GREEN EUROPEAN JOURNAL

Why the EU Needs to Rethink its Approach to Technology

Article by Konrad Bleyer-Simon
January 13, 2022

Ransomware-attacks on critical infrastructure, elections targeted with coordinated disinformation, and overzealous surveillance are some of the downsides of technology that are now well known. The risks that lie ahead – such as the development of autonomous killer robots – are less clearly understood and may seem dystopian, yet these threats are becoming increasingly tangible. Konrad Bleyer-Simon argues that the EU's response must be based on a geopolitical understanding and approach to all these issues.

In September 2021, Europe saw one of its most important elections being targeted by anti-democratic interests, both at home and from abroad. After 16 years under Chancellor Angela Merkel, German citizens cast their vote to elect a successor who could take over what is widely considered one of the most influential public offices in Europe. For a relatively brief window of time during the campaign in early 2021, the Green candidate, Annalena Baerbock, was seen as the favourite – but by summer she had fallen back to third place. There are many reasons why she lost a significant amount of her initial support: she is relatively young and inexperienced, made some mistakes during the campaign, and as a woman was disadvantaged by what remains an extremely macho political environment.

Online disinformation, spread and amplified through social media and messaging apps, is also likely to have contributed to the decline in support for Baerbock. The online activist network Avaaz found that 44 per cent of political disinformation during the campaign was aimed at the Greens. When it comes to disinformation about the candidates for chancellor, 72 per cent targeted Baerbock.

While most disinformation in the German election was homegrown, created by conspiracy theorists and far-right activists, there was increased fear that Ghostwriter – a hacker group linked to the Russian military intelligence service GRU – would step up its operations. It reportedly orchestrated phishing attacks in the German Bundestag. In previous years, Ghostwriter hacked into accounts of politicians and spread anti-NATO disinformation in Poland and the Baltics. Russian disinformation actors are also believed to have contributed to the outcome of the Brexit referendum, and Kremlin-supported hackers played a role in the publication of the Macron Leaks in the run-up to the 2017 French presidential election. Elsewhere, the "infodemic" around Covid-19 amplified anti-vaccination and anti-mask sentiments that led to many otherwise avoidable casualties during the fourth wave of the pandemic.

Tech is not what it promised to be

Although disinformation is probably the most talked about digital threat, it is far from being the only technological risk democracies are facing these days. Distributed-denial-of-service attacks are taking down government and financial service websites and ransomware attacks paralyse the work of hospitals and other core infrastructure. They not only cause financial damages to the companies and organisations targeted but can also have a much broader impact. There have been reports of hospitals delaying procedures and in the US the death of a new born was attributed to the impact of hacking attacks.

The revelations of Edward Snowden taught us that authoritarian and democratic governments alike are building up their surveillance infrastructure, often buying and selling technology and data from each other. While officially technologies built in democratic societies are intended for defence and prevention, this is not always the case in practice. This was made clear once again in 2021 when the government of the EU member Hungary was exposed for using the sophisticated Pegasus spyware to hack into the phones of journalists and opposition politicians.

Just a decade ago, social media providers Facebook and Twitter were praised as catalysts of pro-democracy revolutions (chiefly the Arab Spring); now they are widely seen as tools or accomplices of autocracies. The leaks of the Facebook Papers, for example, revealed that the company’s products contributed to unhealthy teenage body images, ignited ethnic conflicts in developing countries, and amplified hateful messages. It emerged that, despite knowing about these problems, the company turned a blind eye for the sake of profit.

> *Social media providers Facebook and Twitter were praised as catalysts of pro-democracy revolutions (chiefly the Arab Spring); now they are widely seen as tools or accomplices of autocracies.*

Weaponised artificial intelligence

Digital threats come in different shapes and sizes, but probably the most significant element of the array of new technologies is artificial intelligence (AI), which aims at copying some aspects of the functioning of human intelligence to solve tasks like translating texts, turning off the lights in the apartment, or safely driving a car from A to B. These technologies are developed through machine learning, which means that after a certain point the programme begins to code itself: its neural networks allow it to absorb a huge amount of data and look for patterns. As such, AI becomes a technology that uses algorithms and computing power to make sense of the environment it functions in and act autonomously. Although current AI remains in the “soft” category and is thus relatively limited in its applications, combined with control over large chunks of data, hardware, and skilled IT professionals (or even hackers) it can provide unprecedented opportunities for state and non-state players. AI is already used by bots who spread disinformation, it enables microtargeting of polarising political messages, while face scanners and virtual assistant technologies take surveillance and control to unprecedented levels.

A dangerous use of this technology that merits close attention is the development of autonomous precision weapons. Their use is already more widespread than one would assume, for example, the Eurofighter Typhoon aircraft or various surface-to-air systems use sophisticated artificial intelligence to execute their key tasks. They are officially intended for defence purposes, but the technology can just as easily be used to inflict harm. While there is much discussion about only using these technologies with a "human in the loop", the two biggest AI players, China and the US, are unwilling to support international efforts to effectively regulate "killer robots". This is all the more disturbing as the list of countries and actors relying on AI in military settings is increasing. Turkey has developed – and is reportedly already using – a drone called Kargu-2 which can autonomously target and identify people, while the Islamic State has deployed commercially available, non-military drones laden with explosives. If regulation lags behind such developments, we will be increasingly confronted with the threat of home-made killer robots, assembled from goods that were legally bought in hardware shops.

Sure, at this point the technology is not yet perfect. Pro-democracy protesters, for example, can still fool facial-recognition systems with the use of some face paint. But often the weaknesses of AI are the features that distinguish human from machine: the ability to differentiate soldiers from civilians, to weigh non-monetisable costs and benefits, or to realise when a mission needs to be aborted. There are many actors out there who would not think twice about using the technology despite the risks.

> *While there is much discussion about only using these technologies with a "human in the loop", China and the US, are unwilling to support international efforts to effectively regulate "killer robots".*

The main players

Most of the large companies interested in the development of AI and digital technology are based in the US and China. The most well known are the five American GAFAM companies (Google, Amazon, Facebook, Apple and Microsoft[1] – sometimes IBM is included as well, making them the G-MAFIA). Thanks to the large Chinese market, Alibaba, Baidu, and Tencent are just as influential internationally. These companies have already outpaced financial companies in wealth and influence (and with a significant potential to shape policies). Europe does not have equivalents, and even among the few companies established in Europe, many are contemplating a move to the United States.

Although these companies are known mainly for their flagship projects – such as smart devices, digital marketplaces, social media, and search engines – many of these private companies are more effective than public projects when it comes to developing new AI technologies. The American Defense Advanced Research Projects Agency (DARPA) was among the first organisations to experiment with self-driving cars, but Tesla and Google X turned out to be more effective at pursuing their development. The Chinese eHang has gone even further, it reportedly built a self-driving passenger drone.

The way forward for Europe

The many challenges posed by technological development require a strong policy response. Surveillance, disruption, its potential impact on armed conflicts and the excessive influence of the key AI and technology companies are just a few of the problems associated with technological development today. Other disruptive effects, such as the pollution caused by server farms and the extractive industries built around hardware production, are also increasingly recognised.

For the past decades, Europe has stood idly by while the main players shaped the course of technological development. Now it is time for the EU to define what it wants from the digital world, which might require thinking seriously about a European approach to technological sovereignty. This includes the creation of a European value chain but also a better understanding of the ways in which Europe can counteract the harmful developments in technology and set global standards.

> *Surveillance, disruption, its potential impact on armed conflicts and the excessive influence of key AI and technology companies are just a few of the problems associated with technological development today.*

This is all the more important as these technologies can also have a positive impact on our societies: they can revolutionise healthcare, transportation, or political decision-making, and forecast natural disasters or social conflicts. Many experts also see a potential for improvements in environmental protection. Encompassing all these aspects, it is undeniable that technology and AI together constitute one of the key geopolitical issues that the EU will have to deal with in the coming decades.

Not long before the pandemic and the ensuing lockdowns, the European Commission came out with its White Paper on Artificial Intelligence. This is a “regulatory and investment-oriented approach with the twin objectives of promoting the uptake of AI and addressing the risks associated with certain uses of this new technology.” It admits that Europe has been doing badly so far compared to the US and China and highlights that AI investments in North America are at least four times as high as in the EU.

In order to become a global player, come up with a European approach, and remain competitive – while also averting risks – the EU must pay attention to four components: the quality of data, the abundance of well-trained professionals, the quality of software (or algorithms), and computing power. In terms of data, it will be hard to compete with the surveillance capitalism of the US or the authoritarian approach of China that trains its facial recognition software with a database that includes almost the entire Chinese population. Still, Europe should not be discouraged from compiling its own data (as mentioned in the 2020 EU data strategy). The other areas, however, provide more opportunities. Building on the knowledge that can be found, among others, in the AI cluster of Paris or Germany's Cyber Valley, Europe has the potential to become significant, but real efforts are required. The key is to increase investment in research, technology, and education, as well as to provide incentives for experts to stay in Europe.

It is also important to curb the technological behemoths that dominate the AI space. The EU, thanks to Commissioner Margrethe Vestager, has spearheaded some important antitrust efforts to curtail the anti-competitive practices and tax dodging of large tech companies; these were followed by a strategy focusing on regulation and investment. The EU's digital package (comprising the Digital Services Act, the Digital Markets Act, the AI Act, and others) aims to establish a framework that ensures fair competition and protects citizens' fundamental rights in the digital space. Moreover, the Democracy Action Plan establishes platform regulation as an essential component of efforts to safeguard democracy. The pandemic recovery package will invest in the digital economy, notably by encouraging the production of semi-conductors. But there is still a lot more to do – the investment remains insufficient and there is an urgent need to work on the coherence of the European strategy. The EU must step up its efforts to control the military use of AI, protect citizens' data, and end the abuses carried out by the dominant players.

A change in the air?

While there is more to be done, the direction of EU efforts is promising: to provide an alternative to the dominant Chinese and US approaches, there is an emphasis on "human-centric" and "trustworthy" AI. The EU data strategy aims at creating a single market of information, but without the controversial surveillance methods of the current AI great powers. The Commission's document on human-centric artificial intelligence highlights the need for an ethical and legal framework that prevents, for example, algorithms being shaped by the kind of Western, male, upper middle-class bias that exacerbates injustices in some of the current uses of AI, such as in parole decisions or the grading of high-school students.

In the latest edition of the Green European Journal, Green MEP Alexandra Geese and cyber-policy-expert Marietje Schaake share their views about the current challenges and opportunities related to AI, technology, and the European approach to dealing with them. Both experts emphasise the need for the EU to act in a united fashion, as well as for the digital space to be a key component in geopolitical debates. What happens in relation to algorithms, online platforms, hacking, and other digital phenomena is at least as important to Europe's security as the classic security issues, such as nuclear proliferation or terrorism. If Europe is to succeed in this area, it will need a real European approach, a commitment to investment, the protection of digital rights, and coalition building. Some of the approaches on the table are promising, but more must be done and, given the breakneck pace of technological development, there is no time to lose.

[1] Google is often identified through its parent company Alphabet. Similarly, Facebook announced in October 2021 that the social media site was just one of the products offered by the newly established company Meta.

Konrad Bleyer-Simon is a research associate at the Centre for Media Pluralism and Media Freedom. He pursued doctoral studies at the Human Rights Under Pressure joint programme of the Freie Universität Berlin and the Hebrew University in Jerusalem.

Published January 13, 2022
Article in English
Published in the *Green European Journal*
Downloaded from https://www.greeneuropeanjournal.eu/why-the-eu-needs-to-rethink-its-approach-to-technology/