European Parliament

Disruption by technology

Impacts on politics, economics and society

IN-DEPTH ANALYSIS

EPRS | European Parliamentary Research Service

Authors: Philip Boucher, Naja Bentzen, Tania Lațici, Tambiama Madiega,
Leopold Schmertzing and Marcin Szczepański

PE 652.079 – September 2020

EN

AUTHORS

Philip Boucher, Scientific Foresight Unit (STOA), Naja Bentzen, Tania Laţici and Tambiama Madiega, Members' Research Service, Leopold Schmertzing, Global Trends Unit, and Marcin Szczepański, Members' Research Service.

Graphics by Samy Chahri, EPRS

This paper has been drawn up by policy analysts from the Directorates for the Members' Research Service, Impact Assessment and European Added Value and the Library and Knowledge Services within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament.

To contact the authors, please e-mail eprs@ep.europa.eu

LINGUISTIC VERSIONS

Original: EN

Translations: DE, FR

Manuscript completed in July 2020.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

PE 652.079
ISBN 978-92-846-6958-5
doi:10.2861/718464
QA-04-20-446-EN-N

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)

Executive summary

Rapid and dramatic change

Disruption is a specific form of change which occurs relatively quickly or dramatically. Technology has long been seen as a source of disruption to our lives, communities and civilisations, provoking disruptive change at all scales, from individuals' routine daily activities to dramatic competition between global superpowers. This disruption can have both positive and negative effects, although they are often unevenly distributed across different groups.

In the current wave of data-driven internet technologies, the disruptive force of innovation has become a central feature of many firms' business models. However, the key disruptive force of 2020, the coronavirus pandemic, is non-technological. In this context, technologies have been deployed as an antidote to disruption, not least in enabling some social and economic activities to continue while maintaining physical distance.

Disruption by technology

Technology development disrupts the economic system by creating (and destroying) certain business models, supply chains and patterns of employment. In defence, technological innovation has a disruptive effect on all aspects of military activity, from logistics and training to strategic decision-making and physical combat.

Democratic debates have been disrupted by technology developments such as social media. Many of these online platforms benefit from emotional, polarising content and sometimes promote disinformation that can increase rifts in society and undermine democratic processes, whereas facts and information rarely go viral. Social norms, values and identities have also been disrupted by technologies, affecting our most profound understanding of ourselves, our activities and relationships with others.

Disruption to international relations has also been attributed to technology development, adjusting the global balance of power, and even transforming the international system itself. In response to these disruptions, laws and regulations are changing towards a more flexible approach to policy-making, with the emergence of smart regulatory tools.

Converging disruptions

Disruptions in these different domains converge, along with other disruptive forces such as the coronavirus, to propel other phenomena such as extended state and commercial surveillance.

Often, technology disruption can provoke the same kind of tensions at different scales. For example, access to information that informs citizens' voting and purchasing decisions is unevenly distributed, in the same way as it is for company directors and world leaders making strategic choices. Likewise, households, small businesses, large multinationals and nation states all need to find a means of working together with digital tools to make good decisions while maintaining their autonomy.

It is not clear where these tensions will lead us, but our path in this increasingly technology-dependent world will be decided to a great extent by the social, political, and economic choices we make now.

Contents

1. Introduction

Technology development has long been considered as a disruptive force, provoking change at all scales, from individuals' mundane daily activities to dramatic competition between global superpowers. But what do we mean by disruption, and what is disruptive about technology?

First, consider disruption. We can understand it as a specific form of change that occurs relatively quickly or dramatically, but it also implies that the change is provoked by an external stimulus, rather than from within. Sometimes this stimulus is natural, such as an earthquake, while other times it is social, as in political revolutions. While disruption can have negative connotations, its effects depend on the perspective. Moments of dramatic change present challenges and opportunities, but their impacts are unevenly distributed across the different groups affected.

Next, consider technology. While technologies can appear as an external force, they are also deeply social, in the sense that an important part of their existence depends upon human activity. Without a sitter, the chair is reduced to simple pieces of wood. It only becomes a chair by its being **for** sitting on. In this sense, technological artefacts only exist as such through their use by people.[1] Since technologies can only disrupt through human activities, technological disruptions are more like revolutions than earthquakes.

Indeed, technology developments are frequently described as revolutionary. From fragile but lucrative porcelain to crude but deadly gunpowder, from the printing press that invented public opinion to the TV that some say made people 'bowl alone', new technologies have regularly changed the course of lives, communities and civilisations. In the current wave of data-driven internet technology, its disruptive force is a central feature of the business model. This is perhaps exemplified by the 'move fast and break things' motto, initially adopted by Facebook but coming to symbolise the willingness – and even determination – of Silicon Valley firms to disrupt what they see as antiquated social norms, political ideas and economic models, often with a 'better ask forgiveness than permission' approach to legal compliance.[2]

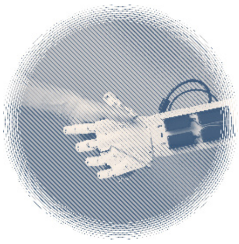
The key disruptive force of 2020 is non-technological: Covid-19. The pandemic may be a natural disruption in the sense that it is a biological phenomenon, but it was certainly enabled by human activities including global trade and long-distance travel. The response to the virus is deeply technological, including the search for treatments and vaccines, the development of contact tracing apps, and the widespread shift to working from home and socialising at distance via internet communications. In this context, technologies are positioned as an antidote to disruption. If, however, these technologies succeed in disrupting coronavirus and re-establishing normality, society could emerge as even more deeply dependent on technologies.

It is in this context that this report examines how technologies can be disruptive. Each chapter is dedicated to the disruption of a different domain: the economic system; the military and defence; democratic debates and the 'infosphere'; social norms, values and identities; international relations; and the legal and regulatory system. Subsequently, surveillance is presented as an example of how technological disruptions across domains can converge to propel other phenomena. Reflections on technology disruption in the context of Covid-19 are embedded throughout all sections.

[1] The social construction of technologies is further explained in P. Boucher What if all technologies were inherently social?, EPRS, European Parliament, 2018.

[2] P. Nemitz, Constitutional democracy and technology in the age of artificial intelligence, Philosophical Transactions of the Royal Society, 2018.

2. Disrupting economies



Technology is often a factor in rapid changes to the economy, including established models, value chains and job markets. These changes are likely to be even more dynamic in the future as workers and organisations from all economic sectors are faced with a multitude of new technologies which generate both opportunities and challenges. Indeed, many argue that digital transformation is a modern form of creative destruction, irreversibly changing economies and jobs.

Business models and value chains

Technology shifts can challenge even the most successful business models. The difficulty of swapping one core technology for another has been demonstrated. By some estimates, only a quarter of efforts to find growth beyond core business succeed. Amazon is an example of successful entrance on new markets with its storage (cloud) and IT services. The difficulty arises because incumbent firms focus their resources on their existing customer base at the expense of developing and applying new technologies that appear from their vantage point to be less profitable. The bankruptcy of Kodak with the arrival of digital cameras illustrates how technology as a source of competitive advantage can morph into a serious burden.

Nokia and Apple

In 2007, when Apple entered the mobile phone market, Nokia held a 50 % market share. By 2019, Apple had a 20 % share with its relatively high price iPhones, and Nokia just 1 %. Nokia's market value dropped from US$150 to US$15 billion between 2007 and 2019, while Apple's skyrocketed from US$110 billion to US$1.4 trillion. Many experts suggest Nokia's key mistake was to focus on hardware (mobile phones) while overlooking software (operating systems and apps). Apple, on the other hand, saw smartphones as an entirely new product category with huge potential for value creation beyond the purchase of the device.

It is difficult for mature companies to change their core business, since they need to identify in advance the causes of possible failure (including potential technological disruption) and the strategies for maintaining success.[3] New firms based on emerging technologies can improve their offer faster and gain a massive global value base, challenging the incumbents. Digitalisation, for example, was based upon using technology to boost the productivity of skills and capital and accompanied by the rise of intangible assets such as intellectual property, software and algorithms. Illustrating the scale of the transition it caused, the world's largest companies in 2008 were characterised by ownership of fixed capital assets, but as the intangible economy took over, by 2018, the five biggest global firms were technology-based.

Technological disruption has been identified as an external factor that pressures innovation of existing business models and value chains.[4] While many innovations are incremental, some can dramatically change price and performance. For example, the internet enabled the gradual emergence of the platform economy, which in turn dramatically disrupted the traditional economic landscape by transforming established business processes, consumer behaviour and value creation, as well as the structure of many industries. These companies developed and implemented a

[3] One approach is to set up autonomous units with the freedom to explore new opportunities.

[4] J. Lee, T. Suh, D. Roy, M. Baucus, Emerging Technology and Business Model Innovation: The Case of Artificial Intelligence, Journal of Open Innovation, Technology Market and Complexity, 2019.

breakthrough in digital business models, based on leveraging the power of software and ubiquitous connectedness.

Disruptive technologies are often seen as enabling simpler, more convenient and affordable products and services, new value propositions, lower costs and lower profit margins, and the creation of new business structures.[5] These characteristics can be seen when comparing platform businesses to their traditional counterparts (e.g. Amazon vs high-street shops, Airbnb vs hotels, or Uber vs taxis). Disruptive technologies can also create new markets (e.g. cryptocurrencies), lead to the failure of dominant firms (e.g. Blockbuster) and generate significant competitive advantages (e.g. Google search engine).[6] While traditional models were based on controlling tangible/fixed assets along a vertical value chain, platforms use artificial intelligence (AI) and big data to orchestrate knowledge obtained from third-parties (users) and capture its value.[7]

Evolving supply chains

First identified in the 'global factory' of China, Covid-19 and its associated confinement policies have disrupted global supply chains. The crisis has focused attention on supply risk management and the supply chain dependence on China. Globalisation, lean business models and 'just-in-time' production also expose supply chains to external, uncontrollable shocks. Furthermore, rising wages in China reduce the efficiency of global supply chains. Possible solutions include reshoring and tightening the chains (nearshoring). While this was generally considered too costly, robotics and automation render it increasingly accessible. One long-lasting effect of the crisis may be the development of risk management practices based on technology and digital infrastructure that can prevent future crises from having the same devastating effect.

As well as creating novel value chains, technology is also transforming many traditional ones. Industrial value chains are increasingly decentralised and globalised. Firstly, digital technologies allow critical phases of production such as product design, engineering and manufacturing, to take place in different locations, enable supply chains to span across continents, and allow supervision of the international movement of production components, goods, workers and investments. Secondly, digital technology, internet and production are increasingly merged into one cyber-physical system covering manufacturing, servicing, customisation, and even energy management. This phenomenon is still at an early stage, but will be stronger in the future.

Job markets

Automation – either replacing humans with machines or using machines to perform previously impossible tasks – creates major disruptions on job markets. From 2013 to 2018, installations of industrial robots increased by 19 % per year. Europe is already the second largest market for robot workers, and half of the top 10 countries for robots per worker are EU Member States. Meanwhile, AI broadens the range of tasks that can be automated.

[5] A. Cozzolino, G. Verona, F.T. Rothermael, Unpacking the Disruption Process: New Technology, Business Models, and Incumbent Adaptation, Journal of Management Studies 55:7, 2018. See how the technology-empowered use of data creates strong competitive advantages for platforms in M. Szczepański, Is data the new oil? Competition issues in the digital economy, EPRS, European Parliament, 2020.

[6] G. Sordi Schiavi, A. Behr, Emerging technologies and new business models: a review on disruptive business models, Information and Management Review, 2018.

[7] See how the technology-empowered use of data creates strong competitive advantages for platforms in M. Szczepański, Is data the new oil? Competition issues in the digital economy, EPRS, European Parliament, 2020.

The impact of automation on unemployment can be fluid and nuanced. Job losses can be offset as the workforce adapts and new jobs are created. Higher productivity and lower prices can also increase salaries and consumer demand, boosting employment in other industries. Current disruptive technologies such as AI, big data or the internet of things (IoT) also create entirely new jobs and, by this logic, this wave of automation will have similar 'rebound' effects to previous waves. However, insufficient jobs may be created for displaced workers without appropriate skills. Education and training (which may positively or negatively influence the level of technical and digital preparedness of society) and the overall mix of sectors (receiving positive and negative spill over effects from automation) will play key roles in how the future plays out.[8]

Many future workers are likely to be increasingly dependent on atypical work contracts, and will need to retrain and reskill to keep up with the pace of technological change. This may be difficult and costly for many, particularly the most vulnerable to job losses. Technological disruption can also have uneven impacts on workers, depending on their skills and occupations. These effects may also vary across countries and regions. The rise of the gig economy already poses questions about workers' wellbeing and social protection, including pensions, insurance, and maternity leave among other things. Disruptive technologies might lead to job polarisation, as jobs at different skill levels are affected differently. Since technological change is skill-biased, it leads to a process in which the disruption predominantly benefits workers with higher skills. In parallel, those employed by the undisputed beneficiaries of technological disruption are enjoying better employment quality and rewards than those in sectors which struggle with keeping up with the digitalisation. Left unmitigated, the skills-bias and the strong concentration of profits and financial means could exacerbate existing income and wealth inequalities. However, the undesirable effects could be mediated by some market forces such as labour costs and the profitability of investment in labour-replacing technologies. Consumer choices and social preferences regarding labour market regulations and ethical standards could also play a role, as well as institutional norms and regulations and the role of trade unions.[9]

Covid-19 and employment

The most severe impact of the Covid-19 crisis is likely to concentrate on the already most vulnerable segments of the working population. Many lower-income workers cannot do their work from home, but at the same time are not allowed to return to work. This also applies to those working in gig economy. While lockdown measures have increased our reliance on some of them, such as delivery couriers, others experienced an abrupt end to demand for their services and far weaker social protection than other employees. Furthermore, if individuals in the first group fall sick in the course of their work or need to quarantine, they rarely receive sick pay. The crisis has therefore confirmed the vulnerability of platform workers due to inadequate social protection. A situation the EU had already highlighted before the crisis.

The pandemic has also led to an unprecedented 'experiment', as working from home becomes the 'new normal' for many, raising questions about work-life balance and data security. While the longer-term effects are still unknown, it seems likely that teleworking will be more widely used from now.

[8] See for example D. Kleinert, E. Fernández-Macías, J-I. Antón, Don't blame it on the machines: Robots and employment in Europe, CEPR Policy Portal, 2020 and B. Vermeulen, J. Kesselhut, A. Pyka, P.P. Saviotti, The Impact of Automation on Employment: Just the Usual Structural Change?, Sustainability, MDPI, Open Access Journal, 2018.

[9] OECD, Employment Outlook 2019: The future of work, 2019.

3. Disrupting defence

Having an edge in technological innovation and industrial ability is generally associated with an international leadership position.[10] While the EU has just begun to speak of technological sovereignty, the United States of America is ever more outspoken about maintaining military supremacy, as is China about achieving military modernisation. Intelligent systems are disrupting defence as thoroughly as communications systems did in the past. As technological superiority once again becomes entangled in geopolitics, this section illustrates how innovation disrupts the full spectrum of defence, and is structured around the DOTMLPF-I concept: doctrine, organisation, training, material, leadership, personnel, facilities and interoperability.[11]

Doctrine: Automation meets strategy

Military strategy and doctrine formulation are increasingly disrupted by AI-enabled technologies, which speed up automation systems and processes. Intelligent systems are already used to inform strategists through long-term forecasting and rapid analyses. The '*deus ex machina*' concept – whereby conflict could be ended through unmatched and highly destructive technological superiority – is a perennial dilemma in defence innovation. Just like the belligerents' search for technological breakthroughs in the Second World War culminated with the atomic bomb, present and future strategy-making has to undertake even more complex risk assessments with regards to developments such as hypersonic weapons.[10] Deeper reflections about the role of technological innovation in global power projection are increasingly required when designing strategic priorities and, particularly, red lines.[12] This includes accounting for possible asymmetries in accessing key and dual-use technologies.[13] Strategists have the double task of adapting to the disruptions in their own work while reflecting about the impact on and future role of new technologies in policy objectives.

Organisation: Modern bureaucracies

Defence institutions are built on precise structures and strict chains of command, which could inhibit innovation. Institutions with flexible structures, reduced red tape and narrower hierarchies could facilitate doctrine to respond to disruptive innovation. Institutions themselves are already experiencing disruptions to their administration, communications, recruitment, financial management and security as a result of AI-enabled predictive technologies. While this trend could lead to increased efficiency and speed, it could also lead to a reshaping of the military workforce. Science fiction novel *Drone State* imagined this in the form of an AI supercomputer threatening the jobs of human police intelligence analysts in a futuristic Europol.

Training: Virtual battlefields

Military training and exercises already use technologies to better simulate theatres of operation, and to train for scenarios in which technologies are deployed offensively by adversaries. Virtual and augmented reality simulations, for example, provide a safer, cheaper and less environmentally damaging alternative to traditional training in the field. Uniformed officers and policy planners could increasingly benefit from more realistic learning experiences through AI-enabled training platforms which 'accurately mimic the actions of individual adversaries' but also adapt to different user responses.[14] New applications can also offer tailored learning experiences by adjusting

[10] R. Smith, The Utility of Force: *The Art of War in the Modern World*, Penguin Books, 2006.

[11] Initially used as DOTMLPF by the US military, the interoperability element was added by NATO.

[12] Red lines could include moral and ethical considerations, emphasising human-centric technological developments.

[13] F. Gaub, Global Trends to 2030, ESPAS Report, 2019.

[14] D. Fiott, G. Lindstrom, Artificial Intelligence: what implications for EU security and defence?, EUISS, December 2018.

teaching styles to a student's own progress and goals. In turn, personnel training also increasingly focuses on using, deploying, maintaining, repairing, and teaming up with smart applications.

Material: Smart weapons

From weapons systems to high-tech wearables, modern armies have higher demands for digital gear. Defence industries are prioritising the development of such equipment while investing in moonshot programmes to develop game-changing breakthrough technologies such as quantum computing.[15] This invites the question, is industry developing technologies to meet military demand, or is the military pressured to procure the latest technologies available on the market?[16] Defence institutions are increasingly compelled towards public-private partnerships to access new technologies, largely developed in the private sector.[17] Supply chain security and dependence on foreign sources for strategic equipment is already a politically sensitive topic, intensified by the Covid-19 crisis. Acquisition of dual-use technology, e.g. 3D printing, cognitive computing, hypersonic weapons, high-energy lasers, space technology and human enhancement biotechnology could be increasingly used as a bargaining chip in the competition between powers.

Leadership: Hypercommand for hyperwar

Dynamic and complex situations demand faster and better informed decision-making processes. Officers at all levels of command are empowered with technological support that is bound to disrupt traditional working methods. For example, AI-enabled analytical tools collect immense amounts of data from various sources, process it, and translate their findings into a format that human operators can make use of. Such tools can perform forecasting based on historical data analysis and generate live simulations of various crisis scenarios. As operational environments, whether physical terrains, cyberspace or outer space, are bound to become more dynamic and critical decisions might need to be made within fractions of a second,[18] human decision-making capabilities could be overwhelmed without support from automated advisers, which can quickly make sense of live sensors and imagery transmissions from a chaotic battlefield.

Military technologies endowed with advanced sensors, cameras and recording abilities, such as bee-sized drones or fully autonomous boats for example, can provide information superiority and strategic advantages for decision-makers as long as they are matched by proportionate analytical capabilities at headquarters. While some argue that intelligent machines can improve decision-making by providing a clearer and more objective view of conflict situations, others are concerned about the ethical aspects of decisions increasingly informed – or taken autonomously – by technologies.[19] This is further complicated by considering a possible nuclear aspect.

Personnel: Machine-assisted soldiers and soldier-assisted machines

Contemporary warfare demands new skills from armed forces. Just as automation affects civilian jobs, machines are poised to take over mechanical and repetitive roles in the military while empowering humans in strategic thinking and creative tasks. For example, the sheer quantity of data – including millions of hours of drone footage – is collected faster than human analysts can analyse it, so military personnel are increasingly required to supervise, check and assist intelligent systems in their processing of this data.[20] On the contrary, jobs demanding emotional intelligence

[15] P. Guest, The subatomic age: Asia's quantum computing arms race, Nikkei, 2020.

[16] While technologies such as the internet or nuclear power were initially developed for military purposes and only later adapted for civilian uses, new technologies are experiencing a reversal of this trend.

[17] Famous examples include Project Maven, a partnership between Google and the US Department of Defense, and the cloud services contract (Joint Enterprise Defense Infrastructure) between the latter and Microsoft.

[18] Artificial Intelligence in Land Forces, German Bundeswehr, 2019.

[19] M. Horowitz, The promise and peril of military applications of AI, Bulletin of the Atomic Scientists, 2018.

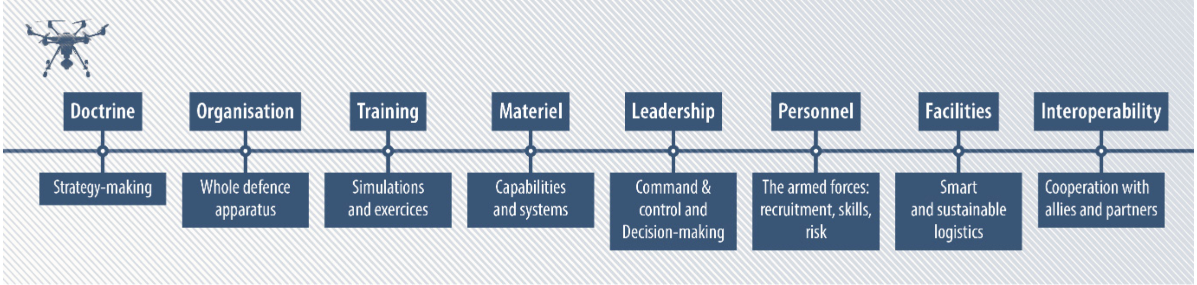
[20] P. Scharre, Killer Apps, *Foreign Affairs*, 2019.

and critical thinking, such as psychotherapy, might increase demand for humans as 'the force' digitalises.[21] Drones and robots are already deployed alongside soldiers to reduce human risk exposure with AI-powered (semi-) autonomous partners providing protection, such as the Battlefield Extraction Assist Robot, which is meant to extract soldiers from the battlefield. Analytical technologies can further reduce risk as they can identify the smallest pixel change in images that could indicate hidden objects and communicate them in real time to soldiers in the field. In some cases, personnel can avoid physical deployment altogether, for example by operating remote-controlled drones or demining robots. The benefits of these disruptions come with risks, in particular their vulnerability to hacking, or jamming of communication systems. Even without the ability to decrypt signals, detecting their presence can serve as intelligence for adversaries.

Facilities: Intelligent logistics

Logistics and planning have always been key factors in successful defence, as illustrated by Napoleon's defeat in Russia or the Battle of the Bulge at the end of the Second World War. Logistics have historically been tightly knit with transport innovations that disrupt the conduct of warfare. These range from the use of horses as a main means of military transport and high-end warfare, to steam ships and rail, up to contemporary technologies such as (semi) autonomous transport systems. Predictive maintenance technologies are increasingly deployed, using connected sensors to anticipate when components in systems such as aircraft or engines will become defective.[14] AI-enabled analyses can also be used to identify safe locations (e.g. for landing, evacuation and supply) and to calculate supply needs and inventory. These technologies cumulate into benefits for human, financial and natural resources while reducing the element of surprise. However, as the connectivity of critical infrastructure increases, so do vulnerabilities to cyber-attacks targeting communication channels. For example, fast progress on AI-enabled software trained to automatically defend against cyber-attacks and even retaliate is already impacting the way cyber warfare is led.

Figure 1 – Defence disruptions by domain


Doctrine
Strategy-making
Organisation
Whole defence apparatus
Training
Simulations and exercices
Materiel
Capabilities and systems
Leadership
Command & control and Decision-making
Personnel
The armed forces: recruitment, skills, risk
Facilities
Smart and sustainable logistics
Interoperability
Cooperation with allies and partners

Source: EPRS.

Interoperability: Can technological superiority be shared?

Interoperability is challenged by the emergence and adoption of new technologies by allies. As different forces digitalise and innovate at different speeds in a race for technological superiority, it can become more difficult to operate their technologies together. Gaps between more and less advanced allies could emerge and eventually impair military action. Different cyber capabilities and visions of cyberwarfare are already visible and there is a risk that incompatible systems could mutually classify each other as hostile, despite their human masters' formal alliances.[22]

[21] J. Perkins, More than Killer robots, Modern War Institute, 2019.

[22] M. Smeets, Cyber Command's Strategy Risks Friction With Allies, Lawfare, 2019.

4. Disrupting democratic debates

Disintermediators, disinformants and our infosphere

Our information sphere is constantly evolving, and regularly disrupted and shaped by technological innovations: a 3 000-year old clay tablet depicts scenes of information designed to trick its readers; the invention of the printing press in 1450 disrupted and revolutionised the dissemination of information. The advent of social media has changed our online lives, in particular since Facebook entered the scene in 2004, followed by YouTube in 2005 and Twitter in 2006. Back then, many embraced social media as a blessing for freedom of speech: anyone with internet access and a smartphone could and still can have a say, without gatekeepers such as traditional media. A decade later, however, the flipsides began to curb this initial enthusiasm. The big online platforms have absorbed most of the advertising revenues that used to fund traditional media, weakening the latter's role and making many people more reliant on social media for news; roughly two-thirds of US adults and over half of Europeans get their news on social media. At the same time, online disinformation (deliberately deceptive information) became a key component in the Kremlin's ongoing hybrid war against Ukraine since 2014.The Brexit referendum in the United Kingdom, the 2016 presidential election in the United States and a number of other elections have brought new realisations about the effect of disintermediation on our public space for debate.[23] Violence sparked by false information spread via social media has cost countless lives and caused severe problems for many societies.[24] The mounting concern over digital disruptions of our infosphere has been accelerated by the infodemic – an overabundance of both accurate and false information – accompanying the ongoing Covid-19 pandemic.

The attention-fuelled 'junk cycle'

For social media platforms, user attention is crucial for advertising revenues: time is money. In other words, the more time users spend on online platforms, the more money these companies earn. Search engines and social media such as Google, YouTube, Facebook and Twitter are using algorithms – automated predictions of what users are interested in seeing – to spark engagement and maximise revenues. Based on users' habits and their history of clicks, shares and likes, algorithms filter and prioritise the content that users receive. As users tend to engage more with content that sparks an emotional reaction and/or confirms already existing biases, this type of content is prioritised.[25] On a social scale, this can amplify divisions, prevent the correction of clearly false information and contribute to political and societal polarisation. When data from 87 million Facebook users (including 2.7 million EU citizens) were improperly shared with the political consultancy company Cambridge Analytica, predictions about sexual orientation, race and intelligence were used to microtarget and mobilise voters in the US Presidential election and the UK referendum on EU membership. As calls mount for more algorithmic accountability and transparency, users and digital journalists compete to post potentially viral content first, in a continued quest for likes and shares that contribute to the 'junk cycle'.[26]

[23] H. Berghei, Weaponizing Twitter litter: Abuse-forming networks and social media, Computer, 2018.

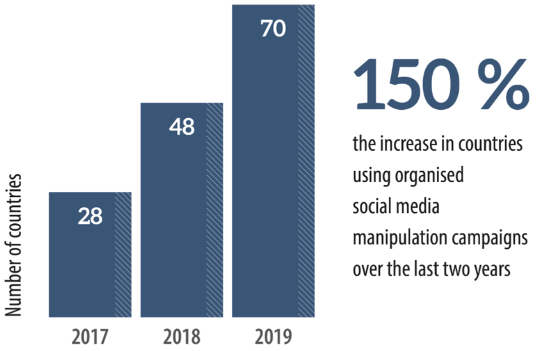
[24] Hate speech about the Rohingya Muslim minority in Myanmar, leading to ethnic cleansing, was spread via Facebook. In India, a series of mob lynchings were linked to messages circulating on WhatsApp.

[25] G. L. Ciampaglia, F. Menczer, Biases make people vulnerable to misinformation spread by social media, The Conversation, June 2018.

[26] R. Somaiya (2019). The Junk Cycle, Columbia Journalism Review.

Growing evidence of online disinformation across the world

Figure 2 – Increase in organised social media manipulation 2017-2019



Data source: Oxford Internet Institute.

Just as the 'clickbait' industry benefits financially from catching people's attention, an increasing number of state actors benefit politically from the disintermediated infosphere by using computational propaganda techniques. These include AI-enabled illegal harvesting of data to profile and microtarget users, algorithms and automated 'bot' accounts,[27] as well as human curation by cyber troops or 'trolls' to 'purposefully distribute misleading information over social media networks'.[28] Such activities can feed into coordinated campaigns of foreign state and non-state agents to influence democratic processes and political decision-making.[29] In this context, disinformation turns one of democracy's greatest assets — free and open debate — into a vulnerability. This affects most people across the world: Almost 60 % of the global population are active internet users.[30]

A 2019 Oxford Internet Institute (OII) study[31] found increasing social media manipulation by governments and political parties across the world. According to the OII, Facebook and Twitter found evidence of seven states – China, India, Iran, Pakistan, Russia, Saudi Arabia and Venezuela – engaging in information operations to influence foreign audiences in 2019, including via considerable cyber troop numbers. However, 10 times as many countries use such techniques to influence domestic audiences: In 2019, there was evidence of organised social media manipulation in 70 countries, compared to 48 countries in 2018, and 28 counties in 2017.[32] According to the OII, 26 countries used computational propaganda domestically to control information, suppress fundamental human rights, discredit political opponents and overpower dissent.

Coronavirus crises accelerating change

Crises, including pandemics, can exacerbate existing trends and tension. When emotions run high, online rumours spread 'faster and more easily' than a virus.[33] Since news about the new Covid-19 outbreak – initially suppressed by the Chinese Communist Party – was officially confirmed by the World Health Organization (WHO) China Country Office on 31 December 2019, the virus has provided fertile breeding ground for misinformation, disinformation and conspiracy theories across the world. Some of this false information is deployed as an attempt to sell fake cures or treatments; others use manipulated, attention-grabbing information to boost online traffic and increase advertising revenue. In combination with failure to communicate transparently, this undermines

[27] Wilson, D.G. The Ethics of Automated Behavioral Microtargeting, AI matters, vol. 3, issue 3, 2017.

[28] Woolley, S.C. and P.N. Howard, Computational Propaganda Worldwide, Oxford University, 2017.

[29] J. Pamment et al, Countering Information Influence Activities: The State of the Art, July 2018.

[30] https://www.statista.com/statistics/617136/digital-population-worldwide/

[31] Bradshaw, S. and P.N. Howard, The Global Disinformation Order 2019, Oxford Internet Institute, 2019.

[32] Here, at least one political party/government agency was using social media to influence public opinion.

[33] WHO Director-General speech, Munich Security Conference, 15 February 2020.

trust in official health advice, governments, global health organisations and scientists, that is, the very institutions that responsible for organising a global response to the pandemic.[34]

Due to the high demand for trustworthy information about the outbreak, the WHO has been working closely with tech companies to make trustworthy content visible. At the same time, however, the spread of conspiracy theories by authoritarian states such as China and Russia, including via social media, has raised concern that a combination of disinformation and heavily promoted health diplomacy, echoed by local proxies in Europe, could pave the way for wider influence after the crisis. Moreover, by undermining local advertising overnight, the pandemic has accelerated existing trends towards reducing print days, cutting staff and closing down the offices of local news media.[35]

How to disrupt the disruptions? The EU response

In recent years, the EU has stepped up efforts to fight disinformation. In 2015, the European External Action Service (EEAS) East StratCom task force was launched to counter ongoing disinformation campaigns by the Kremlin. The European Parliament has consistently supported the team, including via its budgetary powers. Additional Task Forces, focusing on the southern neighbourhood and the Western Balkans, respectively, were created in 2017. The European Commission's April 2018 communication 'Tackling online disinformation: a European approach' was built upon with the creation of a voluntary code of practice where major online platforms and advertisers agreed to combat disinformation, An action plan against disinformation, also helped to strengthen the EU's capability to counter disinformation ahead of the European elections, with initiatives such as the Rapid Alert System (RAS), set up in March 2019.[36] During the pandemic, and in response to the call of the members of the European Council and EU Foreign Affairs Ministers, as well as to the concerns of the European Parliament, the Commission and High Representative published a joint communication on 'Tackling Covid-19 disinformation – Getting the facts right' in June 2020, urging more coordinated action to address the risks for open societies.[37]

The ongoing reflection in the EU to boost EU rules and resilience, including by passing legislation to fight disinformation in the forthcoming digital services act, has intensified during the pandemic. The Commission aims to launch a European democracy action plan[38] in late 2020, to help improve the resilience of democracies and combat foreign interference in European elections. The strategy aims at countering disinformation and adapting to evolving threats and manipulations, as well as at supporting free and independent media. The action plan on human rights across the world envisages support for independent and pluralistic media, access to information and the fight against disinformation, as well as efforts to raise public awareness and stimulate public debate around actions to counter disinformation. The Covid-19 pandemic has shed new light on the dynamics[39] between the EU and major online platforms and advertisers, many of which teamed up with the WHO in February 2020 to combat the spread of false information about Covid-19. While many of these companies have made more efficient efforts to tackle the coronavirus infodemic, compared to their seeming reluctance to counter political disinformation (perhaps partly because they had verified, authoritative information from the WHO and national authorities to promote), the pandemic has highlighted the responsibility of these companies and the room for improvement.

[34] E. O'Reilly, Coronavirus "infodemic" threatens world's health institutions, Axios, 2020.

[35] K. Doctor, Newsonomics: Tomorrow's life-or-death decisions for newspapers are suddenly today's, thanks to coronavirus, NiemanLab, 2020.

[36] See Legislative Train Schedule: Online platforms, the digital single market and disinformation, European Parliament.

[37] N. Bentzen, The EU's response to the coronavirus 'infodemic', EPRS, European Parliament, June 2020.

[38] See Legislative Train Schedule: A new push for European democracy. European Parliament.

[39] Social media companies open new front in fight with EU, *Financial Times*, 2 April 2020.

5. Disrupting social norms, values and identities

Social values, norms and identities are cultural products that shape what we find important (values), what behaviours we consider appropriate (norms), and how we make sense of ourselves and our relationship to others (identities). They shape each other and can vary substantially between individuals and over their lifetimes. However, they are best understood on a broader social scale. Disruption in this context could be described as relatively fast or dramatic changes to the dominant norms, values and identities in a community or society. It may be provoked by wider phenomena such as natural disasters, cultural or civic movements, economic transitions or, as we consider here, technological developments. Despite the potentially negative connotations of the word 'disruption', change to social values, norms and identities is a constant fact. Since our norms guide what we see as 'normal' and our values provide a benchmark for determining what is 'good', it is difficult to objectively evaluate any changes to them. It is also difficult to isolate technological disruption from other forms of disruption. For example, more widespread use of innovative video conferencing tools as the primary means of conducting social, professional and familial relationships may appear to be a technological trend, but the real driver of increased use in 2020 is probably not innovation itself, but physical distancing rules established in response to the Covid-19 pandemic. Nonetheless, this section provides illustrative examples of how technology development can disrupt values, norms and identities.

Values: What is happening to privacy?

Social values are principles that are considered important by a society. Several values are articulated in EU law as inviolable fundamental rights. However, values themselves are not natural or objective laws, but dynamic and subjective concepts. They change over time and between cultures in response to their context. While this change can be resisted, imposing values beyond their 'use by date' can lead to friction.

Privacy is valued so much by Europeans that it is protected as a fundamental right to 'respect for private and family life, home and communications' and by specific regulations such as the General Data Protection Regulation (GDPR). There is a broad and long-standing sentiment that our privacy should be protected from various forms of intrusion. Nonetheless, the concept of privacy is neither fixed nor objective, but differs across cultures, over generations, and even during our lifetimes.[40] The concept of privacy in terms of personal spaces was barely recognisable until the 19th century. Even the wealthiest people that could afford large homes would still receive guests and conduct business in the bedroom. Today, it is normal for bedrooms to protect privacy not only from visitors but also from our own family. The concept of protecting the privacy of information is a little older. Eavesdropping and reading other's letters were punishable offences as far back as the 14th century.

While the long-term trend may be towards greater value for private spaces and information, the last decades of technological development have provoked several disruptions to the concept of privacy, as well as its protection. European (and, to a greater extent, US) courts link the legal protection of privacy to the extent to which people expect it, and the extent to which this expectation is

[40] See J. Holvast, History of Privacy in: V. Matyáš, S. Fischer-Hübner, D. Cvrček and P. Švenda. (eds). The Future of Identity in the Information Society, Advances in Information and Communication Technology, vol. 298. Springer, Berlin, 2009.

considered reasonable.[41] This approach implies that, as citizens are exposed to intrusions of privacy and expect less of it, their legal entitlement to privacy is also eroded.

The digitalisation of contemporary life has gone hand-in-hand with changes to how many people value privacy. It becomes increasingly normal for people to share much more of their personal lives online. Even for those that do not do so, their basic web services are often provided by mediators in exchange for access to their data, enabling sophisticated analysis of their habits, preferences, ideas and movements. The younger generation of 'digital natives' that grew up with social media and smartphones have been described as fatalistically accepting their lack of privacy and engaging in dangerously open sharing practices. However, closer examination reveals a more complex situation as young people develop sophisticated hierarchies of online activities, for example maintaining a completely open public presence (designed for high visibility, or to feign aloof nonparticipation) alongside a fiercely guarded personal digital space (such as a secure folder) and several other profiles with a range of identities and sharing policies designed for engaging with specific communities in different ways.[42] In this light, the social value of privacy is surviving and, perhaps, thriving by adapting to its context.

Norms: How do we access information?

Social norms are understandings of appropriate conduct in a given context. Closely linked to social values, they guide and even govern what is considered normal, shaping how we behave and how we think others should behave. Since they are subjective and dynamic, changing norms are, in a sense, the norm. They are also regularly disrupted by technologies. For example, freezers and microwaves provoked radical changes in mundane household routines for the storage and preparation of food with profound effects on material consumption.[43]

The internet has provoked radical changes to our norms for accessing news. Until recently, most people read newspapers and tuned in to television and radio broadcasts. Gradually, people began accessing more news online, and increasingly via platforms that curate content for individuals. These changes in how individuals access information cumulate into social norms with profound structural effects. The norms of payment for news has shifted to a model driven by personalised advertisements, with implications for how news is produced – often in a shorter format with a greater degree of personalised targeting designed to provoke emotional reactions – and also how it is consumed, with more fragmented content via a range of platforms.

Coronavirus: Technology and social norms

The unfolding Covid-19 crisis is probably the disruption of a generation. However, the role of technology has principally been to mitigate its disruptive effects on social norms. Video conferencing and other internet technologies maintain communication channels, reducing the impact on our work and social lives. In some cases, they allow social distancing measures to be reduced to mere physical distancing. We might see some norms 'in the making', for example, in how we greet each other without any physical contact. Other norms might be used as partial solutions to the crisis, including our near constant use of smartphones which could provide data as a proxy for our location and relative distance from others. These temporary changes could end up being more permanent as, for example, digital interfaces increasingly replace physical contact in human interactions.

[41] Nouwt, S., B. de Vries and C. Prins (Eds) (2005) Reasonable Expectations of Privacy? - Eleven country reports on camera surveillance and workplace privacy. T.M.C. Asser Press.

[42] Benjamin, G. (2017) Privacy as a Cultural Phenomenon. Journal of Media Critiques 3(10).

[43] E. Shove, Comfort, Cleanliness and Convenience: The Social Organization of Normality, Oxford: Berg, 2003.

The effect of these changing norms has been vulnerability to disinformation as well as social and political polarisation.

Identities: How do we know where we come from?

Our identities are complex understandings of who we are, including our bodies and minds as well as our role and sense of belonging within our families, wider communities and societies. From human enhancement to online platforms for niche communities, several new technologies can shape and perhaps disrupt our identities. A particularly interesting example, DNA testing, seems to provide definitive objective answers to questions about our bodies, families, and ancestry. By analysing bodily materials, DNA tests compare genetic information to reveal similarities which have been used to identify health risks, blood relationships, or ancestral heritage.

Such DNA test results can provide apparently hard evidence of who people are and where they come from. For example, results might show an individual's ancestors originate 28 % from Finland, 15 % from Portugal, 11 % from Italy, etc. However, both the accuracy and meaning of these numbers are contested. The results reflect levels of genetic similarity with other people's DNA, who live in these places and whose DNA happens to be recorded in the same database. As such, the same DNA in different databases gives different results. Furthermore, historic and contemporary migration challenge the link between heritage and residence. In any case, 'Finnish' DNA would not in itself make someone Finnish, legally or culturally. The use of DNA tests to answer questions about our identities prioritises biological measurements over other elements such as our culture and lived experiences. The recent controversy surrounding Senator Elizabeth Warren's DNA highlighted that, sometimes, identity has much more to do with community participation than blood and ancestry.

When individuals take DNA tests, they might risk disruption to their identity as a member of a family. For example, many people have discovered that their siblings are actually half-siblings, or that they have more close relatives than they knew about, leading to difficult family conversations. This does not only affect the test-taker, as results can disrupt other people's identities without their consent. Commercial databases regularly reveal the identity of biological parents that donated sperm or whose children were adopted under the assumption of anonymity.[44]

Members of white supremacist communities have taken DNA tests and discovered evidence of 'non-white' ancestry which disrupted a key element of their identity and, in some cases, precluded them from further participation in their community.[45] While these groups may see greater significance in bloodlines than many others, the case highlights the worrying potential of DNA tests as a gatekeeper of access to communities, to benefits designed for specific groups and to access services such as insurance. There is also the potential for commercial and state surveillance, indeed, police forces have begun to use commercial DNA databases to identify suspects.[46]

[44] DNA tests have 'unearthed affairs, secret pregnancies, quietly buried incidents of rape and incest, and fertility doctors using their own sperm to inseminate patients'. S. Zhang, When a DNA Test Shatters Your Identity, The Atlantic, 2018.

[45] Interestingly, responses from their community included criticism of the meaning of tests, showing that – even for those particularly attached to bloodlines – DNA testing does not always have the final word on identity. A. Panofsky and J. Donovan, Genetic ancestry testing among white nationalists: From identity repair to citizen science, Social Studies of Science, 49(5), 653–681, 2019.

[46] Police have identified individual suspects from DNA traces by scanning databases containing commercial DNA samples for matches with distant relatives. See J. Kaiser, We will find you: DNA search used to nab Golden State Killer can home in on about 60% of white Americans, Science, October 2018.

6. Disrupting international relations

One might argue international politics disrupts technology as often as the other way around. The Second World War, for example, facilitated the development of nuclear weapons. Nevertheless, there are some interesting patterns to the interaction between technology and international affairs. Information and military technologies, discussed in previous sections, are clearly 'political', but the rapid invention or diffusion of all kinds of technology can affect international politics. For example, the appearance of porcelain in Europe from China in the 18th century led to fierce state competition between several European powers who wanted to reverse engineer the technology, their race for status and economic gain involving everything from imprisonments to espionage.[47]

Rapid technology innovation and diffusion has three key effects on the international political system:[48]

1. First, new technologies often affect the political, economic, social, military and technological contest between states, the international system's main actors.
2. Second, they are also changing the international system itself, introducing new norms, ideas, types of actor or areas of contest, and making old norms redundant.
3. Third, they can become identified as global risks by the international community.

Some general-purpose technologies such as nuclear and information technology can be found in all three categories. The following sections illustrate each of these effects, mainly with reference to the digital transformation that has triggered the biggest disruptions of the last 30 years, and will probably continue to do so in the decades to come.

Contest between states

Significant technological disruption can increase competition, even lead to rivalry, between states as seen during the Cold War space race between the USA and the Soviet Union.[49] Both nations invested in rapidly improving rocket technology, which had international ramifications including spin-off effects for the nuclear arms race and space militarisation. More general, massive science investments contributed to the next technological revolution: information technology.[50] The moon landing in 1969 was a political victory that tilted the balance in the Cold War towards the USA. Towards the end of this period of history, it helped to lessen superpower rivalry: The last Apollo module memorably docked in space with the Soviet Soyuz spacecraft, demonstrating a new will for cooperation.

Today, many disruptive technologies affect inter-state competition. Three of the most important are AI, fracking and 5G.

[47] M. LIebermann, 'Das weiße Gold', in: GEO Epoche No 67, S. 54-61, 2014.

[48] Many of these observations also apply to domestic politics. Technology also changes the political contest between political actors and between ruler and the ruled. It also changes the rules of the game and often resolving issues requires cooperation. In both the state and international relations context, technology is not an intruder, something from the outside, but one of many things developed by humankind for a purpose. Some researchers say it is an actor in its own right.

[49] P. Lowman, Our First Lunar Program: What did we get from Apollo?, Goddard Space Flight Center, NASA, September 2007.

[50] G. Navarria, How the Internet was born: A stuttered hello, The Conversation, October 2016.

The race for leadership in AI looks much like the space race. It promises to dramatically increase international status and political, economic, social, military and technological power. A further commonality is the symbolism of the race for states, and its framing as a contest of values between societies. In contrast to the space race, the AI race is co-driven by the private sector as a major source of knowledge and capital. The quest for paradigm-shifting advancement in AI could acquire a dynamic similar to the moon landing.

The improvement of hydraulic fracking caused the USA to become less energy dependant on foreign oil and therefore on oil producing allies. This has contributed to Saudi Arabia's recent aggressive stance on many foreign policy issues. Fracking has also affected the oil market, contributing to the recent disagreement between Saudi Arabia and Russia in the Organization of the Petroleum Exporting Countries (OPEC). With reduced incentives for involvement in the Middle East and North Africa, the USA might continue to scale back its involvement there, creating opportunities for other powers, large and small.

The new 5G telecommunication standard has been developed since at least 2013, with the EU and China setting common standards in 2015. What started as constructive international cooperation turned into a confrontation between China and the USA due to fears that the Chinese state will obtain access to critical data and systems. This seems likely to lead to two increasingly divided technological camps, and, possibly, a global economic and political schism.[51]

Changing the international sphere

There are many examples of technologies changing the norms, theories, type of actors or areas of competition in the international political arena.

Armed drones and use of AI contest basic norms such as the humanitarian law of armed conflicts by challenging both the current restrictions on lawful targeting and the notion of human control over weapon systems. With slow progress in negotiations, and both technologies becoming widespread, this problem is likely to continue.

Digital disruption has also infused political theory with some new ideas. First, Silicon Valley was a hotbed in the re-emergence of an anti-political modernism:[52] that is, the belief that technology, not politics, is the main way to improve society. However, many political actors perceive that this political naivety has helped to polarise politics, enable fringe groups to acquire power, increase the influence of antidemocratic forces, and aid the spread of mis- and disinformation. Second, the rise and recent decline in the notion that the internet and social media could create a fairer and more complete public sphere[53] that might one day complement representative democracy. Third, big data and AI provide fertile ground for political theorists and philosophers. Yuval Harari, for example, has outlined the emerging concept and ideology of 'Dataism', the belief that algorithms can answer our questions better than we can: 'Once that happens, humans will lose their authority, and humanist practices such as democratic elections will become as obsolete as rain dances and flint knives'.[54]

Communication technology disruptions such as satellite TV, the internet and social media helped actors that could tell a story onto the centre of the international political stage. This contributed to

[51] Eurasia Group, Eurasia Group White Paper: The Geopolitics of 5G, November 2018.

[52] M. O'Mara, The Church of Techno-Optimism, *The New York Times*, 28 September 2019

[53] C. Fuchs, Social media and the public sphere, in: TripleC: Communication, Capitalism & Critique, Open Access Journal for a Global Sustainable Information Society, 12(1), 2014, 57-101, 2014.

[54] Y. Harari 'Yuval Noah Harari on big data, Google and the end of free will', *Financial Times*, 26 August 2016, in: D. Réchard (Ed.) Global Trendometer 2018, EPRS, European Parliament, July 2018 (p. 24).

the decrease of state power, not only over domestic politics (the 'governance turn'), but also in international politics. Such powers have reappeared with some force in recent times, as states have learned to live and thrive within and outside this new media environment. Authoritarian regimes from Syria to Russia demonstrated that they can disrupt global media to their advantage while using their military superiority to win conflicts, even when the other side had the better story to tell. A return to absolute state power is unlikely, but not impossible. While new disruptive digital technologies such as blockchains will further diminish state power domestically and internationally, the future of AI is a big uncertainty in the medium term. It could boost the centralisation of power to states, companies or even single individuals with effects that make all opposing trends insignificant.

Cyberspace – the global digital technology environment – is the prime example of a new domain in which states and other actors compete. It has become the testing ground for new forms of espionage and sabotage, propaganda and disinformation (the spread of deliberately false information), and the spread of revolutions and counterrevolutions. Due to increasing international tensions, both cyberspace and outer space have grown in their importance as areas of 21st century international competition. Domains, however, are not neutral. They create new actors and power relations. Shoshana Zuboff has described how big tech companies gain enormous power by using knowledge as a weapon.[55] Domains also change the actors that compete in them. The EU, for example, is redefining itself as the vanguard against these tech companies; an 'ethical superpower' and protector. Cyberspace or outer space might develop to the extent that they transform the state-based international system.

Global risks

Technology has shown it can disrupt political actors to the point where there is a consensus developing to deal with it internationally. The key example of this is the complex set of international agreements that today regulate military and civilian nuclear power. As things stand, there are only a few examples of productive talks aimed at limiting the risks of digital technologies, and the future does not currently look any more promising. Due to the current geopolitical situation, international talks and negotiations to regulate AI and automation (esp. of weapon systems), cyber security and space weaponisation are stalling, while classic existing regimes covering nuclear and conventional disarmament are crumbling.

Gene modification[56] has improved radically, and become cheaper and easier through the CRISPR/Cas9 method. In 2017, a Chinese scientist broke ethical guidelines and laws to use CRISPR/Cas9 to produce the world's first gene-edited baby, highlighting the potential and danger of this new technology. International regimes are complicated by various heated national ethics debates and positions. The global vulnerability to the SARS-CoV-2 virus has surely highlighted the power of biological weapons to malign actors around the world.

Together, these experiences show that, unfortunately, actors are much quicker at profiting from a technologically disrupted international system than they are at coming together and fixing it.

[55] S. Zuboff, The age of surveillance capitalism, 2019.

[56] B. Ashok and J. Karsten, Is there a responsible way forward for gene editing?, Brookings Institution, October 2019.

7. Disrupting laws and regulations

This section focuses on how technological disruption challenges the enactment and implementation of laws and regulations. The current debate on EU rules in areas such as AI, IoT and financial technologies (FinTechs) has prompted reflection on the efficacy of current legal and regulatory frameworks and the exploration of new approaches to define and implement EU rules to govern emerging technologies.

Technological disruption and normative approach

The pace of technological innovation makes it harder to use traditional legal and regulatory mechanisms. Legislators and regulators face a range of challenges to govern emerging technologies: technology evolves faster than the law's ability to keep up (the 'pacing problem'); passing new rules adds to an increasingly large and complex body of laws and regulations (the 'volume of rules' problem); legislators face difficulties to properly categorise new technologies (the 'coordination' problem); and they lack of proper information about how those technologies are shaped (the 'knowledge' problem).[57] Additionally, in an online and dematerialised world, it is more difficult for law enforcement agencies to enforce the rules (the 'enforcement problem'), for instance with regard to copyright infringement and blockchain regulation. As a result, the Member States and the EU legislators' traditional normative approach needs to adapt.

One remarkable feature of the current normative approach in the high-tech sector is that the elaboration of legal norms is increasingly driven by cooperation mechanisms and less by authoritative mechanisms such as hard law. Traditional 'state-based regulation' (generally top-down 'hard-law' rules) are increasingly used with more informal governance mechanisms, based on a 'soft-law' approach driven by the cooperation between key actors in the ecosystems. As a result, the role of states has been shifting from a traditional *dirigiste* approach to a more inclusive approach, where private parties play an increasingly important role, for instance in the context of standardisation processes, self-regulation and co-regulation initiatives. The imposition of 'hard law' governance in the field of new technologies could decline and soft law governance becomes widely used in fields such as AI and IoT. EU level guidance on data processing in the fight against Covid-19 is a further example of how EU rules and their implementation should be quickly adapted or clarified through soft-law instruments.[58]

New legal concepts governing the legislators' normative work in the high-tech sector have been coined in the last decades. Legislators are increasingly required to set up legislation that is 'future-proof' and 'forward-looking', i.e. resistant to change and flexible enough to adapt to constantly evolving market structures and actors.[59] A flexible approach to rulemaking promotes innovation, requires lawmakers to adopt a proactive rather than a reactive stance and rests on a complex balance between flexibility and legal certainty.[60] In this respect, policy-makers are confronted with a dilemma to design 'technology-neutral' rules such as the GDPR, which are abstract enough to last and yet detailed enough to provide legal certainty. They also need to reconcile the need for a reliable

[57] For an overview see R. Hagemann, J. Huddleston Skees and A. Thierer, Soft law for hard problems: the governance of emerging technologies in an uncertain future, Colo. Tech. L.J., 2019.

[58] See EDPB, Twentieth plenary session of the European Data Protection Board - scope of upcoming guidance on data processing in the fight against COVID-19, 2019.

[59] See the Opinion of the European Economic and Social Committee on 'Future proof legislation', 2016.

[60] See S. Ranchordás and M. van 't Schip, Future-Proofing Legislation for the Digital Age, 2019. See also European Commission, EPSC, Towards an Innovation Principle endorsed by better regulation, 2016.

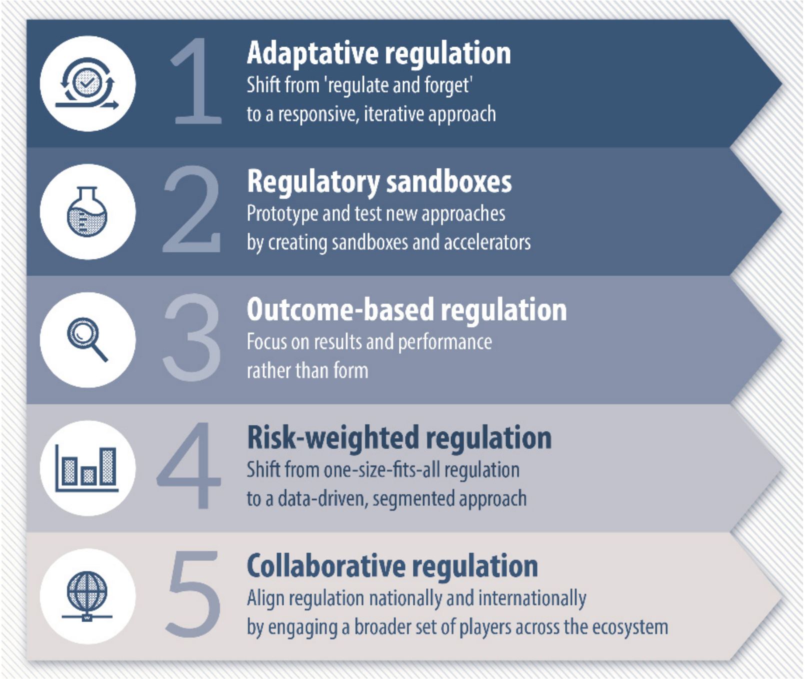
and secure legal environment that can foster innovation, without intervening prematurely which can hinder innovation.

Furthermore, policy-makers are increasingly required to engage with ethical and technical considerations before enacting rules in the high-tech sector. For instance, before setting new rules in the field of robotics it is necessary to reflect on the distinction between 'objects 'and 'humans' as (bio)robotic applications are increasingly built into human bodies.[61] Similar ethical questions are raised in the field of AI where legislators are increasingly called to set an ethical framework before legislating on technologies such as facial recognition.[62] Moreover, the complexity of new technologies require that legislators understand the technological constraints that affect the implementation of the rules. Topical examples include how automated content filtering can be imposed on large platforms[63] or how to regulate AI algorithms when their complexity make their decisions difficult to explain and justify (the 'black box' effect).[64]

Technological disruption and normative instruments

Given technological development and changing business models, it is necessary to have adaptive regulation in place.[65] To this end, the 'smart regulation' or 'responsive regulation' approach helps policy-makers to formulate more flexible, imaginative and innovative forms of policy instruments especially in the field of emerging technologies such as AI and Fintech.[66] While there is no agreed definition of smart regulation, a number of key principles can be identified (see Figure 3). Smart regulation is primarily about responding to the 'pacing problem', aiming at cyclical regulation rather than long-lasting rules that set fixed legal standards for decades. Smart regulation is also about responding to the coordination and knowledge problems by being more interactive and including more stakeholders including interest groups,

Figure 3 – Smart regulation



1 **Adaptative regulation**
Shift from 'regulate and forget'
to a responsive, iterative approach

2 **Regulatory sandboxes**
Prototype and test new approaches
by creating sandboxes and accelerators

3 **Outcome-based regulation**
Focus on results and performance
rather than form

4 **Risk-weighted regulation**
Shift from one-size-fits-all regulation
to a data-driven, segmented approach

5 **Collaborative regulation**
Align regulation nationally and internationally
by engaging a broader set of players across the ecosystem

Data source: Deloitte.

[61] See R. Leenesa, E. Palmerinib, B.-J. Koopsa, A. Bertolinib, P. Salvinic and F. Luciverod, Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues, Law, Innovation and Technology, 2017.

[62] See W. Wiewiórowski, Facial recognition: A solution in search of a problem?, 2019

[63] See E. Engstrom and N. Feamster, The Limit of Filtering, 2017.

[64] See Y. Bathaee, Artificial Intelligence Black box and the Failure of Intent and Causation, Harvard Journal of Law & Technology, 2018.

[65] See N. Singh, How can we regulate disruptive technologies? 2019.

[66] For an overview of the notion of 'smart regulation' see N. Gunningham and D. Sinclair, Designing Smart Regulation, 1999. See W. Eggers, M. Turley and P. Kishnani, The future of regulation Principles for regulating emerging technologies, 2018.

professional bodies, industry associations and quasi-regulators (such as certification bodies).[67] This approach enables legislators to get a more complete and diverse perspective on the issues, as well as potential solutions, while contributing to greater acceptance of regulatory interventions by the relevant stakeholders. Finally, smart regulation requires policy-makers to shift the focus from input to outcome-based regulation, leaving them more room to innovate.

Smart regulation requires a range of new normative instruments, i.e. a smart regulation toolbox. The ordinary EU legislative procedure, whereby it takes years to enact and transpose a text at national level, is not flexible enough. Other mechanisms may be more appropriate, including coordination of national regulators, executive agencies and the use of implementing and delegated acts.[68] Furthermore, smart regulation can be implemented through a broad range of instruments including traditional 'hard law' as well as 'soft-law' instruments such as notices, guidance, standardisation and certification processes, regulatory impact assessments, periodic evaluation, and sunset clauses, which enable legislators and regulators to constantly re-evaluate the effectiveness and reach of the various instruments.[69] Moreover, rather than going through the lengthy process of legislation, policy-makers could rely upon trial and error through 'sandboxing' approaches with rapid feedback and evaluation mechanisms (see box). In this context, a key issue for technology regulation is to balance the use of new flexible instruments – enabling private interests and ideas to drive the rulemaking process – while maintaining legislators' normative powers to safeguard the general interest.

Sandboxing refers to the use of controlled spaces for businesses to experiment, test and validate new products, services or business models under the close supervision of the regulatory authorities. Legal and regulatory requirements are relaxed to allow this experimentation while consumer risks are limited through specific safeguards. The approach can improve regulators' understanding of new technologies and EU regulatory sandboxes are already under consideration for AI,[70] FinTech,[71] and surveillance solutions in the context of the fight against the Covid-19 pandemic.[72] In the increasingly complex high-tech environment, sandboxing may become more widely used as a first step before the enactment of rules. For instance, in its European strategy for data[73] unveiled in February 2020, the European Commission proposes an approach that avoids overly detailed, heavy-handed ex-ante regulation for setting up a new EU framework for data access and use. The Commission opts instead for a more agile approach including regulatory sandboxes and experimentation. Against this background, EU policy-makers will have to further reflect on how best articulate sandboxing exercises and legislative initiatives.

[67] See N. Singh, How can we regulate disruptive technologies?, 2019.

[68] See Digital Europe: Next Steps A European Agenda for the Digital-9+, Lisbon Council, 2019.

[69] See R. Leenesa and others, Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues, Law, Innovation and Technology, 2017.

[70] See A. Renda, Artificial Intelligence Ethics, governance and policy challenges, Report of a CEPS Task Force, 2019.

[71] See W.-G. Ringe and C. Ruof, Keeping up with Innovation: Designing a European Sandbox for Fintech, ECMI Commentary No 58, January 2019.

[72] See A. Pierucci and J-P. Walter, Joint Statement on the right to data protection in the context of the COVID-19 pandemic, 2020. See European Commission, Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States, 15 April 2020.

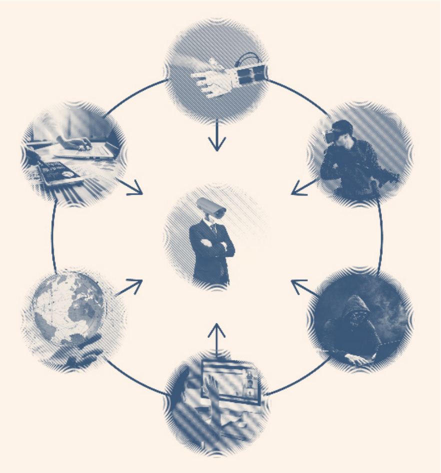
[73] See European Commission, A European strategy for data, COM(2020) 66 final.

8. Converging disruptions: The case of surveillance

The disruptions described so far are interwoven with each other as well as with other trends and disruptions. Together, they influence several other phenomena that are important in our everyday lives. One such example is surveillance, which is clearly shaped by all six of the domains of technological disruption described in the previous chapters, as well as by non-technological disruptions such as Covid-19 and wider social, political and economic trends. There are many forms of surveillance, but here we refer primarily to digital varieties for both state and commercial purposes.

Digital surveillance plays an increasingly important role in the **economic system**. As Bill Jordan[74] points out, digital devices have fast become an integral part of our domestic sphere. Thermostats, cars, credit cards, street cameras and mobile phones help harvest raw material that is fed into 'prediction' products that are traded in 'behavioural futures markets'. They can be used by corporations to not only predict our behaviour, but also to nudge, steer or modify our behaviour in an automated manner. Shoshana Zuboff argues that, instead of exploiting labour, this new 'surveillance capitalism' exploits our experience and our actions to control the future, based on secretly gathered data. Zuboff warns that surveillance capitalism represents an unequal and asymmetric model of knowledge: the companies know everything about us, whereas citizens, users, even policy-makers have limited or no insight into the data they have accumulated, or how actions are taken on the basis of this data.

Figure 4 – Disruptions can converge to shape other phenomena, such as surveillance



Reaching almost half of the world's population, information and communications technologies are the most pervasive in the world. Zuboff argues[75] that such practices were 'invented at Google, travelled to Facebook, engulfed Silicon Valley and have since spread through every economic sector'. In the infosphere, personalised political advertising – based on users' profiles, habits and history of clicks, shares and likes – is one of the most visible disruptions to **democratic debates**. As discussed in Chapter 3, the Facebook/Cambridge Analytica scandal was a wake-up call in this regard,[76] as data was gathered without the knowledge or consent of users and improperly used in a way that undermined democratic processes. Jordan argues that 'the continental European countries, and Germany in particular, are more alert to these dangers' than the USA (who benefits financially from this system, as many of the world's tech giants are based there). China's social credits system, as well as its large tech companies (notably Huawei) enable the Chinese Communist Party to gather information about debts or unpaid fines, facilitating authoritarian behavioural control.[74]

[74] B. Jordan, Authoritarianism and how to counter it, Palgrave Pivot, Cham, 2020.

[75] S. Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, London: Profile Books, 2019.

[76] D. Holloway, Explainer: what is surveillance capitalism and how does it shape our economy?, The Conversation, 2020.

Following the lead of the GDPR's global influence, the EU's responses to the threats of 'surveillance capitalism' – including anti-trust rules and the digital services act – could have a significant impact beyond Europe.

The rapid worldwide diffusion of social media and big data and the accompanying upsurge of surveillance has disrupted all three aspects of **international relations** discussed in Chapter 6, that is, contests between states, the international system itself, and global risks. First, questions about the legitimacy of surveillance is a major part of the bigger contest between the USA, China and the EU. China sees its surveillance as an integral part of its authoritarian system, not only to improve control but also to better react to the needs and sentiments of its population. The USA provides high safeguards against state surveillance of its citizens, but allows for nearly unfettered commercial and foreign security surveillance. The EU tends to combat surveillance as it regards the protection of personal data as a fundamental right. Second, regarding the international system itself, a state's power is increasingly determined by their relational influence or, as Florence Gaub puts it, their capacity 'to influence the policy decisions of other states'.[77] This is visible in all three powers' attempts to convince other states to adopt their view, including by actively exporting surveillance technology and legislation. Thirdly, surveillance could develop into a truly global risk. Some international cooperation exists, but efforts to curb commercial and state surveillance are in their infancy and short-term progress appears unlikely.

Coronavirus and surveillance technology

Another key disruption for surveillance is presented in the ongoing Covid-19 pandemic. Many look to technology for solutions to problems including the search for vaccines and treatments and means of breaking the cycles of transmission. Others, however, may see the crisis as an opportunity to embed further opportunities for data surveillance, either as a means of extending control over people (as employees or citizens), or as a means of generating profit through targeted products and services. Governments across the world have launched contact-tracing technology such as apps to help curb the spread of the virus. Although most are voluntary and do not collect or use any participants' location data, there is nonetheless growing unease over the potential impact of handing over personal data to private companies and governments on our individual and collective rights. Against this background, the EU has published guidelines* aiming to ensure that the mobile tracing and warning apps are interoperable across the EU, and that they are voluntary, transparent, temporary, cybersecure, using temporary and pseudonymised data. In this way, the pandemic has acted as not only an accelerator of risks, but also as an opportunity for the EU to step up and defend its citizen-centric values.

* See: Coronavirus: a common approach for safe and efficient mobile tracing apps across the EU, European Commission, May 2020

Revisiting Chapter 5 and the disruption of **social norms, values and identities**, many of the changes observed in this domain could foster wider and deeper surveillance. Regarding social norms, it is clear that our mundane habits and daily activities – such as reading news and conversing with others – have changed in ways that enable more detailed monitoring from commercial and state actors alike, creating ideal conditions for greater surveillance. Similarly, identities are for many people increasingly defined in machine readable terms such as DNA profiles and participation in online communities, rather than by culture and lived experience. Again, this change creates ideal opportunities for commercial surveillance as the data is used to target the promotion of products, services and ideas, and also for state surveillance as illustrated by the function creep of DNA databases as a new tool for law enforcement. As we become accustomed to

[77] See Global trends to 2030: Challenges and choices for Europe, ESPAS, 2019.

the presence of surveillance technologies, including the monitoring of our online activities, the way we value our own informational privacy is changing, sometimes in sophisticated ways. However, lower social expectations of privacy, particularly online and in in public spaces, can be accompanied by diminishing rights to privacy. This, again, creates opportunities for wider and deeper surveillance. It is worth highlighting that methods of state and commercial surveillance have been reimagined, redesigned and redeployed as new bottom-up forms of 'citizens' veillance' – such as 'watching the watchers', self-surveillance and environmental monitoring – that reflect citizens' values, promote their interests and protect their rights.[78]

Surveillance takes a slightly different form in the domain of **defence**, which includes information-gathering as well as state-supported espionage.[79] Both forms of surveillance have always been vital for defence as the right information is essential to the success of military operations and for national security. Information-gathering for defence includes intelligence, surveillance, target acquisition and reconnaissance with the aim of providing a comprehensive picture of one or more locations by using all the sensors and equipment available. Such surveillance is secretive by default, particularly as the 'watched' are likely to alter their behaviour if they are aware of the 'watcher', especially in a conflict situation. Nevertheless, privacy issues are central when asking 'what constitutes national security interest?' and determining the limits. All the more in a context in which technologies enable new dimensions of recording and storing capabilities, long endurance, increasing adaptability to different environments (from desert to dense urban spaces), and camouflage. Scholars have studied the theory of 'just war' as it applies to intelligence gathering[80] but, given the suspension of the usual standards of morality in wartime, the acceptability of surveillance in this context is not always clear.

Turning to the disruptive effects of technology in **laws and regulations**, the recent policy debate around the adoption of location-tracking[81] measures to fight the Covid-19 pandemic is one of many examples of how EU policy-makers are engaged with addressing surveillance technologies. So far, the EU institutions have used a soft law approach to foster harmonised deployment of technologies that abide by the GDPR and e-Privacy Directive. The European Commission asked[82] telecom firms to hand over anonymised mobile metadata in order to help analyse patterns of diffusion of the virus, and has adopted guidelines[83] for ensuring that new tools respect citizens' privacy. Furthermore, the EU will scrutinise[84] Google and Apple initiatives to develop contact-tracing technology to ensure it meets the bloc's privacy standards. While a quick response is vital to tackle the disease, democratic oversight is also crucial. The European Parliament stresses that, as co-legislator and as the only institution directly elected by universal suffrage, it must be included as an integral and essential part of all discussions on the EU's response to the crisis, and has called on the Commission and the Member States to publish the details related to the contact-tracing applications on mobile devices and allow for public scrutiny and full oversight.[85]

[78] See P. Boucher, S. Nascimento and M. Tallacchini, Emerging ICT for citizens' veillance: Theoretical and practical insights, Science and Engineering Ethics 24 (3) pp 821–830, 2018.

[79] While information-gathering can be executed without breaking laws, espionage involves uncovering secret information.

[80] J. Galliott, and W. Reed, Ethics and the Future of Spying, Technology, National Security and Intelligence Collection, Routledge, 2016.

[81] C. Dumbrava, Tracking mobile devices to fight coronavirus, EPRS, European Parliament, April 2020.

[82] S. Stolton, EU's Breton defends COVID-19 telecoms data acquisition plans, Euractiv, 2020.

[83] European Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection, 2020.

[84] N. Drozdiak, Google, Apple covid-19 tracking tech faces EU scrutiny, Bloomberg, 2020.

[85] See European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP)).

9. Concluding remarks

This analysis presents brief reviews of how the development and application of technology can disrupt several domains. In disrupting economies, it shows how technologies create (and destroy) certain business models, supply chains and patterns of employment. In disrupting defence, it demonstrates how innovations are transforming militaries from logistics and training to strategic decision-making and physical combat. In disrupting democratic debates, it shows how the business models of social media – which benefit from emotional, polarising content – have become a platform for disinformation that can increase rifts in society and undermine democratic processes, whereas facts and information rarely go viral. At the same time, however, these dynamics also affect trust in these companies, seemingly leading to more awareness among advertisers – who seek to protect their brands – about which platforms they associate themselves with.

In disrupting social norms, values and identities, our analysis shows how technology changes our most profound understanding of ourselves as well as the way we undertake the most mundane daily activities. In disrupting international relations, it illustrates how technology can adjust the global balance of power, and even transform the international system itself. In disrupting laws and regulations, it shows how the pace of innovation calls for a more flexible approach to policy-making, heralding the emergence of smart regulatory tools such as sandboxing and collaborative governance. A further chapter then explains how these various types of technological disruptions can come together, along with other disruptive forces such as Covid-19, to propel other phenomena such as extended state and commercial surveillance.

Sometimes, the same tensions of technology disruption play out at different scales in different domains. Technologies such as AI already generate substantial profits and functional benefits, and appear to have room to grow, but the distribution of benefits and risks as well as control over information are unevenly distributed. This applies to individuals using social media platforms to inform voting choices or purchasing decisions, as well as to world leaders and military commanders making strategic choices. For any actor operating at any scale, it is difficult to prepare for disruption because the future causes of failure or success cannot be seen in advance. In this context, it is also worth mentioning the force of human creativity and desire for a better world as shown, for example, in the reimagining of surveillance technologies as opportunities for participatory activities to build communities, empower citizens and deliver tangible health and environmental benefits.

The impact of technology on employment is often discussed in terms of quality and quantity of jobs, but another key element is how humans and machines can work together in a system to make good decisions while maintaining human autonomy. Again, this dilemma plays out beyond workplaces, across domains and scales as households, small business, large multinationals and nation states all face the same question. It is not clear where these tensions will lead us, but our path in this increasingly technology-dependent world will be decided to a large extent by the social, political, and economic choices we make now.

Contemporary disruptive technologies are prompting a shift towards a smart-type regulation (i.e. less top-down, less command and control, more participatory). As a result, EU policy-makers are increasingly using a range of normative instruments that rely less on the ordinary EU legislative procedure and more on flexible soft-law mechanisms such as guidelines and sandboxing approaches, which require greater cooperation with private actors. The European Parliament could align itself more closely with the elaboration of such mechanisms to ensure democratic oversight on measures that de facto set the legal and regulatory environment.

Technological development has long been considered as a disruptive force, provoking change at many levels, from the routine daily activities of individuals to dramatic competition between global superpowers. This analysis examines disruption caused by technologies in a series of key areas of politics, economics and society. It focuses on seven fields: the economic system, the military and defence, democratic debates and the 'infosphere', social norms, values and identities, international relations, and the legal and regulatory system. It also presents surveillance as an example of how technological disruption across these domains can converge to propel other phenomena. The key disruptive force of 2020 is non-technological, namely coronavirus. The pandemic is used here as an opportunity to examine how technological disruption interacts with other forms of disruption.

QA-04-20-446-EN-N

This is a publication of EPRS | European Parliamentary Research Service

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

PE 652.079
ISBN 978-92-846-6958-5
doi:10.2861/718464