultural contexts. In the political domain the rise of digital-authoritarianism and digital totalitarianism are the worst upcoming dangers[2]. During the Hong Kong protests in 2019-2020, the Chinese government used information from video surveillance, face and licence plate identification, mobile device locations, and official records to identify targets for imprisonment. The same happened in Xinjiang, according to Human rights watch (2022). The study is the most recent in a series that has highlighted the extensive use of sophisticated monitoring, more conventional security measures, and political indoctrination camps in the area, which has acted as a proving ground for methods and innovations later used elsewhere. China's extreme tech programs that border on digital totalitarianism are noto-

[2] Retrieved from: https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

rious. The country's «social credit system» tracks citizens' behaviour, keeping track of everything from speeding tickets to social media posts that are critical of the government. Then, everyone will be given a special «sincerity score». A high score will be necessary for anyone hoping to obtain the best housing, set up the fastest Internet speeds, enrol their children in the most prestigious institutions, and obtain the most lucrative employment opportunities (Kayyali 2022; Lasota *et al.* 2021).

On the contrary, the digital repression that took place in Myanmar in 2021 is one example of the opposite strategy on how authoritarian states can leverage their control over such communication highways to stifle resistance. In addition to regular internet outages, the junta, a military and political force that seized forceful control of the nation, blocked access to social media sites. On February 4, 2021 Facebook, which has more than 22 million users in Myanmar (roughly 40% of the population) was blocked. Before Facebook was banned, anti-coup activists frequently used it to plan large-scale acts of civil disobedience, such as doctors refusing to work in military hospitals, and staging fake car accidents, and sit-ins on trains to cause traffic disruption. After Facebook was banned in the country, protesters moved to Twitter to organise their acts, which was also blocked the next day. Later, on February 9, the junta proposed a cybersecurity law that, according to Human rights watch, would «give it sweeping powers to access user data, block websites, order internet shutdowns, and imprison critics and officials at non-complying companies».

The same kind of digital repression is currently used by the Iran regime against the wide protest following Masha Amini's death on September 16, 2022 (Al Jazeera 2022). The strong interest of several authoritarian regimes in controlling and dominating digital technology can also be linked with the shortsightedness of both American West Coast's «big tech» and the Us Government. The latter's approach was potentially determined by the trust in Hu Jintao's opening-up and the underestimation of Xi's authoritarian attitude, which favoured the rapid change of China's technological ecosystem, which can be referred to as «red tech». This is given by the fact that the technology that seeks to serve either the Chinese communist party (Ccp) or similar non-democratic counterparts has chosen to pursue its defined objectives in opposition to fundamental liberties and constitutional pluralism. China's example is relevant not only because the Prc is pushing for building «national champions» that can outcompete big techs such as Google and Apple, but also because China's technology capabilities directly serve interests, ideologies and inclinations of the Ccp in China and worldwide (Tyagi 2021).

3. International politics and the digital revolution

In contrast to the Cold War dynamics we should also underline that the Ict revolution together with globalisation created deep and consistent interconnections and interdependences between the major world powers in the global political and economic arena.

As was argued by Henry Farrell and Abraham Newman (2020) in Foreign Affairs, «The global economy has become vastly more complex and vastly more interconnected in recent decades, but foreign policy expertise has lagged behind». This is given by the fact that, notwithstanding the complexity of supply chain dynamics, «those who study them rarely engage with policymakers». For this reason, according to Farrell and Newman (2020), «the result is that policymakers now face a dilemma similar to the one surgeons faced at the dawn of the age of modern medicine: pressing demand to fix problems but limited knowledge of how to do so».

As to international economic relations in the digital era, since an increasingly large part of services are provided at zero marginal cost, value creation and value appropriation concentrate in the innovation centres and where intangible investments are made. This leaves less and less for the production facilities where tangible goods are made (Pisani-Ferry 2019). One of the most symbolic examples in this regard is the Internet, which at the beginning was viewed as an extremely decentralised network, but in fact it has evolved into a much more hierarchical hub-and-spoke system, whereby the hub sits in the middle and allows each of the spokes to move in one direction of delivery and meet at a central power, making the entire system more efficient, but at the same time create huge oligopolies. This notwithstanding, asymmetries emerge due to the network structure, leading to major consequences at the geopolitical and geoeconomic level, where democratic values can be undermined.

This is the reason why it is crucial to consider the new international interdependencies, in a time when International relations theories have been challenged by major events such as pandemics, energy crises and the new nuclear threats connected to Russia's military invasion of Ukraine. As Joseph Nye (2018) stated when choosing research agendas, «We did not need to go through the front door». As Nazli Choucri and David Clark (2019) wrote in their book[3], as one of the results of the Ecir Minerva project (Choucri 2015), «our purpose is to show how cyberspace has permeated all levels of international relations – influencing interactions within and across levels – and thus demonstrates its ubiquity in world politics. We shall proceed from bottom-to-

[3] See also Mit (2019).

top, starting with the individual. The same core logic holds when we proceed from top-to-the-bottom. Indeed, 'reversing the Images' is a well-known phrase in international relations. The state system remains critical, but it is no longer the only actor wielding the power and influence. Proceeding along the lines of the well-known levels of analysis model, we put forth a set of propositions that reflect developments of theory consistent with the 21st century realities».

Some other interesting research projects are related to the impact of the Covid-19 pandemic both on the digital revolution and international politics such as, for example, recent Crystal C. Wright (2020) and Abdullah Alhammadi (2022) papers. According to the former, telemedicine had been an underestimated opportunity in the healthcare industry, but during the pandemic (and thus social-distancing), it helped reduce barriers in diagnosis, investigations, and treatment – in addition to allowing patients the benefit of staying in their homes, decreasing risks of infection (Wright 2020). With regard to the latter paper, the analysis of neo-realist and neo-liberal theories in the context of Covid-19, Alhammadi (2022) argues that it has been unsurprising that neorealist priorities of state actors surrounding short-term national self-interest have gained an upper hand since January 2020, in an international system full of unprepared and panicking states. The neoliberal focus on international cooperation also explains subsequent multilateral attempts to work together to distribute knowledge, technology, aid, vaccines, and certain economic costs of the pandemic internationally – so long as doing so can be achieved in a manner that does not interfere with national self-interest. But at the end of the game China and Russia did not reach their political targets due to the weakness of their technical and managing abilities. The sudden policy shift in China in December 2022 from zero-Covid to opening up is still difficult to understand. The main reason seems to be the high level of rebellion by significant part of the population (*ibidem*).

During a time of significant disruptions in the global supply chains, the recent Eric Schmidt-backed Special competitive studies project (Scsp) report indicates that the traditional Silicon Valley approach is changing: China surprised the Us on key «battleground» technologies – including wireless 5G, microelectronics and Ai – as the Asian nation's industrial policy enabled it to dominate markets for drones, high-capacity batteries, critical minerals, solar panels, turbines and shipbuilding. «The Us has some immense economic advantages, but there are some warning lights flashing», Liza Tobin, the project's senior director and a former China director for the Us National security stressed, adding that «the Us needs an America-style industrial strategy that leverages competition in our dynamic private sector and has carefully targeted incentives in sectors where we need to lead». The report calls on the Us government to boost microelectro-

nic production with the help of a large fund to unlock private capital, create an open-source security centre to assist investments in digital infrastructure, establish a national security commission on digital finance and give regulators more power to screen investment flows to China that could threaten Us National security. «We have been pleasantly surprised at reactions from Silicon Valley» Tobin said, «we have seen a sea change where a lot of investors, venture capitalists, technologists, are eager to engage in this American project, interested in national security. Wall Street is a bit behind Silicon Valley, but we see the turn happening» (quoted in Schmidt 2022).

With regard to microelectronics, also the Eu has been accelerating its formal steps for building what has been defined by the Commission as «a more resilient chip supply chain» (European Commission 2021a), especially after Germany, the Eu's economic powerhouse, notified Brussels (in December 2021) of the new Important project of common european interest (Ipcei) to support transnational cooperation projects on microelectronics. This Ipcei, the second after one in 2018, includes twenty member States which aim to target the whole value chain of semiconductors, also supporting First industrial deployment (Fid), but on the budgetary side of the project there are still uncertainties. On the other hand, the Us approved in August 2022 the «CHIPS and Science Act», providing $52.7 billion for American semiconductor research, development, manufacturing, and workforce development (The United States Government 2022a).

4. The Eu and Us digital and data privacy cooperation: an update

The different speed of the Eu and the Us in microelectronics seemed not to characterise (at least initially) the field of data privacy cooperation between the two sides of the Atlantic. However, for several reasons the cooperation between the Eu and United States in the area of data transfer turned out to be more difficult than expected. The Court of Justice of the Eu invalidated (Decision 2016/1250) the adequacy of the protection provided by the Eu-Us Data protection shield (Privacy shield 1.0)[4]. Following the Court decision the

[4] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A3104_8. See also Council Decision (Eu) 2016/920 of 20 May 2016 on the signing, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016D0920.

Eu and Us teams negotiated to establish a new legal framework. On October 7, 2022, President Biden signed an executive order on «Enhancing safeguards for United States signals intelligence activities» (The United States Government 2022b). Along with the regulations issued by the Attorney General, the new order implements the Eu-Us agreement on Privacy shield 2.0 into Us law, after the political agreement between President Biden and Eu Commission's President Ursula Von der Leyen concluded in March 2022 (European Commission 2022). The executive order introduces new binding safeguards to address all the points raised by the Court of Justice of the Eu in its previously mentioned decision, limiting access to Eu's data by Us intelligence services and establishing a Data protection review court (Dprc). On that basis, the European Commission will now prepare a new decision, as well as all the relevant procedures. For Europeans whose personal data is transferred to the Us, the new executive order provides for:

- binding safeguards that limit access to data by Us intelligence authorities to what is necessary and proportionate to protect national security;
- the establishment of an independent and impartial redress mechanism, which includes a new Data protection review court (Dprc) to investigate and resolve complaints regarding access to their data by Us national security authorities;
- the executive order requires Us intelligence agencies to review their policies and procedures to implement these new safeguards.

These are significant improvements compared to the Privacy Shield 1.0, adopted in 2016. The new safeguards in the area of government access to data will complement the obligations that Us companies importing data from the Eu will have to subscribe to.

There are at least two other issues to address in order to improve Ict and digital cooperation between the two sides of the Atlantic. The Us and the Eu should share common goals at international level in order to fight ransomware, disinformation and finalise a common approach to cloud computing both at civil and military level. This is especially true given the fact that, according to a survey carried out by the German council on foreign relations (Dgap), roughly 46% of respondents claimed that the Eu should move closer to the Us, in the context of the Us-China tech confrontation (while 0% expressed the need to move closer to China).

In order to address the latter issue (cloud computing) we should take note in particular of the recent Google-Thales partnership that is finalised to narrow France's gap with Us companies (Thales 2021; Lefavrais 2022). Cloud computing is an important part of digital technology, and has become the key

pillar for the digital economy (Ma 2021). In 2019, the size of the public cloud market of the world's top 35 economies was strongly correlated to their digital economic volume. However, as the second largest economy, China contributed 16.3% of the global Gdp (World Bank, data in 2019), while the public cloud market only accounted for 5.1% of global Gdp (Idc, data in 2019). This data shows a significant mismatch between the public cloud market and the Gdp, which may restrict the growth of digital economy in China (*ibidem*). This notwithstanding, the compound annual growth rate of China's public cloud market has been around 40% higher than that of the Us in the past five years. As far as Cloud computing is concerned the recent China-Saudi Arabia agreement agreement might open new tension between Washington and Riyad (Saikal 2022). On the first topic, instead, it is interesting to note that Hungary has not been invited to the International summit on combating ransomware which was held at the White House at the end of October 2022 (Euractiv 2021). A potential obstacle to countering both ransomware and the illegal use of cryptocurrencies can indeed be found in the political affinity between Orban (Hungary's Prime minister) and Vladimir Putin (see also Fig. 1).

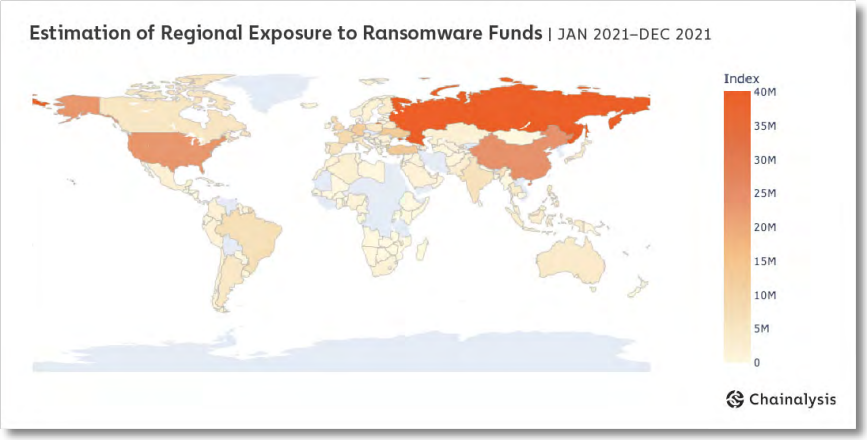

Fig. 1. Estimation of regional exposure to ransomware funds (January 2021-December 2021). *Source*: https://www.euractiv.com/section/digital/opinion/cloud-computing-matters-to-europe-decision-makers-should-help-it-grow/.

5. Democracy in digital societies

In order to investigate this crucial issue, which the above mentioned challenges may affect, this paragraph will refer to a lecture addressed on the

occasion of the Conference on «Cyber, politics and elections» on January 17, 2017, at Tel Aviv University (held by prof. Marco Mayer together with Barbara Carfagna, professor and journalist for the Italian Rai 1). Firstly, it is important to outline the main features of contemporary democracy which, based on my address at the abovementioned lecture, not only include free, regular and fair elections, constitutional limits to majority rule, an independent and impartial judiciary, civil liberties and independent media, but also encompass decent living standards and effective national security with well-functioning law enforcement institutions.

Even in the most resilient democracies new digital technologies and relevant networks challenge central concepts of the idea of «open society». In «The open society and its enemies», Karl Popper famously asserts that the difference between an «open» and a «closed» society is that the former «sets free the critical powers of man», whereas the latter submits to «magical forces» (Mayer and Carfagna 2017).

Joseph Nye (2018) wrote, in his essay «Protecting democracy in an era of cyber information war», that «Democracy depends upon open information that can be trusted. Authoritarian states can exploit and weaponize this openness. Information warfare is not new, and it has always presented a challenge to democracy, but technology has transformed the nature of the challenge». According to Nye (2018), indeed, the element which has opened a new frontier in information warfare is «the speed with which such disinformation can spread and the low cost and visibility of spreading it». A paradox can also be drawn from Nye's essay, whereby given all these new kinds of threats, when democratic governments react, «they run the risks both of doing too little, but also too much», because measures that restrict openness and trust of social media or cyber platforms would become «self-inflicted wounds». According to Nye, this would imply an imitation of authoritarian practices, and therefore it is necessary to identify and choose the most suitable measures to react to such threats or attacks. For instance, «dealing with fake news designed to polarize, disrupt, and suppress voting also requires action by the companies but with procedures for protecting transparency in algorithms and processes that reveal difficult trade-offs regarding free speech». Nye then concludes by stating that «American actions have been inadequate [...] but some useful steps have begun, and this discussion has suggested more that can be done. We are only at the beginning of a long process of protecting democracy in an era of cyber information war».

Digital transition and market power

As the focus shifts once again towards economic issues and relevant globalisation processes, the key question that arises is how the competitive analysis of market power should be adapted to digitalisation. Indeed, new forms of domination by major companies and the growing tendency to outsource fundamental (i.e. financial market) decisions to algorithms, intrinsically challenge this idea of free and fair competition in an open society. Both markets and fair competition are at stake both at the European and global levels.

By analysing a working paper of the Oecd, published in 2021, it appears that there has been a shift in market power towards large firms, since complex technologies requiring large amounts of data and highly specialised skills may be easier for large firms to develop (McMahon *et al.* 2021). This results in a trend towards greater concentration, higher mark-ups and falling business dynamism in the economy, which might be potentially detrimental to consumer welfare. A further Oecd document, published in 2022, reviews a range of concepts and terms recently applied to digital market dynamics that are related to market power. This includes particular types of «power» held by firms in digital markets (e.g. bottleneck power), and designations developed to capture the influence of specific firms in the context of new regulatory initiatives (e.g. gatekeepers). Moreover, the Oecd note highlights the risk of growing divergences in the application of new regulatory designations, concluding that market power should remain a core guiding principle as the competition policy community faces these new challenges in the digital era.

Freedom of press journalism and the digital revolution

Another pillar of open societies is press freedom. The question therefore arises as to what extent the digital revolution has affected journalism. A profession that used to be reliant on newspapers and Tv is now based on websites that can be accessed from smartphones, computers, and even smartwatches. This technology has tremendously impacted journalism. Even the profession of journalists is at stake as anyone has the potential to tell a news story due to the accessibility of the media over technology. Stories can be published artificially worldwide in a matter of seconds. Television has the potential to broadcast digital media immediately. However, the utilisation of such new tools doesn't seem to create a positive impact. As a result of the advancement of technology, the media is more accessible and manipulative than ever due to the use of social media and the advancement of the Internet. Stories can also be published almost instantaneously and can be viewed by everyone with either a

computer or a cell phone. However, as the media becomes more dependent on technology, stories have a much higher risk for the potential to receive a bias or be manipulated easier than previously. In an article by Dan Rather and Elliot Kirschner (2018), published in 2018, the authors argue that even if it is true that the digital age enables people to more easily access information, the fundamental element that keeps democratic societies honest is the investigative and on-field journalism that is behind those news.

6. The digital transition and Next generation Eu

Drawing from what has been argued in the section on how the technological revolution is affecting international politics, market economy and freedom of the media show that digital societies are not Alice's Wonderland as many scholars had envisaged in the Nineties. Nonetheless, besides these dark sides the ongoing digital transformation has also many positive outcomes and this is why – together with the green transition – the European Union decided that the digital transformation would be one of the two priorities of Next generation eu (Ngeu), whose main funding instrument is the Recovery and resilience facility (Rrf). The twelfth recital of Regulation (Eu) 2021/241, which established the Rrf, indeed outlines the aims and the means by which the Eu should pursue the digital transformation, stating that «Reforms and investments should in particular promote the digitalisation of services, the development of digital and data infrastructure, clusters and digital innovation hubs and open digital solutions». The recital further stresses that the digital transition should be carried out by respecting «the principles of interoperability, energy efficiency and personal data protection» and that it should «allow for the participation of Smes and start-ups, and promote the use of open-source solutions»[5]. The Eu thus sets out a novel form of governance with member States, through a mechanism of annual cooperation between the Union's institutions and the member States to ensure that the Union jointly achieves its ambition.

Less than a month after the entry into force of the Rrf regulation, the Commission presented (on March 9, 2021) a communication entitled «2030 Digital Compass: the European way for the digital decade»[6] which established four key priorities for meeting the Eu's medium to long-term objectives while

[5] Regulation (Eu) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and resilience facility.

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52021DC0118&rid=4.

enhancing its strategic autonomy. The digital targets for 2030 are indeed digital skills, digital infrastructures, digitalisation of businesses, and digitalization of public services. Whereas in its communication the Commission states that «digital infrastructure and rapid connectivity bring people new opportunities», it also recognises the fact that the Covid-19 crisis has exposed the vulnerabilities of the Eu's digital space, its increased dependency on critical, often non-Eu based, technologies» and it has «highlighted the reliance on a few big tech companies, saw a rise in an influx of counterfeit products and cyber theft, and magnified the impact of disinformation on our democratic societies». The digital compass tool will provide the monitoring and governance mechanism to track the digital decade's four goals, including Key performance indicators (Kpis).

In mid-November 2022, the Eu's leading institutions – Council, Parliament and Commission – concluded negotiations on Eu values in the digital world, agreeing on an «Interinstitutional declaration on digital rights and principles», which followed a proposal put forward by the Commission in January 2022. In the margins of the European Council, on December 15th, 2022, the European Parliament, the Commission and the Council (with the rotating Czech presidency) signed the text of the declaration, which was thus adopted.

When considering the first of the four digital targets for 2030, while aiming at endowing the Eu's population with basic digital skills, following the European pillar of social rights action plan and the Digital education action plan, the «Path to the digital decade» projects the target for those aged 16-74 with at least basic digital skills to 80% in 2030. Moreover, digital training and education should support a workforce in which people can acquire specialised digital skills to get quality jobs and rewarding careers. In addition, addressing the major shortage of cybersecurity skills in the Eu workforce will be essential, as an important component of protecting the Eu against cyber threats. Therefore, in addition to the target on basic digital skills established in the European Pillar of social rights action plan, the Eu shall have a target of 20 million employed Information and communication technologies specialists in the Eu, with convergence between women and men.

As to digital infrastructures, the Commission has identified an initial list of areas where cooperation among member States is necessary to reach the Digital decade targets, encompassing a European Common data infrastructure and services, the endowment of next-generation low power trusted processors, the pan-European deployment of 5G corridors, the acquisition of supercomputers and quantum computers, connected with the EuroHpc joint undertaking, the development and deployment of ultra-secure quantum and space-based communication infrastructures, and the deployment of a network of

Security operations centres, as part of the Eu Cybersecurity strategy. Together with a more connected Public administration, a European blockchain services infrastructure (Ebsi) will be key to secure growth along with European digital innovation hubs (Edihs) and high-tech partnerships for digital skills through the Pact for skills.

Looking closer at the digitalisation of businesses, it can be seen that the Eu's priorities mainly centre on building a real data-driven economy as a catalyst for innovation and job creation, favouring the digital transition of enterprises and improving the business capabilities in crucial sectors leveraging digital capabilities (e.g. Ai, cloud and cybersecurity).

The last – but not the least important – of the four targets foresees the digitalisation of public services. By 2030, the Eu's objective is to ensure that democratic life and public services online will be fully accessible for everyone, including persons with disabilities, and will benefit from a best-in-class digital environment providing for easy-to-use, efficient and personalised services and tools with high security and privacy standards[7]. In its 2021 Communication on the digital compass, the Commission also stresses that secured e-voting would encourage greater public participation in democratic life, user-friendly services will allow citizens of all ages and businesses of all sizes to influence the direction and outcomes of government activities more efficiently and improve public services. Europe must harness digitalisation to drive a paradigm change in how citizens, public administrations and democratic institutions interact, ensuring interoperability across all levels of government and across public services[8].

As an example, drawing from the previous paragraphs, it can be seen that during the pandemic telemedicine consultations grew more in one month than they did in the previous 10 years, and this played a key role in keeping queues down at hospitals and maintaining patients in good health[9]. According to the Commission's 2021 communication, «the ability for European citizens to access, and control access to, their Electronic health records (Ehr) across the Eu should be greatly improved by 2030 based on common technical specifications for health data sharing, interoperability, developing the secure infrastructure, as well as taking actions to facilitate the public acceptability of sharing health information with the medical community».

[7] See https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52021DC0118&rid=4.

[8] See «Digital Public Services» on Futurium a platform dedicated to Europeans discussing Eu policies. https://futurium.ec.europa.eu/en/digital-compass/digital-public-services?language=en&page=2.

[9] See Digitalisation of public services. https://knowww.eu/nodes/60507ae3769f0200084816d1.

In its proposal for a regulation establishing a framework for a European digital identity (eId) (Com 2021/281)[10], the Commission underlines the need to achieve, by 2030, a «wide deployment of a trusted, user-controlled identity, allowing each citizen to control their own online interactions and presence». Digitalisation also plays a key role in the development of «Smart villages», i.e. communities in rural areas that use innovative solutions to improve their resilience, building on local strengths and opportunities. Moreover, rights and law enforcement are included in the digital transformation process which, according to the Commission, «should also enable modern and efficient justice systems, enforcement of consumer rights and an increased effectiveness of public action including law enforcement and investigation capacities», since «what is illegal offline is also illegal online, and law enforcement must be best equipped to deal with more and more sophisticated digital crimes».

7. Properties of the digital transition and the Italian Recovery and resilience plan (Rrp)

In order to explain how the four cardinal points of the Digital compass are to be implemented at the national level, it is essential to consider the main targets of the Italian Rrp for digital transition, including digital education and e-health. Before analysing the Italian case, it can be argued that there are eight properties that characterise a digital society, and all must be present in order to identify a society as «digital»:

- Hyperspeed: fibre optic, G5 bandwidth explosion;
- Hyperconnectivity: everything connected, 24/7;
- Hypermemory: petabytes, Big data mining, Machine learning;
- Hyper-automation: Iot proliferation, i.e. bot and journalism with Ai;
- Hyper-identity: Trackability/Anonymity/Camouflage;
- Hyper-binary logic: yes/no - that can become an «intellectual prison»;
- Hyper-attraction: emotional involvement; compulsive behaviour; social contagion by hate and fake; easy to enter vs. difficult to exit; silo-based groups, digital addiction pathologies;
- Hyper-reality: Metaverse, Augmented reality (Ar), Virtual reality (Vr), Mixed reality (Mr).

[10] See https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52021PC0281&from=EN.

Each property is measurable and can be combined within a dynamic matrix and applied to any number of cases. The most important element to emphasise is the fact that each of these properties represents a challenge for the effective performance of democratic institutions and the relevant decision-making processes.

This draft theoretical framework based on eight properties must be implemented considering the differences between national societies. Due to differing Italian institutional, historical, political and cultural legacies, the impact of the digital revolution on the key factors (i.e. institutional architectures, political culture and legislation, but also public and private sectors energy, finance, environment, health, security and justice) the Rrp will have some specific features. Taking into account the mentioned properties, at least some critical difficulties can be identified considering the Rrp's digital transition implementation programme, linked to the Italian specific political, cultural and institutional context.

Digitalisation is included in the first «mission» of the Italian Rrp, which allocates around 40 billion euros (roughly 27% of the overall recovery budget) to digital transformation both in the public administration and the private sector. Given Italy's position in the Digital economic and society index (Desi) – 20th out of the Eu-27 with a score of about 5 points lower than the Eu average in 2021[11] – the above mentioned resources represent a historic opportunity for the country to combine investment and structural reforms aiming at overcoming its digital delays. Notwithstanding the ambitious objectives such as increased interoperability in the Public administration, coverage of ultra-broadband networks on the whole national territory and the creation of a National strategic pole through a new cloud model, Italy's technological ecosystem presents some weaknesses, such as the national 5G plan for the mobile market, within the framework of the strategy for ultra-broadband. A slowdown has indeed emerged in the opening of tenders since the international ecosystem is already starting to move towards 6G (Brunetti and Gollin 2022). Another issue which can potentially hamper implementation of the plan is the availability of territorial data throughout the country (*ibidem*), which is critical for digital infrastructures. In the case of Italy, however, since territorial information is largely fragmented, the effectiveness of administrative decisions might be jeopardised.

[11] See Italy in the Digital economy and society index (Desi), https://digital-strategy.ec.europa.eu/en/policies/desi-italy.

8. Conclusion

As was discussed in the previous paragraphs, especially concerning the implications of the digital transition for the evolution of democratic and non-democratic regimes, one key element to be highlighted lies in the nature of digital networks. Although they can be perceived as decentralised and efficiency-enhancing, they hide strong power concentration, which can affect democracy on the one hand, and undermine free and fair market competition on the other. The latter concept can be also linked to the ability, for one political actor (a state), to have a wider range of suppliers or providers when it comes to energy products and digital services. This article has therefore mentioned the role of international interdependencies, in a time when traditional IR theories have been challenged by major events such as pandemics, energy crises and the new nuclear threats connected to Russia's military invasion of Ukraine.

But before considering inter-governmental relations, this paper highlighted one major upcoming danger related to the internal dimension: digital-authoritarianism. The three national cases that have been analysed are indeed characterised by the seizure of digital platforms and media by the authoritarian governments, that use them mainly to either penetrate into and control citizens' private lives (as in the case of China) or to thwart resistance and protests (Myanmar and Iran).

On the external dimension, cyberattacks coming from state-sponsored groups in countries like China, Iran and Russia are mounting, making the Eu-Us digital and Ict cooperation a renewed priority. The Us and Eu's common goals should indeed aim at fighting ransomwares, disinformation and finalising a common approach to cloud computing both at civil and military level. After stressing the importance of a closer trans-atlantic cooperation in this field, the article has focused on the Eu's domestic effort to enhance its digital capabilities. The «2030 Digital compass» must be the reference point for bringing about improved interoperability and data protection, which can be realised with new digital infrastructures. The latter objective is the second of the four digital targets for 2030, together with digital skills (the first), digitalisation of businesses and of public services. The Rrf regulation includes the latter dimension, whose introduction into the Eu's priorities was mainly driven by the fact that the Covid-19 crisis exposed the vulnerabilities of the Eu's digital space and its increased dependency on critical, often non-Eu based, technologies. This has especially been the case of Italy, that – besides having long been dependent on energy imports from the Russian Federation – strengthened its «digital dependency» on China, not only through what I often referred to as

the «Digital silk road», but also in the private sector with the Chinese digital giants, such as Huawei.

It is therefore essential that the unique opportunity presented by the Recovery and resilience plan becomes reality, particularly for the digital transformation, which lies at the core of the no-longer-new cyber domain in the strategic spheres of power.

References

Al Jazeera (2022), *Clashes as Thousands Attend Mahsa Amini Memorial in Iran's Saqqez*, Al Jazeera, 26 October, https://www.aljazeera.com/news/2022/10/26/clashes-thousands-attend-mahsa-amini-memorial-iran-saqqez.

Alhammadi, A. (2022) *The Neorealism and Neoliberalism Behind International Relations During COVID-19*, in «World Affairs», 185(1), pp. 147-175.

Brunetti, M. and Gollin, A. (2022) (eds), *Digital Transformation and NRRP*, Mondo Internazionale, 7 March, https://mondointernazionale.org/en/focus-allegati/digitalizzazione-e-pnrr#_ftn1.

Choucri, N. (2015), *Final Report: MIT-Harvard Collaboration, 2009-2014*. Explorations in Cyber International Relations, Available at https://ecir.mit.edu/sites/default/files/documents/ECIR%20Final%20Report.pdf, (last accessed on 20th December 2022).

Choucri, N. and Clark, D. D. (2019), *International Relations in the Cyber Age: The Co-evolution Dilemma*, Cambridge, MIT Press.

Clark, D.D. (2010), *Characterizing Cyberspace: Past, Present and Future, ECIR Working Paper, 3*, Cambridge, MIT Press, https://dspace.mit.edu/bitstream/handle/1721.1/141692/Clark%20%282010%29%20Characterizing%20cyberspace.pdf?sequence=1 (last accessed on 20th December 2022).

Council of the European Union (2022), *Declaration on Digital Rights and Principles: EU Values and Citizens at the Centre of Digital Transformation - Consilium*, https://www.consilium.europa.eu/en/press/press-releases/2022/11/14/declaration-on-digital-rights-and-principles-eu-values-and-citizens-at-the-centre-of-digital-transformation/ (last accessed on 5th December 2022).

Digital Rights and Principles: Presidents of the Commission, the European Parliament and the Council sign European Declaration (2022) European Commission - European Commission. European Commission, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7683 (Accessed: January 30, 2023).

Euractiv (2022), *White House hosted International Summit on Combating Ransomware*, Euractiv, 2 November, https://www.euractiv.com/section/cybersecurity/news/white-house-hosted-international-summit-on-combating-ransomware/.

European Commission (2021a), *IPCEI on Microelectronics. A Major Step for a More Resilient EU Chips Supply Chain*, https://ec.europa.eu/commission/commissio-

ners/2019-2024/breton/blog/ipcei-microelectronics-major-step-more-resilient-eu-chips-supply-chain_en (last accessed on 21st December 2022).

European Commission (2021b), *Digital Public Services*. Futurium, https://futurium.ec.europa.eu/en/digital-compass/digital-public-services?language=en&page=2 (last accessed on 5th December 2022).

European Commission (2021c), *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as Regards Establishing a Framework for a European Digital Identity*, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52021PC0281&from=EN (last accessed 5 December 2022).

European Commission (2022), *European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework*, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087 (last accessed on 21st December 2022).

Farrell, H. and Newman, A. (2020), *The Folly of Decoupling from China*, Foreign Affairs, 3 June, https://www. foreignaffairs. com/articles/china/2020-06-03/folly-decoupling-china.

Hambling, D. (2022), *Will Ukraine deploy lethal autonomous drones against Russia?*, «New Scientist», 1 November, https://www.newscientist.com/article/2344966-will-ukraine-deploy-lethal-autonomous-drones-against-russia/?utm_source=onesignal&utm_medium=push&utm_campaign=2022-11-02-Will-Ukraine-us.

Human Rights Watch (2022), *China: Xinjiang Official Figures Reveal Higher Prisoner Count*, https://www.hrw.org/news/2022/09/14/china-xinjiang-official-figures-reveal-higher-prisoner-count (last accessed on 21st December 2022).

Kayyali, A. (2022), *How Technology is Steering Us Towards Digital Totalitarianism*, Inside Telecom, 14 July, https://insidetelecom.com/how-technology-is-steering-us-towards-digital-totalitarianism/.

Lasota, M., Bailey, M. and Karlekar, K.D. (2021), *Myanmar's Escalating Digital Repression-and Activists' Digital Resistance*, PEN America, 10 May, https://pen.org/myanmars-escalating-digital-repression-and-activists-digital-resistance/.

Lefavrais, S. (2022), *Thales and Microsoft Partner to Provide Azure Customers with FIDO and CBA Phishing-resistant Authentication*, https://cpl.thalesgroup.com/blog/access-management/phishing-resistant-mfa-with-ms-azure-cba-thales-fido2, (last accessed on 21st December 2022).

Lilyanova, V. (2022), *The Digital Dimension of the National Recovery and Resilience Plans*, EPRS, European Parliamentary Research Service, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733606 (last accessed on 21st December 2022).

Ma, P. (2021), *A Comparison of the Cloud Computing Market between China and the United States*, Alibaba Cloud Community, Alibaba Cloud Research Center, https://www.alibabacloud.com/blog/a-comparison-of-the-cloud-computing-market-between-china-and-the-united-states_597886 (last accessed on 3rd December 2022).

Mayer, M., Mazurier P.A. and Martino, L. (2014), *How would you Define Cyberspace?*, Available at https://www.academia.edu/7096442/How_would_you_define_Cyberspace (last accessed on 20th December 2022).

Mayer, M. and Carfagna, B. (2017), *Is there Room for Democracy in the Digital Society?*, paper presented at the Cyber, Politics and Elections Conference, Tel Aviv University, Tel Aviv, Israel, 17 January.

McMahon, M., Calligaris, S., Doyle, E. and Kinsella, S. (2021), *Scale, Market Power and Competition in a Digital World: Is Bigger Better?*, OECD Science, Technology and Industry Working Papers, 1, Paris, OECD Publishing. doi:10.1787/c1cff861-en.

Mit Sloan Executive Education (2014), *The Digital Business Transformation Imperative*, 12 June, https://exec.mit.edu/s/blog#.XFIWfc1lA2w.

Mit (2019), *Cross Cutting Themes: Knowledge System and 21st Century International Relations*, https://ecir.mit.edu/research/cross-cutting-themes-knowledge-system-and-21st-century-international-relations (last accessed on 21st December 2022).

Nye, J. (2018), *Protecting Democracy in an Era of Cyber Information War*, Hoover Institution, https://www.hoover.org/research/protecting-democracy-era-cyber-information-war (last accessed on 3rd December 2022).

Oecd (2022), *The Evolving Concept of Market Power in the Digital Economy*, OECD Competition Policy Roundtable Background Note, www.oecd.org/daf/competition/the-evolving-concept-of-market-power-in-the-digital-economy-2022.pdf, (last accessed on 3rd December 2022).

Pisani-Ferry, J. (2019), *Farewell, Flat World, Project Syndicate*, 1 July, https://www.project-syndicate.org/commentary/digital-economy-fuels-geopolitical-competition-by-jean-pisani-ferry-2019-07.

Rather, D. and Kirschner, E. (2018), *Why a Free Press Matters*, «The Atlantic», 15 August, https://www.theatlantic.com/ideas/archive/2018/08/why-a-free-press-matters/567676/.

Rusi (2022), *Armed Drones in the Middle East-Iran*, https://drones.rusi.org/countries/iran/ (last accessed on 20th December 2022).

Saikal, A. (2022), *Xi's Saudi visit a Sign of China's Growing Influence in the Middle East, The Strategist.* Austrian Strategic Policy Institute, https://www.aspistrategist.org.au/xis-saudi-visit-a-sign-of-chinas-growing-influence-in-the-middle-east/ (last accessed on 13rd December 2022).

Schiavi, F.S. (2022), *Assessing Russian Use of Iranian Drones in Ukraine: Facts and Implications. ISPI*, https://www.ispionline.it/it/pubblicazione/assessing-russian-use-iranian-drones-ukraine-facts-and-implications-36520 (last accessed on 20th December 2022).

Schmidt, B. (2022) *Google Billionaire warns US Technology Edge over China Slipping, Bloomberg*, 1 November, https://www.bloomberg.com/news/articles/2022-11-01/google-billionaire-warns-us-technology-edge-over-china-slipping.

Thales (2021), *Thales and Google Cloud Announce Strategic Partnership to Jointly Develop a Trusted Cloud Offering in France*, https://www.thalesgroup.com/en/group/

investors/press_release/thales-and-google-cloud-announce-strategic-partnership-jointly (last accessed on 21st December 2022).

The United States Government (2022a), *Fact Sheet: Chips and Science Act will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China The White House*, https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/, (last accessed on 21st December 2022).

The United States Government (2022b), *Fact Sheet: President Biden signs Executive Order to Implement the European Union-U.S. Data Privacy Framework. The White House*, https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/ (last accessed on 21st December 2022).

Tyagi, G. (2021), *Battling Chinese Big Tech Encroachment in India*, Observer Research Foundation, 12 June, www.orfonline.org/expert-speak/battling-chinese-big-tech-encroachment-in-india/.

Us Army (2021), *Army Digital Transformation Strategy,* https://www.army.mil/article/251286/army_releases_digital_transformation_strategy (last accessed on 21st December 2022).

Vergun, D. (2022), *Digital Transformation, AI Important in Keeping Battlefield Edge, Leaders say. U.S. Department of Defense*, https://www.defense.gov/News/News-Stories/Article/Article/3058028/digital-transformation-ai-important-in-keeping-battlefield-edge-leaders-say/ (last accessed on 21st December 2022).

Wright, C. C. (2020), *COVID-19 Pandemic and the Digital Revolution*, in «ASA Monitor», 84(8), p. 30.