Aspen Institute Germany

Aspen Transatlantic Workshop

„Present at the New Creation? Tech. Power. Democracy.”

September 27 – September 29, 2018

Essays

The Aspen Institute Germany thanks its generous supporters:

LOTTO STIFTUNG BERLIN

VOLKSWAGEN AKTIENGESELLSCHAFT

Estonian Embassy in Berlin

Deep Fakes and the Western Information Architecture

Christoph Abels

The rise of information technology in the 21st century dawned the beginning of the information age. The knowledge-based society that emerged as a result of rapid technological developments is accompanied by societal changes, impacting our everyday lives. Especially in the realms of information collection, distribution, and reception, technology unfolded massive behavioural influence: We can easily check recent news developments on our smartphones, share interesting articles on social media, and discuss world affairs in private WhatsApp groups, comment sections on Facebook or via Tweets. Although it was probably never easier to get information, technology also facilitated the distribution of disinformation. While we already struggle to cope with fake news and related propaganda schemes, with strong developments in the field of AI, we are facing a new threat that is even more potent in its power to undermine public trust and poison public debate: deep fakes.

What are deep fakes?

The camera never lies. An alleged truism, that still might be valid for the camera itself, but hardly for everything that happens after it has done the job. Today, technology provides lay users with powerful tools to alter videos and pictures – in a way that is much more advanced than forged imagery was ever before. This new kind of forgery is called ‘deep fakes’. The term refers to the use of deep learning tools to create fake videos and images in which existing material is altered to create misleading impressions about messengers and messages, i.e. that a certain person has said something he or she actually never said. An impressive example was made by director Jordan Peele, who created a video of former President Barack Obama insulting President Donald Trump[1]. As with disinformation, understood as false or misleading information intended to intentionally deceive and may cause harm to the public,[2] deep fakes can be used to impair democratic as well as policy-making processes. An important difference is that phenomena like fake news mostly do not have the persuasive impact of actual videos or audio material. Primarily, because people are used to ‘trust their eyes’ – and most people are probably unaware of a large number of biases that make eyesight a less trustworthy companion, just think of Fata Morganas or Rubin’s vase. But there is also at least some psychological evidence, showing that easy messages are more likely to persuade people using a video than using merely text-based communication.[3]

[1] Romano, A. (2018). Jordan Peele’s simulated Obama PSA is a double-edged warning against fake news. *Vox*. Retrieved from https://www.vox.com/2018/4/18/17252410/jordan-peele-obama-deepfake-buzzfeed

[2] European Commission. (2018). *Tackling online disinformation: a European approach*. Retrieved from https://ec.europa.eu/digital-single-market/en/news/communication-tackling-online-disinformation-european-approach

[3] Chaiken, S. & Eagly, A. (1976). Communication modality as a determinant of message persuasiveness and message comprehensibility. *Journal of Personality and Social Psychology, 34*(4), 605-614.

Another problem arises with what I call second level deep fakes, where videos are altered in a way that make them appear to be genuine content, but include small flaws that allow the recipient to eventually identify them as forged. This identification is intentional and tries to deceive recipients in a way that is more subtle: Although thinking that a manipulation attempt was successfully detected, the manipulator’s false trail make the recipient to reject the message he or she just encountered. A method like this could be used to discredit factual statements, and further erode public trust.

Deep fakes and the Western information architecture

The Western information architecture consists of different informational environments, where people receive their daily information from. These environments can be traditional sources like news outlets, social media platforms as well as exchanges on an individual level. While traditional media outlets still play a significant role, more and more discussion about public affairs happens on platforms and websites like Facebook, Twitter and Reddit. Beyond that, an increasing number of people use social media as a source for news.[4] Societies also strongly rely on social media as a forum for public debate. As a forum to discuss ideas, reflect on own attitudes towards societal affairs as well as a basis for informed decisions.

The 2016 U.S. presidential election has shown that social media with its unfiltered communication flow can be weaponized to make individuals a target for information operations. Their ability to customize messages and distribute information on a large scale make social media a useful tool for hostile actors. Especially since the users themselves can be utilized to spread deceptive messages, intended to further the propagandist’s agenda. Cases where hostile actors tried to exploit social media’s communication potential are legion. The 2016 presidential election is only one particularly prominent case. Deep fakes might dwarf these cases in their ability to harm democratic processes by exploiting social media in the same way other disinformation does but with a much more potent payload that influences people more easily and persistently. Naturally, the Western information architecture is much more vulnerable towards these operations than states that lack the West’s commitment to democracy and freedom. With its Great Firewall, China, for example, is arguably more effective in its attempt to counter disinformation campaigns. Its citizens, however, pay a huge price in form of large-scale censorship and a highly curtailed freedom of expression.

What should be done

Since deep fakes will ultimately address the individual, it is crucial to harden this line of defence. That means, educating people about the technical possibilities to alter videos and pictures and help them to develop a sophisticated media literacy. An individual’s basic understanding of technology and a critical attitude towards sources will be the best and eventually last protection against deep fakes. Beyond that,

[4] Shearer, E., & Gottfried, J. (2017). News Use Across Social Media Platforms 2017. *Pew Research Center*. Retrieved from http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/

research that tries to identify forged content needs to be strengthened, since an eventually automated identification will enable social media platforms to delete deep fakes quickly or even before they are uploaded. Although identifying these fakes is complex, there is already some progress of forensic experts from DARPA's programme on Media Forensics (MediFor).[5] However, other countries need to strengthen their research programmes as well. Germany's Agency for Innovation in Cybersecurity, which was recently announced, is another initiative that aims at enhancing the country's defence capabilities. It is unclear, however, whether the agency, with its comparatively small budget of 200m Euro over the next five years,[6] will actually contribute to the fight against deep fakes and disinformation campaigns. A transnational agency that fosters international research cooperation would be a more effective solution, since these global problems need to be addressed on an international level. Accordingly, President Macron's suggestion for a 'European DARPA' should not have been dismissed that easily[7]. We need to gain the upper-hand in this technological arms race that will test our resilience over the next years. Probably, the worst is yet to come.

[5] Defense Advanced Research Project Agency. (2018). Media Forensics. Retrieved from https://www.darpa.mil/program/media-forensics

[6] Delcker, J. (2018). Germany to launch US-style agency to develop cyberdefense. *Politico*. Retrieved from https://www.politico.eu/article/germany-to-launch-darpa-style-agency-to-develop-cyber-defense/

[7] Macron, E. (2017). *Sorbonne speech*. Retrieved from http://international.blogs.ouest-france.fr/archive/2017/09/29/macron-sorbonne-verbatim-europe-18583.html

Reflections on Technological Change and Democracy in Advance of the Aspen Institute Seminar

Daniel Baer

While the consequences of technological change on our economy—in terms of the way that automation and AI will ultimately transform production—may ultimately be more significant than the ways in which technological change has affected and shaped our politics, I am, for now, more optimistic about the former than the latter.

Panels and conferences about the “future of work” are ubiquitous today, and most of them are framed around some prediction about the elimination of some enormous share of present-day jobs in the coming decades. While I don’t deny the scale of likely change, its unpredictability, or its consequences for large numbers of individuals, in some sense “’twas ever thus.” We have heard these predictions before—even as recently as a generation ago when the prediction was that computers were going to render all those who used to be responsible for analog / manual recordkeeping irrelevant. At each moment of technological change, there have always been predictions of mass unemployment, of economic shifts that mankind will be unable to cope with. These predictions have never before proven anything other than the fact that we reliably fail to imagine the way that we will adapt and the possibilities that new technologies will open for material improvements in human lives.

In a way, there is reason to be hopeful about the sphere of politics, too. After all, in America, there was a period around the end of the 19th century and beginning of the 20th when populism was on the rise, tabloid newspapers provided the medium for yellow journalism, and economic transformations wrought grievances in the public that fermented into a foul brew. But people figured it out—people learned about the variable trustworthiness of news sources, they learned about the problem of political charlatans and showmen, and, especially after the Great Depression arrived, high politics seemed to have recovered its normalcy in America, just as it was degrading in Italy, Germany, and elsewhere in Europe.

And perhaps we’ll emerge from our present predicament too. Digitalization has revolutionized one of the functions of publishing—distribution—but we haven’t yet figured out the way to revolutionize and replace the other function: being a mark of quality. But maybe we will, and maybe citizens, having learned the lesson of voting based on lies, and newly able to discern which voices deserve trust, and which do not, will restore normalcy to politics in the world’s democracies.

And perhaps the convulsions of today’s politics in Europe and the U.S., when you set aside the treason and performance art of some leaders, is really just a crisis of political economy that will serve as a catalyst for a needed re-imagining of the relationship between government and the economy. And when that happens, our politics can shift again to a less nihilistic and revolutionary mode.

But perhaps not.

An uncomfortable thought for a liberal democrat is this: what if the main damage being done to our politics through the medium of technological change is not that foreign powers are manipulating the populace or that political figures are whipping up a frenzy on social media but rather that the ordinary citizen has shown that when she or he is empowered to speak in the public square, the instinct of tribalism and all that is anathema to liberalism, predominates? What if it’s not mainly Trump or anyone else who is the problem, but rather that liberalism has written its own destruction by empowering citizens who are unable to restrain themselves from being a mob (pre-)determined to undermine liberalism’s principles for the sake of grievance or material spoils? What if the leaders *are* following the people? What if it is the radical democratization of the discourse of politics that social media has effected—where everyone is is a pundit and elites no longer get to mediate our political choices—that has brought us to the brink of democracy’s downfall?

Reflecting this worry, in recent months, I have heard or seen a number of Americans joke that the Trump era—in which the selection of the President and his administration’s policies appears to have been driven by large numbers of citizens accepting falsehoods promulgated on social media—is a great argument for aristocracy. Much truth is said in jest, and perhaps, for some of the elite, the Trump era has given an excuse to voice an “I told you this would happen.” As in: “see, I told you we shouldn’t give the common folks too much power.”

But no liberal can really believe that that a benevolent aristocracy is an alternative that satisfies our theoretical and ethical commitments. And so the challenge in front of us is clear: how to sustain a democracy where the people are not merely a check on power, but empowered to drive the application of authority. Constitutions have long been seen as the bulwark against the tyranny of the majority—but now we need them, and the institutions they create, to take on more complex and subtler tasks.

Democratic Decline Aided by Tech Sector Lawlessness: Crafting a Transatlantic Solution

Constance Chucholowski

Democracy is in decline. In long-standing democracies, specifically those that founded and over the last 60 years contributed to preserving the post-war liberal world order, domestically manufactured sentiment and external meddling, have borne elected leaders who are disassembling the post-war order their predecessors built. Technology is both fueling anti-democratic sentiment and hastening anti-democratic leaders' efforts to usher in a new, go-it alone world order. A coordinated, transatlantic approach is necessary to curb technology companies' dominance and check their unintended power over civil liberties and information flows.

More than any traditional or cyber weapons system, democratic decline is perhaps the greatest security threat of the early 21st century. Elected world leaders' efforts to undermine human rights, limit civil liberties, and stifle free press, as well as reject internationally agreed treaties and abandon international behavioral norms has substantially weakened states' legitimacy. This, along with their rejection of international trade and security cooperation has disrupted the post-war liberal world order on which we have come to depend. In times of distinct anti-democratic or isolationist policies, the transatlantic axis served as the greatest guarantor of the post-war liberal order; that axis, too, is fractured.

Undoubtedly, democratically elected leaders are causing the democratic decline from within (Steven Levitsky and Daniel Ziblatt draw a chilling picture of past elected leaders' devolution into authoritarianism and warn of current elected leaders' identical paths in *How Democracies Die*). However, these leaders' emergence and continued exaltation was precipitated not only by fears of globalization, extreme income inequality, and shifting demographics, but the onset of big technology firms whose algorithms dictate what users see and when they see it. A small number of technology companies that control swathes of personal information, often against peoples' will, and at the behest of businesses desperate to squeeze profit margins, are aiding in the decline of democracy.

Less than ten years ago political scientists and development practitioners understood technology as the harbinger of freedom, allowing people to organize themselves, realize their voices, and rise up against dictators to secure democracy in their lands; they watched the Arab Spring unfold with cautious optimism. Today, it is clear technology firms' services are utilized almost as often to trample civil liberties, spread falsehoods, advantages for autocratic leaders, and disseminate hateful, divisive messages. Technology firms have quantified our daily lives and gained unprecedented control over our interactions with the "public sphere online." Consequently, technology firms have become bad actors' weapons of choice; they are the vehicle for disinformation and are utilized to weaponize people against their own states.

Behavior on the part of some tech giants is legal, yet lawless. For two-decades, policy-makers’ naivety and excitement about big tech’s net benefit overwhelmed any attempt at reigning in technology firms. Fast and loose digital policy, largely unbinding, has proven ineffective. Any effort by firms to check their own power or to monitor their services has ended in apologies and promises to do better, with an air of, “we are not responsible for bad actors and users have a choice.”

Officials and government bodies, mainly European, from liberal MEP Guy Verhofstadt to former Green MEP Jan Philipp Albrecht, and the UK Treasury Department to the German Kartell Authority have raised concerns about tech firms’ dominance and called for member state or EU-level action. Targeted approaches of stricter data privacy controls or revised anti-trust rules may address the concentration of power gained from collecting and processing citizens’ personal data, yet fail to limit the vehicle that bad actors will undoubtedly continue to weaponize to disperse false information, affecting democratic processes and upending democracies.

A robust solution to end the weaponization of technology companies rests on transatlantic cooperation. It is essential that the EU and the U.S. see big tech’s influence on their respective democracies for what it is: an unintended, uncontrollable consequence of amassing unchecked power. They must acknowledge the geopolitical impact of online firms with access to droves of information about citizens’ behavior, stored in the physical pockets and homes of users. Google, Amazon, Facebook, Apple (simply, but reluctantly put, GAFA, plus others) quantify our daily lives to make information useful for expanding their own businesses or servicing those who pay – whether for add space, data usage, or access.

The transatlantic axis has the opportunity to set a precedent for the standard a digital ecosystem on which or with which its citizens interact continuously must provide when it comes to security, data privacy, misinformation, manipulation, and competition. Carefully crafted and binding guidelines delineating algorithm transparency, data collection and usage, and usage codes of conduct must guide technology firms’ business practices not vice versa.

Such guidelines could take the form of an EU-U.S. framework, similar to the EU-U.S. Privacy Shield agreement – call it the EU-U.S. Platform Defense agreement – and be applicable in both directions. A first step by the EU and U.S. would ensure tech companies that will use their competitive advantage but do not abide by the code of conduct are excluded from serving EU or U.S. users.

In a recent piece entitled “Taming the Tech Monster,” MEP Guy Verhofstadt advocated using a blockchain approach to limit tech sector dominance. A more targeted blockchain-based system, whereby users source each other’s information in a transparent but anonymous way before it is dispersed widely based on a firm’s algorithm, would be an ideal filter tool for companies to comply with a “Platform Defense” agreement.

Ultimately, policy-makers must weigh the impact of a regulatory framework for reigning in technology companies whose success rests on the volume of data they obtain from users, whose power is conferred upon them unwittingly, by those users, and whose influence however circumstantial, is causing a decline in democracy, against the potential impact of doing nothing. A binding framework that demands transparency and flags false information, coordinated by both sides of the Atlantic would better preserve transatlantic geostrategic interests and would serve to foster greater competition in the technology space to foster continued growth in the digital economy.

Redistributing the Gains of Automation to Adapt to the Changing Nature of Manufacturing

Robert Fisher

Since President Trump assumed office, his administration has put a strong emphasis on foreign trade and pursued various policies aimed at shielding the U.S. manufacturing industry from foreign competition. In a 2016 study conducted by Pew Research Center, 57 percent of respondents (and 64 percent of Trump-voters) stated that trade policy is a very important factor for their voting decision.[1] Therefore, one would assume that competition through foreign trade is one of the key threats to the U.S. economy and its workforce. However, the recent trend towards protectionism is the outcome of a common misconception: The effect of offshoring on the U.S. economy and employment is rather marginal compared to the effect of automation.

As Michael Hicks and Srikant Devaraj of Ball State University in Indiana have shown in their 2015 publication *“The Myth and the Reality of Manufacturing in America“*, 87.9 percent of jobs lost in U.S. manufacturing between 2000 and 2010 can be attributed to productivity growth caused by increasing automation. While the Great Recession certainly caused output decline, the whole manufacturing sector still grew by 17.6 percent between 2006 and 2013 (2.2 percent per year on average). Therefore, the notion that U.S. manufacturing is in decline is factually incorrect. Simply put, U.S. manufacturing is in decent shape, it just doesn’t require as much manpower as it used to: Based on the average product of labor in manufacturing, Hicks and Devaraj have shown that between 1998 and 2013 productivity has grown throughout all sectors of manufacturing and by 32 percent on average.[2] This has lead to a polarization in employment that is often referred to as the hourglass economy: because middle-skill routine tasks are being automated, job opportunities are increasingly concentrated in high-skill, high wage and low skill, low wage jobs that are too abstract to be automated.[3] This process can be expected to intensify even more as more complex tasks will be automated in the near future.

Although this insight is focused on the United States in particular, the changing nature of manufacturing in industrialized societies transcends national borders. According to a study by McKinsey published in 2017, approximately 23 percent of total work

[1] Doherty, Carroll/Kiley, Jocelyn/Johnson, Bridget (2016): *“2016 Campaign: Strong Interest, Widespread Dissatisfaction“*, Pew Research Center, July 7th 2016, retrieved from: http://assets.pewresearch.org/wp- content/uploads/sites/ 5/2016/07/07-07-16-Voter-attitudes-release.pdf

[2] Hicks/Devaraj (2015): *“The Myth and Reality of Manufacturing in America“*, Ball State University, retrieved from: https://conexus.cberdata.org/files/MfgReality.pdf

[3] Autor, David (2010): *“The Polarization of Job Opportunities in the U.S. Labor Market“*, MIT Department of Economics, retrieved from: https://economics.mit.edu/files/5554

hours the United States and 24 percent in Germany could be automated between 2016 and 2030.[4]

Voters in western democracies increasingly perceive themselves as losers of globalization. While they have experienced a modest income growth since the emergence of globalization, it does not match the vast gains experienced by the middle class in asian emerging economies or by the global top one percent.[5] This development should be taken very seriously. If voters in the U.S. or the EU are under the impression that non- democracies like China are more effective at increasing their citizens income and wealth, it appears likely that they would start to grow dissatisfied with their liberal democratic governments and more open to populism and authoritarianism. Ultimately, the perceived legitimacy of a government also stems from its capability to provide sufficient conditions for its citizens to prosper.

To combat this development, both the cost and the gains of the technological revolution have to be distributed more equally. Rather than essentially harming employment in manufacturing and causing wage polarization, technology should be utilized as a source of investments that can provide opportunities and foster further innovation.

A fairly straightforward way of redistributing gains from automation would be the introduction of a robot-tax that companies would have to pay based on how much of their human workforce has been substituted through automation. The state would be reimbursed for the cost of automation — in the form of declining employment — and the proceeds could be reinvested into the welfare state as well as in measures that would make the economy and the workforce more adaptable to technological progress, most importantly education and (digital) infrastructure.

[4] Manyika et. al (2017): *“Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation“, McKinsey Global Institute,* retrieved from: https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/ Future%20of%20Organizations/ What%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/ MGI-Jobs-Lost-Jobs-Gained-Report-December-6-2017.ashx

[5] Milanovic, Branko (2016): *“Why the Global 1% and the Asian Middle Class Have Gained the Most from Globalization“*, Harvard Business Review, retrieved from: https://hbr.org/2016/05/why-the-global-1-and-the- asian-middle-class-have-gained-the-most-from-globalizat

Element AI for the Aspen Institute Workshop

Jean-François Gagné

Why We Need an Ethical Framework for AI

Ethics is a topic of conversation everywhere in the AI community. Many organizations are flaunting the ethical standards that they've created or revamped for their organizations trying to show that they are on the right side of history. But while it's clear to most people machines should follow ethical rules, I don't think we've done a good job of explaining the limitations of implementing those rules and why we still need to develop an ethical framework for machines. After all, don't we already have ethical frameworks to use? Yes, we do, but for the behavior of people in society, not machines automating our world. A productive conversation about regulating AI will depend on us figuring out how we even translate our stated values, whatever they may be, into a language that machines can understand.

How we currently shape our ethics

As people, we are born into a framework, a training system that starts with our parents teaching us their values and shaping the fundamental structures for our behavior. After only just a few years of development, we mix in another, broader set of instructions at school. There we are taught how to engage in social relationships, learning stories about what's right and wrong—starting out as simple nursery rhymes and evolving into detailed histories of the ongoing debate of Right vs. Wrong.

Eventually our values are more or less set in stone and we become full adults responsible for applying them, though the training is not yet done. Our businesses and institutions impose long-standing agreements for how those values are applied in Montreal, September 2018 day-to-day life. Through codified rules and objectives, we have a long list of explicit ethics of what one should do as a citizen. But, also embedded throughout society we have checks and balances on behaviour—subtle cues or outright whistleblowing—that enforce implicit ethics we have not yet formalized.

We have this gray area because some things are still up for debate. This debate includes the old familiar quagmire of our conflicting ethics when it comes to laying off workers, as well as previously unimagined situations like finding any criminal in China within 15 minutes using cutting-edge facial recognition technology. We don't always see how actions can accumulate harmfully or have carry-on effects that are bad for society. Thankfully, we have this robust system of checks and balances that keeps the debate going and acts as certain guardrails against runaway behavior as we figure it out—an extension of the role our parents and teachers. Our overall ethical framework as people is ultimately a dialogue; it is constantly evolving, updating with new generations of people and the continuing debate of Right vs. Wrong.

The void of an ethical framework for machines

When we create models of the world to automate tasks, we isolate those tasks from our framework of evolving values. We use AI to encode models of the world by training the machine on data. It’s very useful because it creates models we as people are not able to fully understand (otherwise we would have coded them ourselves). These models are becoming exponentially cheaper and more accurate, but also more complicated and less easy to understand as they continuously improve using feedback loops of more data. We cannot comprehend all the possibilities, and therefore cannot preemptively set all of the needed rules for its behavior.

This is OK, if we are able to set guardrails, but right now we don’t have those either. While the machine’s model of the world may capture the ethics from the moment that the training data was captured and the intent was set (consciously or unconsciously), it can run without any further dialogue and effectively operates in a void of any ethical framework. That is because the language of our ethical framework as people (social relationships, institutions, words) is not the same as the language the machine operates in (data).

If we want to apply the power of these tools to certain areas, we will need to introduce new levels of hygiene to our data, and even ethics as people. A hospital can perform incredible feats of healing, but requires a sterile environment to perform. We can perform great feats of societal cohesion with AI, but will need to practice good hygiene with our data, regularly scrubbing for bias or for behavior that will never do well to be automated. It is in engaging with the feedback loops of training data that we will be able to create levers to extend our ethical framework into the machine’s model.

We must extend our ethical dialogue as people to machines. It is by adding more and more of these touchpoints throughout the machines’ development and use that we can speak the same language and become sure they will respect our laws and values. This conversation is going to be very challenging with the machines, but also amongst ourselves to determine how to build the new framework. It is inevitably leading us to revisit our basic values and agreements as a society with automation.

Technology as the Emerging Hard Power Factor in the Global Power Dynamics Game

Esther Kern

Currently, a vast majority of the world’s hardware infrastructure is produced in China as well as many of the momentarily used smartphones. Furthermore, China increased its spending level towards research and development (R&D) in the area heavily in the last decade, while also investing in foreign markets (buzzword ‘Belt and Roads Initiative’). This gives China access to the knowledge and production of critical technologies, which has consequences economically, technologically and security-wise, but may also impact the current global order due to the influence technology will have in the future.

Right now the global order, its power dynamics and related international institutions are still grounded (to a certain degree at least) in the historical roots of World War II and the outcome of the Cold War. However, this might change due to the impact technology already has and will increasingly have in the future on the system. Here, the argument is that technology has the capability of making the shift of being a *soft power factor* to a *hard power factor* in the next decade. Technological development has always impacted society and political systems and the state of a country’s technology sector influenced the economic sector but at the moment it has the capability to evolve as a major strategic and powerful political instrument. This is due to the fact that the changes we are experiencing at the moment are from a different magnitude than previous technological advancements. For one thing, the speed of current developments is faster than ever (one prominent example – it took the telephone 75 years to reach 100 million users worldwide, while it took Facebook 4 1⁄2 years). Furthermore, this is deepened by the possibilities due to the advancement of digitization and the development of a global IT infrastructure. Secondly, the world today is more interconnected offline and online than it was ever before. Changing political situations or financial crises are issues that impact in many cases not only the concerned country but most often at least the region, if it does not have global consequences due to technological advancements. Thirdly, these advancements come with new security risks that are user- and cost-friendly for the attacking party, while the attacked party needs major resources and time defending itself. Fourthly, being the front runner or leader of technological advancements gives a country the capability to set the rules and standards at least for the given technological sector. Therefore, the state of technology of a country (or in the European case of a region) could become the strategic political factor in the global power dynamics game – if utilized wisely.

An illustrative example of how this may look like shows the case of the Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT established in the last decades common standards for financial transactions and messaging between financial institutions.

Today, to send legally secure financial transactions internationally, the bank has to be connected to the SWIFT network. In 2012, SWIFT disconnected Iranian banks from its international network due the sanction regimes by the U.S. and the EU; this blocked these banks from participating in the international finance market. Similar developments are possible with key technologies essential for the functioning of the IT infrastructure, financial and economic sector as well as any other sector relying on technology.

Here, the current lead of China in a variety of important technological sectors could become a major security and strategic risk for the West. Relying on China as being the partner for critical technological parts such as IT hardware works momentarily to a certain degree, however, it is easily imaginable that China (or other countries for that matter) will use that dependence for their own strategic political goals. This could lead to a shift of the global power dynamics. In the future, the one player determining the rules and setting of the global order might as well be the one who has the dominating access over technological knowledge and production. This is even truer for authoritarian states such as China since strategical important companies are either state-owned or the country has at least more power over private companies than Western ones. Additionally, there are a variety of non-state actors such as transnational global active companies or major non-governmental organizations, who are already exercising influence on the global political landscape, which could increasingly use technology for their own political aims.

For the transatlantic alliance, four issues should be of concern: first of all, there should be a wider acknowledgement that technology itself can become an important strategic instrument for global political rule-setting (by state and non-state actors). Secondly, the alliance should work closer together to set an international legal framework incorporating the technological advancements of the last decades, especially in the area of digitization. This also includes combining of the dozens of initiatives by the EU, UN, and other non-governmental players that are already established. Thirdly, there should be higher levels of investment in R&D and/or more initiatives to encourage companies to invest. Here, especially common research projects between countries of the alliance would be useful. Fourthly, the alliance should aim to keep certain levels of knowledge and capabilities of production in the spheres of influence to reduce the dependence in the area of critical technical infrastructure on countries such as China.

Coming Together as a Global Community – Making Technology Work for Everyone

Eva-Maria Kirschsieper

Today's technology presents a great chance to be used for the benefit of people and societies, it can be used to increase prosperity but also to enhance mutual understanding and to contribute to what Germans call “Völkerverständigung”. As Facebook CEO Mark Zuckerberg wrote last year, “progress now requires humanity coming together not just as cities or nations, but also as a global community.” However, creating such a global community, which aims at working for everyone, is challenging. Bad actors around the world are trying to abuse Facebook's tools and other platforms to undermine the democratic process. Fighting these actors is a constant battle, but we are committed to doing what it takes to get ahead of the curve.

Digital technologies have brought great change and disruption to the world of the 21st century. They have an impact on almost every industry. New forms of communication are shaping how our societies evolve. Almost all physical barriers to communication have been overcome by the internet. More than that, digital technology is promoting prosperity in unexpected places. In Kenya, the payment system M-Pesa has promoted financial inclusion and even been lauded for reducing poverty.[1] An MIT study showed that M-Pesa has had significant effects on poverty reduction — especially among female-headed households. With regards to democratic participation, studies have shown that having exposure to “weak ties” (resulting from large social networks) promotes higher levels of political engagement.[2] Moreover, social media has enabled direct communication with politicians, with over 90 per cent of German Members of Parliament having a Facebook profile and over half owning an Instagram account.

But sure enough, digital technologies need people who make good use of it. One possibility is to enable participation and foster the creation of strong global communities — something that is particularly important when looking at the most significant challenges the world is confronted with. Human ingenuity is uplifted when large groups of people work together towards a common goal. On Facebook, there are over 100 million people who are organized in what we refer to as “very meaningful” groups. Participation in such groups has been critical in Germany following the arrival of large numbers of refugees. In Hamburg, for example, the group “Hanseatic Help” provides refugee shelters in the city area with in-kind donations. The organization uses a Facebook group to inform on what items are currently needed the most. Facebook groups have enabled people to organize themselves,

[1] Suri, T., & Jack, W. (2016). The long-run poverty and gender impacts of mobile money. *Science*, *354*(6317), 1288- 1292.

[2] Kahne, J., & Bowyer, B. (2018). The political significance of social media activity and social networks. *Political Communication*, 1-24.

speak out and demonstrate for what they believe is right. From Tahrir Square to the Women's March, the internet has enabled people to organize more effectively and ensure their voices are heard. When the internet enables people from all demographics to have a voice, this should be celebrated as a great success. In that sense, online participation has become a core element of modern democracies.

At the same time, we know that bad actors are using those exact tools in order to undermine the democratic process, to spread hate and destabilize our societies. This is something we do not and cannot tolerate. Our Community Standards define our collective values for what should and should not be allowed. In the past months, we have taken significant action aiming to stop coordinated inauthentic behavior. In order to identify such behavior, we have, for example, started working with partners such as the Atlantic Council, to identify emerging threats and disinformation campaigns from around the world meant to undermine democratic processes. Rooting out these bad actors is not an easy task. In this race, we are investing heavily in technology such as artificial intelligence to stay ahead of our adversaries and ensure that our community remains inclusive for citizens worldwide.

Inclusiveness is one of the key aspects when making sure that digital technology is used for the greater good. Making technology work for everyone and listening to people's concerns regarding technology is what can enable a global and positive framework for technology to emerge. This means taking into consideration the various cultural norms of people around the globe, rooting out bias in the design of technology and promoting transparency — so people understand how technology works and are able to use it in a meaningful way across the globe.

There is a long road ahead to making digital technology work for everyone. We are in the middle of a technological shift, where technological forces are creating disruption and uncertainty. However, if we can walk the road ahead together with citizens around the world, who form our community, we are confident we can achieve a technological order that promotes prosperity and democracy.

Black Elephants, Elusive Security, and the Anticipatory Governance of Emerging Technologies

Georgios Kolliarakis

Protection from threats, both in the domestic and the international arena, lies at a critical junction. The blurring of distinction between accidents and attacks, the hyper-connectivity through technology which accounts both for better situational awareness but also for rapid cascading escalation, and not least the lack of international provisions to set frameworks for security and defence-related R&D in order to minimize abuse and safeguard fundamental rights and principles. In the ‘wicked’ field of international security, technology accounts for delivering major solutions, but also for exacerbating complexity, uncertainty, and value conflicts within and among nation states in tackling threats. The abundance in information, e.g. through Big Data, has not eliminated the constraints of decisions under imperfect and incomplete knowledge, it has rather made it worse and set it under enormous temporal pressure. Technology, however, does not emerge in a vacuum; instead, it unfolds its benevolent or malevolent, intended or non-intended impacts always within institutional, organisational, and cultural contexts. How to make sense of technology and proceed to regulatory action is the focus of this brief note.

Black Swans, Red Herrings, and: The Black Elephants in the Policy Room

Low-probability high-impact events capture the imagination of both analysts and planers. While Black Swans reside in the periphery of the strategic vision field, and therefore can seldom be foreseen, Red Herrings are traded high as potentially disruptive novelties by particularistic interests in order to steer policy attention and financial resources into certain R&D directions. Yet, it is often creeping, low-intensity cumulating events which reach a tipping point and then turn catastrophic. Although knowledge about such developments is available, it gets suppressed, ignored, or distracted from. More than the “Unknown Unknowns”, it is this kind of “Unknown Knowns” that lie in the blind spot of decision makers’ vision and become game changers: Uncomfortable knowledge and inconvenient facts that do not flow into policy planning present 2nd-order risks. Black Elephants are a hybrid breed between the Elephant in the room and a Black Swan: Everyone watches but no one actually wants to see.

Taming the beast before it is outside the cage: Disruption and Destruction potential from Emerging and Readily Available Technologies

There is a long series of emerging and readily available technologies that can have both civilian and military uses and could be deployed against hybrid threats: Artificial Intelligence and its usage in robotics and autonomous systems, a densely interconnected Internet of Things (and Humans), synthetic biology, or nanotechnology, and their usage in pattern recognition, command, control, communications and intelligence (C3I), additive manufacturing, neuroscience for cognitive enhancement to go beyond normal functionality. Key enabling technologies have always a hidden normativity about their potential desirable goals, so they are never entirely 'neutral'. Civilisation, in general, and regulatory intervention, in particular, need to establish red lines and taboo zones for security & defence technology R&D, not in order better deliver security to the citizens, but for the sake of humanity. Currently, political traction is missing for taking the lead from technology firms in exploring the legal, ethical, and also functional ramifications of technologies when they get out of the laboratory into the real world.

Regulatory Gaps and Lags

While technology developments gallop, regulatory action often creeps and lags behind. It not always makes sense to talk merely about legal or ethical 'compliance', since legal frameworks have many grey zones, and, similarly to ethics, are co-evolving. And yet, it is mandatory, that this kind of reflexion about the regulatory, institutional, legal and ethical context takes place in order to prevent backfiring and boomerang effects. Major challenge for policymakers is to learn to navigate within complexity, uncertainty, and ambiguity in a forward-looking manner. What is paramount from an anticipatory governance of security-related technologies perspective, is to put regulatory frameworks in place, which have the longest life halftime possible, so that they can capture the rapidly developing nature of technology R&D for as long as possible. Three strains of intervention are relevant here: *Hard regulation*, in the form e.g. of legislation which comes with monitoring sanctioning clauses. *Soft regulation*, in the form of standardisation or of codes of conduct and ethical self-constraint. And, lastly, further technological R&D to continuously correct imperfections, such as minimising false positives and false negatives in the performance of technology. The new possibilities and constraints of human-machine interfaces within emerging sociotechnical assemblages change the way in which decisions are taken and the threat environment is perceived, so regulation cannot follow a business-as-usual course any more.

Closing down and opening up windows of opportunity for action

As long as the technology game is perceived by politicians in predominantly economic profit terms, and not in security terms, then policy framings are bound to be competitive rather than collaborative: The former are trapped in a nation-wide radius and in rather short-term pay-off horizons. A collaborative, security-oriented framing of the challenge would demand instead a global/trans-national perspective, and a middle- to long-term planning vision. Preventing, or mitigating non-intended undesirable vulnerabilities, such as cascading dynamics leading to socio-technical collapse, out of unprecedented interconnectivity and speed, calls for concerted action in the form of effective monitoring and sanctioning. This, in turn, is premised upon stakeholder-inclusive, public-private governance regimes which aim at corporate responsibility and commitment among governmental bodies, the industry, and civil society organisations for defining rules of procedure. What is more, regulation ought to counteract Red Queen's technology races, that risk to end up to something similar to arms races during the Cold War. Needless to say, there is more to a temporal dimension in a window of opportunity: Trust is an invaluable intangible, and extremely fragile resource among partners under conditions of uncertainty: Trust may give rise to joint policy action or it can undermine it. Currently, populist politics at both sides of the Atlantic seem to instrumentalize security issues for domestic partisan consumption, undermining decade-long efforts to establish international agreements and alliances, credibility, and predictability in transatlantic relations.

Fostering technology literacy and societal context awareness

The mere pressure for common action at international level is not enough. A key prerequisite is consciousness among decision makers and analysts alike about a common problem. To start with, literacy about technology R&D among politicians is sorely missing. The current narratives about the meaning of innovation is at times dangerously naïve, in that it blends out risks, as well as the institutional, organisational, and ethical framework conditions which help transform a technological novelty into innovation which brings about more benefits than costs and has a sustainable positive effect on welfare (security included). What is more, policy action is based upon master frames of ‘primacy’, instead e.g. of ‘resilience’ and this blends out all risks associated with intra- and international socio-economic inequalities as major destabilizing factors for world security. Not least alarming is the role of technology as a vehicle to annihilate the values of liberal democracy, as it has been experienced in the Western world in the past couple of years. Having said that, second, technology developers need, equally, to get a better grasp of the societal and policy context in which the results of their work will unfold their impact, so that they ensure to minimize malevolent uses by design. Third, all involved actors, from politicians, public administrators, scientists, and potential users of security-related technologies need to acquire forward-looking competences in order to widen the horizon of their judgement. Establishing regular and systematic multi-stakeholder exchange in dedicated forums, rather than in an ad hoc, reactive manner whenever a problem has already arisen, may not be a sufficient, yet it is a non plus ultra, necessary condition for bringing diverging logics and languages closer together, and establishing shared understandings about challenges, goals and courses of action.

Technology in the Context of Geostrategic & Democratic Development - Making Sense of Digitization in Democratic Governance Architecture

Julia Krüger

1. Introduction

Technological innovation founded modern civilization in a number of ways: It balanced flaws in human nature, e.g. its weak senses, inspired domestication, and triggered the evolution of social structures up to states – just to name some. Thereby, it revealed distinctive human features: a complex language, consciousness, and sociality - underlaying the varieties of social structures today. [1] Setting specific norms for legitimate emotional or rational behavior – seldomly strict ones – these social structures – whether e.g. groups, parties, or policy fields – frame social coordination (negotiation), dependent upon individual emotional and cognitive resources, learning processes, social interactions, and dominant beliefs, values, and ideas.[2] Information and social interaction aka communication are key to any human organization (coordination).

Therefore, innovations in communication technology are special, with a direct effect on the options for social coordination. With the current speed of data processing, the global reach of communication networks, and the features of digital information – a machine-readable reduction of comprehensive information – digital technologies specifically increase the amount of communication and information up to a level that enables advanced global, social coordination – dependent on people able to adapt to changed information and communication ecologies.

As platforms able to personalize content evolved, combined with social scoring and nudging technologies, the potentials of algorithmic governance[3] (context design) became visible: If data-driven, algorithm-based information and communication self-regulating technologies became linked to the public benefit and democratic governance, they offered the tools for a fully-fledged, efficient, and global democracy.[4] Thus, the goals of technology, their particular design, and their regulation will determine their use for democratic social organization globally.

[1] Luckmann/ Berger 1966: The Social Construction of Reality.

[2] Fligstein/ McAdam 2012: A theorie of fields.

[3] Lenk 2016: Die neuen Instrumente der weltweiten digitalen Governance.

[4] A social order based upon the control of political and administrative power, the rule of law (protecting fundamental human and civil rights), and a voice and vote of people in affairs of their community.

2. Prospects of algorithmic regulation in social coordination

With the internet increasing the amount of information and communication available, and modern internet platforms structuring the immaterial assets for any player for a specific goal efficiently, long-term problems of social (market) coordination are potentially solved:

Whilst the industrial revolution and modern transport produced a growth in production and distribution of goods and services that pushed the boundaries of local markets and enabled national and global ones, producers could not control supply, transport and demand chains because of missing communication technologies. Therefore, market failures occurred frequently, and induced innovations in communication technologies, e.g. post, telephone, or television.[5]

Nowadays, Amazon – a network-based platform – coordinates a huge amount of consumer markets. Based upon a decentral, data-based, algorithm-driven infrastructure, it aligns communication and information with a diversity of market players, interacting in more-sided markets, and created a kind of technological self-regulation. But it results are not restricted to the increase of consumer comfort and business benefits, but include the destruction of local business, the exploitation of human resources, and the exaggeration of traffic as an ecological risk. Its negative external effects seem to overweight the common benefits.

Considering the climate change related need to transform the global economy into a system supplying essential goods and services sustainably for all, one my ask: are there any options to add something like ‘reduction of climate risks’ to its optimization for business, e.g. as a product-scoring according to resources spent on production and distribution? Incentives were given to the production of sustainable, basic goods and services instead of luxury ones, best consumer practices as well as smart forms of delivery. Thus, the right goal combined with technology might generate a global market regulation via platforms to the benefit of humanity, but preservation individual freedom of action and responsibility.[6]

Similarly, a change in content-ranking, e.g. by combining the amount of media interaction with the amount of its social or cultural variety, or with the amount of people reading texts before interacting, Facebook might advance information-based, constructive discourses – another fundamental asset of democracy. Considering IT security, a sector-ranking in LinkedIn, advancing e.g. jobs in critical infrastructure

[5] Beniger 1989: The Control Revolution.

[6] An alternative is constituted by data-driven, algorithm-based hierarchical state regulation, like e.g. in China. Next to its potential to produce a so called ‘eco-dictatorship’, feared by Germans, top-down regulation proved to lack innovation and adaptation over the course of history and the protection of civil liberties and political participation which are key to democracy and the attachment of people to their community (best prevention of deviant, destructive behaviour).

development (energy, water, administration etc.), might help coordinating rare professionals globally.

3. Challenges of algorithmic regulation in social coordination

The potentials of algorithmic regulation are based upon changes in collecting, processing, and communicating information relevant to social coordination.[7] But automating the process of information exchange between all market actors, and delegating human decision partly to machines includes a new challenge related to the construction of social knowledge: The machine-driven efficiency, which is based upon vague social norms put into concrete code, strengthens the impact of underlying logics – rationalities of action – in each business without exception. To produce beneficial outcomes, common norms and values must be translated in code and rankings.

But in the absence of political and social dispute over goals and methods in network-based optimization, technology obviously incorporated only the traditional norms guiding each business. Thereby, dysfunctional modes of social coordination were exaggerated, effectively, creating something like a community carousel threatening to burst now, following the rotation dynamics of singular carousel parts (markets) spinning around without any control.

Setting goals and standards for social coordination in different social arenas constitutes the core responsibility of politics. But international networking and economy withdraw adequate regulatory capacities from national regulation, regulatory objects simply escaped national boundaries. International regulation did not fill the power gap by now, lacking institutions and procedures suited to reconcile the variety of global cultures and interests for a common good.

4. Bringing back politics to algorithmic governance in social coordination

The amount of global problems threatening humanity now and the potential of algorithmic regulation combined with democratic standards bear another chance for international coordination:[8] A digital, international democracy architecture based upon technology supporting the identification of global problems, causes and potential solutions efficiently might provide the means for adequate action. Such a ‘democratic governance platform’ would include at least:

- the exploration of global data related to human problems, economy, and ecology to identify pressing problems and their causes, developing a ranking due to urgency;

[7] Spinner 1994: Die Wissensordnung: Ein Leitkonzept für die dritte Grundordnung des Informationszeitalters.

[8] For the problems: Hawking 2016: This is the most dangerous time for our planet.

- the effective coordination of information related to problems and solutions, considering/ combining the global variety of technological and human analytic resources;
- instruments to develop/ to decide concrete strategies, based-upon human-machine interfaces displaying major options, and to assign responsibility and authority to coordinate necessary changes amongst a variety of sectors and stakeholders;
- instruments to transfer global solutions to local forms of social coordination;
- instruments to constantly assess progress or problems (in reducing risks and harms for now) in order to react appropriate, e.g. using different resources, ideas or tools;
- the development of global, potentially data-driven means to address problems (participation) and a mixed-method solution for assessing the 'government' (legitimacy).

Envisioning democratic governance making sense of increased information and communication technology as a regulation asset for politics and people, leads to central obstacles: Is there any reason to assume political or economic stakeholders, or international communities are open to disruptive changes in global cooperation? Despite the decrease of regulation capacity and international cooperation to solve common problems, they probably would fear loosing their position and personal achievements, and opt for transforming existing standards instead.

5. Conclusion

Choosing the reduction of little risks instead of larger potential benefits is a common choice driving human behavior.[9] Hence, sticking to conservative norms, values, and beliefs – deeply institutionalized in social structures – is consequential, but prevents the exploration of benefits produced by socio-technological change, and its adaptation in social or political coordination. Therefore, a change in using technology for democracy depends on the attitude of political leaders and their willingness to set the right goals and standards for technology design in international coordination. The win was to prove democracy's ability to care for people, to inspire competition and innovation to their benefit, and to adapt its organization, if necessary.

[9] Von Grafenstein/ Hölzel/ Irgmaier/ Pohle 2018: Nudging.

A Threat to Democracy? The Impact of Information Technologies on Elections

Jan Rau

The question of whether and how the internet is shaping democracy is one of the oldest debates surrounding the rise in importance of the internet. Authors like Manuel Castells celebrated the egalitarian access to the internet as a catalyst for democracy, predicting an uprising of the people against incumbent elites and institutions. The Internet was seen as the place where new political movements would coalesce and shake off the bonds of an entrenched and outdated system. However, recent discussions around new media like Facebook and Twitter are more pessimistic. Looking at the two most recent major elections in the US and Germany, the Internet and its new platforms are at least partly blamed for the rise of right-wing actors like Donald Trump and the AfD (Alternative for Germany). Media phenomena like echo chambers and political disinformation are considered as core threats to democracy.

But to what extent can this potential influence of the internet on elections be confirmed? Looking at three widely discussed topics surrounding the impact of the Internet on democratic elections — namely, the internet as a field for new political actors; internet media and political disinformation; and finally internet media and echo chambers—the empirical evidence shows mixed results regarding effects of the internet and social media.

One central field of internet studies concentrates on new political movements and actors and how they use the internet to accomplish (or fail to accomplish) their goals. A central argument is that internet media is used by these new political actors to bypass traditional media gatekeepers. While these new actors often perceive traditional media as biased against them, the Internet offers them a new media realm where they can promote their messages or shape the traditional media agenda. Looking at Internet media as an action field for new political actors, there are indeed compelling arguments that Internet media was a precondition for the success of Donald Trump and the German AfD in entering the political landscape. Donald Trump used Internet media in the primaries to gain a disproportionate amount of attention and outcompete the other candidates, despite lacking the support of the party establishment and spending significantly fewer resources than the other candidates. Trump used the dynamics of a market-orientated media system to circumvent the gatekeeping role of traditional media and push himself into the media agenda. The AfD used Internet media to create a counter-public during the so-called “refugee crisis” in 2015, while circumventing the gatekeeper position of traditional media. Social media remains an important communication channel for the party.

However, assessing the impact of political disinformation on the election results turns out much more difficult. While in the U.S. there was a massive presence of political disinformation prior to the election, political disinformation in Germany only played a subordinate role. This can be reasoned by the substantial differences in the political and the media systems between the U.S. and Germany, where in Germany there is less political polarisation and distrust in media and politics, as well the central role of public media versus the subordinate role of social media. Nevertheless, as communication studies are undergoing foundational transformations with difficulties assessing contemporary media effects, it is not possible to say whether political disinformation had a decisive impact on the elections or not.

The analysis of the role of echo chambers shows similar results. In general, it seems like the importance of echo chambers is overstated as empirical research does not support the idea of large-scale audience fragmentation or significant polarisation caused primarily by the Internet. There are signs that there might be an exception for the political extreme, which in general might have harmful effects on the democratic culture, but this group is still a minority and their influence will remain unclear until further research is conducted. Similar to political disinformation, it is also not possible to say whether echo chambers had a decisive impact on the elections or not. But there are good arguments to say that for both phenomena the overheated discussions were not in a reasonable relation to potential effects.

What becomes salient on the other hand, is that the rise of political actors like Trump or the AfD cannot be separated by the political and structural conditions and developments in the respective countries. The impact of the Internet was imbedded in the respective political and media systems and connected to major political events like the refugee crisis. There is a tendency especially in the public discussion to credit the internet with great impact on major political events like election outcomes. The Internet, without doubt, plays a significant role in these events. Nevertheless, the influence of the Internet is limited compared to other major structural conditions or long-term developments and potential media effect should not be overrated in comparison to other factors. Trump could have gained as much attention as possible but he would have never won the election without the support of a substantial portion of the electorate. The issues which Trump pushed forward like distrust in the established state elites and the government, distrust in the media and anti-immigrant, -refugee and -Muslim prejudices might have been reinforced by him but did not originate in him. The same is true while looking at the impact of real-world phenomena and long-term developments like the aftermath of the financial crisis, fear of globalisation or security issues. Looking at the the AfD, they could have not succeeded without crucial non-media factors. These include similar factors to Trump like globalisation fears and anti-immigrant sentiments but also specific German conditions like major changes in the political party landscape (left orientation of the Christdemocracts under Angela Merkel and declining party affiliation) or persisting disparities between former west and east Germany in terms of politics and economics. All in all, while the Internet clearly is shaping society and politics, at the same time it is important to not exaggerate its impact compared to other deeper and more influential factors.

Regulating AI as a Test Case to Democratic Institutions and Policy Making

Lina Rusch

In many ways, the post-World War global order is facing fundamental challenges. Not only are populism and general lack of confidence in institutions becoming more prevalent in both Europe and North America, the ongoing societal transformations have also shaken the core of our alliances, organizations and other institutions. Moreover, with digitization progressing as fast as it currently seems to, it might soon need an overall reshaping of our current institutional framework. The advent of Artificial Intelligence (AI) in particular is proving to be a test case for our existing order.

How AI challenges the international order

The global multilateral framework has long relied on international law, diplomacy and good faith partnership. In many ways, AI cannot be grasped within the traditional realm of these. As a technological innovation, AI is on several levels more powerful, less understood and more profoundly beyond the grasp of human interference in its decision making than previous ones. As AI-based technologies creep into ever more aspects of life, the more vulnerable humankind becomes its potential underlying effects. Hence, the need for regulation is seen in increasing numbers of states in the world. At the same time, the economic benefits being hard to estimate but potentially boundless, a global race for AI leadership has begun.

Whereas states do not fail to adhere to the idea that the laws of the pre-AI era continue to apply, including human rights such as the right to informational freedom, the sheer mass of big data and AI utilization that can be observed now and even more so in the near future at least casts doubt on expectations that states will be able to continue to guarantee the full bandwidth of human and civil rights in the years to come. The lack of specific agreed-upon digital rights that guarantee individual freedoms are only one part of the medal. The very different directions in which states are developing their AI strategies are another.

On an international level it seems unlikely that international treaties and customary law could be developed on any near-global scale, setting the boundaries for an ethical AI application in a globalised world. Beyond the purely ethical perspective on regulating AI, even the most practical question of how to transfer (big quantities) of data between the relatively like-minded transatlantic partner states remains unanswered, as the once overhauled and soon to be revoked again Privacy Shield, a treaty for data transfers between the US and the European Union, proves.

How AI requires new forms of cooperation & policy making

National policy making that wants to reap the benefits of AI for society and at the same time sets limits to its unbounded spread is inherently limited. It is therefore understandable that at this stage, European policymakers focus on enabling AI economically and shy away from any hard regulation. With a pan-European approach as the only viable solution, this is to an extent understandable. Yet, there seems to be little imagination among policymakers for new kinds of approaches to policy making in the age of AI.
Germany has been at the forefront of trying to generate international treaties that prescribe ethics to the digital realm – with little success. The “Cyberaußenpolitik” of the current and previous Federal Government puts protecting human rights at the centre of its policy efforts, next to guaranteeing a free and secure internet for all. Policymakers need to ask themselves, if diplomatic initiatives and activities in the multilateral organisational framework can be sufficient in achieving these goals at this point. It might be that entirely new modes of cooperation between states and even between states and companies are necessary.

While the answer to these questions could be that lawmakers might use less formalised and more flexible regulatory instruments and create similar international agreements and institutions as in the decades before with other emerging global and transnational challenges, another answer could be that solutions need to be thought entirely out of the box of the present international order.

Present at the New Creation? Tech. Power. Democracy. A Statement

Gary S. Schaal

Hypothesis

I also support the hypotheses that democracy as a form of government will be severely weakened in the coming years due to processes of digitization. The intensity of the weakening will vary depending on the countermeasures taken over the next five years.

There is not *just one major* process that weakens democracy, but a complex network of processes and phenomena that mutually reinforce each other and whose destabilization potential genuinely results from the "essence" of digitization processes. To illustrate this, I will make an analytical distinction between the levels of knowledge, democratic institutions/process/procedures and democratic values:

Knowledge

Relevant voices in the discourse assume that democracy will collapse in the medium term. Some even interpret this as an opportunity to create a new order. But even the representatives of this position cannot name the concrete factors that will cause democracy to collapse (social unrest, autocratic coups, revolution, etc.). Without a precise identification of the factors, however, it is neither possible to avert the collapse nor to guide a transformation in a politically responsible manner.

The main reason for this is that we have high (structural) knowledge deficits in those areas that are characterized by intense digitization processes. These knowledge deficits have different sources. The first source is that there are still no theoretical approaches in the social sciences and the humanities that genuinely reflect on the digital and integrate it constitutively into their basic assumptions. Theories already exist that may be used to analyze transformations resulting from digitization processes - changes in the democratic public sphere, changes in the participation portfolio - but these analyses remain sectoral and unrelated. What is missing are theoretical approaches that are inter- or transdisciplinary and correspond to the cross-sectional character of the digitization processes.

Figuratively speaking, we are currently still looking at digital transformation processes through analog glasses and are therefore limited in our knowledge in a dangerous way. Because due to the factors mentioned above, not only the number of *known unknowns* is increasing, but - much more dangerously - also the number of *unknown unknowns.*

But even genuine digital theories face (epistemic) challenges that are difficult to meet. The processes mentioned above increase the social complexity and thus the complexity of the processes to be analyzed exponentially. The number of emergent events is increasing. But how can emergent events be anticipated?

One area in which the knowledge deficits outlined are a threat to democracy is the (military) security sector. *Hybrid influencing* and *hybrid threats* have only become possible through digitization processes. They threaten democracies below the threshold level of war (at least according to the current understandings), and still have the capacity to destabilize established democracies in the long term. At the same time, they are very difficult to anticipate because the threats themselves are emergent events.

Institutions - Procedures - Processes

Today's institutions and procedures of established democracies can be interpreted as solutions to regulatory challenges ("Ordnungsherausforderungen") on the threshold of modern times, in the context of the establishment of modern nation states. As a result, many of today's democratic institutions and processes no longer meet the requirements of a digitally transformed society in terms of complexity processing capacity, speed or epistemic quality. In the academic and public debates, therefore, an irritating picture emerges: the regulatory challenges to which we are now seeking solutions are similar to the historical challenges that have already arisen on the threshold of modern times. However, the answers differ fundamentally due to the increasing digitality. This simultaneity - the challenges are well-known, the solutions must be innovative - leads to a dualism in the discourse by either over-emphasizing the traditional part (the questions are known, therefor digitization processes do not create a genuinely new problem pressure) or over-emphasizing the need for innovation (we need completely new solutions). The simultaneousness of the familiar and the new is misunderstood, also with regard to the parallelism of analog and digital institutions, procedures institutions - at least for a transitional period.

Due to the fact that the established analog processes and institutions continue to represent solutions for accepted regulatory challenges, they are not completely dysfunctional. However, they are also not so high-performing that they would not have to transform. The longer sub optimally performing institutions, procedures and processes remain in use, the more uncompetitive and dysfunctional the corresponding democracies become.

Values and norms of democracy

Democracy as a form of rule has both an intrinsic (normative) and functional dimension. We value certain norms, values and guiding principles for themselves; we value certain institutional procedures because they are problem-solving. As already mentioned, the problem-solving capacity of analog processes is rapidly decreasing due to digitization processes. But the values and norms of democracy are also under stress. For not all ideals and values can be kept under the conditions of increasing digitality, such as the ideal of privacy (as an aspect of negative civil rights) or data protection.

Institutions are concretizations of guiding ideas, values and norms, i.e. to the extent that certain values and norms no longer apply, institutional reality must also be adapted. Institutional solutions must therefore be found which, under conditions of digitization, represent appropriate concretization of valid democratic values and standards. For example, the triple reading of laws has been implemented with the aim of increasing the epistemic quality of laws. Under present conditions of acceleration ("Gegenwartsschrumpfung"), however, this strategy to secure and retain the epistemic quality of law leads to functional deficits, because the speed requirements for democratic problem solving coming from other systems of society (especially the economy) cannot be met in this way.

At least three questions need to be clarified at the level of the values and norms of democracy and their connection to democratic institutions and procedures:

a) If it is already foreseeable today that not all of today's constitutionally codified values of democracy can be maintained, the core of democratic values and norms to be maintained in the future must be identified asap – this core defines, which norms and values are worth fighting for. This also means identifying those values and norms that cannot be maintained and whose defense binds resources that can be used more productively.

b) It must be identified whether and if so which historically new democratic or constitutional values and norms are necessary. An example of this is the discussion about fundamental rights to "mental privacy" and "cognitive liberty". The normative foundation of democracy also requires a comparison of its central premises with the latest findings in neuroscience, among other things with regard to the premise of freedom of will and the ideal of political autonomy based on it. The same issue can be viewed from different disciplinary perspectives. Paraphrased from the perspective of informatics, the question can be asked whether the ideal of autonomy can still be defended if epistemically better decisions are possible through the use of big data and algorithmic decision making?

c) It is functionally necessary to find equivalents for dysfunctional institutions, procedures and processes’. It is important that the discourses are properly framed: For it is not the ideals that are discursively problematized, but their historically contingent institutional concretization(s). A crisis of a concretization is not a crisis of the values and norms on which it is founded. To give an example: a crisis of political parties is not a crisis of democracy, because parties are a historically contingent form of political decision-making that can be replaced by functional equivalents. The ideal of political autonomy is not called into question by the crisis of the parties. However, if the institutions concerned establish such a link for reasons of maintaining power, democracy's capacity for innovation will be weakened and its stability undermined.

Conclusions

Democracies are under threat since evidence-based, problem-solving policies are becoming increasingly difficult, because digital theories are not yet available and emergent events will increasingly challenge democracies. Its institutions and procedures are no longer sufficiently efficient to deal with complex political issues appropriately. This can lead to alienation of citizens from democracy. In a direct comparison of systems, autocratic states that are technologically well positioned, quasi-states (such as Google) or forms of local self-organization (commons, multitude) are gaining relatively in importance. The self-organized forms can be democratic and are therefor favorable from a normative point of view. But still, the transformation phases will destabilize the established democracies and lead to internal upheavals that can entail high social, economic and political costs.

Therefore, a discourse is needed on which values democracy should still rely under conditions of digitization. And by which institutions, procedures and processes´ these values are to be put into concrete terms. If this discourse is not conducted, democracies become increasingly dysfunctional, both on the normative and on the functional dimension.

The Advent of Digital Dictatorship

Torrey Taussig

Synopsis: Technological advancements once thought of as destabilizing for dictators are now enhancing the staying power of authoritarian regimes. By employing advanced tools of monitoring and censorship powered by AI, authoritarian leaders are able to maintain control over their people without resorting to delegitimizing and overtly repressive tactics. As powerful authoritarian regimes including Russia and China expand their influence abroad and challenge U.S. vital interests around the world, advancements in artificial intelligence will define the future character of great power competition.

The prevailing mood at the end of the Cold War was that authoritarian regimes were transitory and distinctly disadvantaged vis-à-vis democratic states. The logic went that as globalization provided citizens around the world with the ability to trade, travel and access information, a state’s capacity to withstand political shocks would decrease. From this perspective, for autocracies to be stable they would have to either close their borders (geographical and technological) or open their political systems.

Prior to the Arab Spring movements that began in late-2010, consensus among experts and policymakers was that technological revolutions in communications, social media, and access to cell phones would only further this post-Cold War logic, connecting individuals and empowering civil society against strongmen leaders. Simply put, modern technology was primed to move power away from authoritarian governments and place it in the hands of the people.

Yet recent years have witnessed competing, if not contradictory, trends: technological advancements have occurred alongside significant democratic backsliding in almost every region of the world.

One reason for these competing trends is that technological innovation is proving to enhance the staying power of authoritarian governments. First, advanced monitoring and censorship tools allow authoritarian regimes to reap the economic benefits of globalization while maintaining control over their populations. Moreover, dictators are able to centralize control without resorting to costly and overtly repressive tactics that delegitimize the regime. Guns and tanks are not needed to break up protests when governments can instead monitor social media platforms and cell phone communications to determine when and where protests might occur, shutting them down before people even move to the streets. Artificial intelligence promises to make these capabilities even more potent.

From Tiananmen to Tencent[T]

While many have been surprised by this phenomenon, the use of technology to repress citizens in authoritarian states is not new. Technology was a central element of control in totalitarian regimes throughout the 20th century. In 1956, Carl Friedrich and Zbigniew Brzezinski described 20th century totalitarian regimes as "The outcomes of movements directed against the denigration of the state in the liberal age... based upon modern technology and mass legitimation."[1] Indeed, a central feature in the lifeline of undemocratic political regimes has been the shrewd ability of dictators to manipulate, censor and repress communication and information.

Totalitarian ideology as a pillar of authoritarian strength may have lost its legitimacy, but organizational power has not. This set of factors includes the institutional strength of a ruling political party, adaptive coercive capacities over civil society and the media, and state control of the economy. Authoritarian states today are similar to their totalitarian predecessors in that they require these elements of organizational power to implement their goals. Technology was, and still is, a key aspect of that power.

A prime illustration of today's *digital dictatorship* is the powerful surveillance state emerging in China. Today the Chinese government does not have to resort to violently crushing threats to the government, as was seen in 1989 Tiananmen Square protests. Instead China's "great firewall" can monitor and censor online material that is critical of the government. The CCP can also monitor citizens' digital and physical footprints – thereby predicting and removing threats to the regime before they emerge.

Moving forward, improvements in AI and facial recognition technology will make China's estimated 200 million surveillance cameras (four times as many as the U.S.) even more adept at identifying and tracking its 1.4 billion citizens. This surveillance system is already turning China's Xinjiang Province, home to the Uighar minority population, into a police state. Around the country facial recognition technology is also fueling China's nascent social credit system, which will track social behavior and monitor for signs of disobedience to the government.

Alongside the evident dismantling of civil society and open spaces (in the physical and online realms), authoritarian regimes are moving from consolidating power within their borders to expanding influence beyond them. As Xi Jinping's Belt and Road Initiative (BRI) sweeps the globe, one has to wonder whether China's facial recognition technology will begin to accompany development projects in authoritarian states where China does business. Already the technology has been exported to countries in Africa and Southeast Asia. In March 2018, Zimbabwe signed a contract backed by the BRI with a Gunagzhou-based startup to begin a large-scale facial recognition program throughout its security and law enforcement agencies.

[T] China's biggest tech titan that provides a popular instant messaging app.

[1] Carl Friedrich and Zbigniew Brzezinski, *Totalitarian Dictatorship and Autocracy,* (New York: Praeger Publishers, 1956), 8.

AI and Great Power Competition

As America adapts its national security strategy to a new paradigm of great power competition with Russia and China, technology will play a pivotal role in each state's strategy to compete, deter, and at worst, defeat one another in open confrontation. As a result, each nation is prioritizing and advancing its AI capabilities. In July 2017, China's State Council outlined a plan[2] to build a domestic industry for artificial intelligence worth 150 billion USD and turn the country into the world's leading innovation hub for AI by 2030. In September 2017, the Russian state-funded media outlet *RT* quoted President Putin as stating[3]: "Artificial intelligence is the future, not only for Russia, but for all humankind...Whoever becomes the leader in this sphere will become the ruler of the world." Among both authoritarian powers, China's economic supremacy makes it the stronger long-term strategic challenge, despite Putin's proven ability to manipulate social media and interfere in democratic elections. Moreover, Russia's annual domestic investment on AI is around 12.5 million USD, paling in comparison[4] to that of China and the U.S.[5]

Looking ahead, will democracies or authoritarian states have an edge in harnessing the power of AI? On one hand, democracies have proven more capable of producing innovative technologies due to their inherently entrepreneurial character and human talent. On the other, autocracies are able utilize the capabilities of the private sector towards state objectives and maintain uninhibited access to citizens' personal information.

Here China has commanding lead, with access to a treasure trove of data from over 770 million internet users. Combined with a centralized political system, this may give China a key advantage over the United States and other democracies in employing the power of AI. As Yuval Noah Harari, author of *21 Lessons for the 21st Century*, writes[6]: "The main handicap of authoritarian regimes in the 20th century—the desire to concentrate all information and power in one place—may become their decisive advantage in the 21st century." The crucial question will be to what end the CCP is looking to employ technological advancements, at home and abroad. Regardless, signs point in a worrying direction for the future of democracy and democratization.

[2] https://www.scmp.com/business/china-business/article/2115935/chinas-xi-jinping-highlights-ai-big-data-and-shared-economy
[3] https://www.rt.com/news/401731-ai-rule-world-putin/
[4] https://www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development/147178/
[5] The U.S. government's total spending on unclassified AI programs in 2016 was about $1.2 billion, according to In-Q-Tel, a research arm of the U.S. intelligence community.
[6] https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330/

Disrupting Disruption: How Do Democratic Societies Harness New Technologies While Staying True to Their Values?

Daniel P. Vajdich

Recent technological innovations are not the first inventions or discoveries to affect political and geopolitical dynamics—and they certainly will not be the last. Much like today’s social media, the printing press, radio, and television also revolutionized democratic politics by amplifying the ability of political actors to reach voters and vice versa. But there remained certain practical guardrails that placed limitations on who could utilize these technologies and how. By and large, a relatively small number of truly national media owned, controlled, and operated by traditional elites, possessing a general interest in stability, could and would determine an editorial policy that did not deviate too far from the status quo. Consistent with this, these media gave time and space to political actors who were at or near the center of the political spectrum. Only those political actors with substantial financial resources could purchase advertisements to build support, and to attract such financial resources these political actors would need to appeal to well-endowed individuals and businesses whose financial success was contingent on maintaining some variation of the political, economic, and social status quo.

While this oversimplified description of relations between the mass media, economic elites, and political actors paints a bleak picture of nineteenth and twentieth democracy, the general dynamics do hold true—or least they did until recently. The advent of social media and related technologies, however, has undoubtedly led to a democratization of thought leadership. Millions have acquired the means to be heard and to therefore influence. We have witnessed a transition in politics and movement along the governance spectrum from representative democracy to a more direct form of democracy. The elites that have subtly guided liberal democracies in the direction of the status quo are no longer able to play that role to the extent they had. In many ways, the guardrails referred to above have been corroded and in some cases destroyed entirely.

But is this a negative or positive dynamic for our societies? In principle, the notion of more direct democracy is appealing. These technologies have allowed average citizens to circumvent barriers that have existed regarding their ability to participate in important processes related to the governance of their countries. At the same time, the negative practical implications that we have witnessed in recent years cannot and must not be ignored. Social media and related technological advancements have also given a voice and means of influence to actors—both internal and external—whose intentions threaten the stability and integrity of democratic governance. These individuals, organizations, and governments have successfully leveraged such technologies to generate divisions, sow confusion, and undermine what has hitherto been a widespread belief in the general fairness and responsiveness of liberal democratic institutions.

The consequences of these technologies for authoritarian countries, much like liberal democratic societies, are not facilely positive or negative. Social media played a vital role in spurring and sustaining the Arab Spring. While these demonstrations did not result in the sort of change first envisioned, they did demonstrate that new technologies can be used to mobilize individuals on a mass-scale in order to demand better governance and greater openness. Since then, however, these same technologies have been harnessed by the authoritarian governments themselves to stifle dissent and manipulate public opinion.

The most well-known example of this was the exploitation of social media and the penetration of various technological vulnerabilities by Russia to interfere in the U.S. presidential election. This is now widely accepted as fact in the United States. But there is far less consensus regarding what should be done to prevent similar intrusions in the future. The midterm Congressional elections will be held in the United States in early November and it is clear that Russia is once again finding ways to meddle in the U.S. political process. President Donald Trump’s own Director of National Intelligence Dan Coats and Secretary of State Mike Pompeo have both publicly confirmed this. Over the summer, Facebook, Twitter, and Microsoft announced that they had thwarted efforts by Russia and Iran to influence political groups in the United States and closed malicious accounts that originated in the countries.

The recent actions taken by the technology companies indicate that (1) these firms are now much more vigilant about large-scale abuse of their platforms and (2) Russia and others continue to seek ways to influence the American political process by exploiting new technologies that have the potential to either affect public opinion or access private information. Facebook, Twitter, and YouTube are hiring thousands of human content reviewers to remove fake accounts and develop new methodologies to reduce disinformation campaigns. Microsoft, Cloudflare, and Google have launched free tools to protect political campaigns and their IT infrastructure from cyber-attacks that could lead to the release of sensitive or embarrassing information (the latter of course took place when Hillary Clinton campaign chairman John Podesta’s email account was hacked and its contents distributed to the media during the 2016 U.S. presidential election.)

One need not understand from an engineering perspective the technologies developed over the past 10-15 years to fully grasp their immense implications for democracy, governance, and inter-state relations. The technological genie cannot be put back in its bottle—but the genie can and should be tamed in a way that safeguards our security without compromising the values and principles of our liberal democratic societies or their inherent drive to innovate. The Honest Ads Act has been introduced in the U.S. Congress, which would promote regulation of campaign advertisements online by companies such as Facebook and Google but has not been taken up. As previously noted, large tech companies are now much more cognizant of the responsibility they carry, and the consequences they will face should they fail to fulfill that responsibility. The challenge has been widely recognized. But this is merely a start. We must now contemplate concrete action that will begin to address this formidable challenge. These are a few of the potential solutions that should be considered:

- Requiring tech companies to label and properly identify bot and bot accounts;
- Allowing governments to audit tech company algorithms;
- Ensuring data transparency;
- Developing and going public with clearer methods of deterrence for cyber-attacks, especially those that undermine the integrity of political processes;
- Engaging in media literacy campaigns;
- Mandating that online political ads be revealed (per the Honest Ads Act); and
- Creating new agencies and institutions to protect political organizations and processes.

Interdependence, Inclusiveness, Ingenuity: a Three-stage Approach to Technological Progress

Bartosz Wiśniewski

In the world of economics, technology—and technological progress in particular—is widely, yet not universally considered to be the decisive factor behind growth and progress. In complex industrialized and increasingly digitized economies, the factor of expenditure of capital and labor is not enough to convincingly explain why some states enjoy stronger growth than others, or why some are more competitive than other. As the interplay between technology and growth had become internalized in the mindsets of policy- and decision-makers, the need to invest in human capital and research—the two pillars of technological progress—was translated into strategies of innovation-driven growth.

Do all new technologies create openings for qualitative growth? Of course not. It is possible to increase efficiency, decrease the marginal costs, and still get ahead of the competition by doing more for less, or in a shorter period of time. These technological improvements merely sustain the exisiting model of manufacturing or provision of services. It is the disruptive technologies that upend the status quo and force the dominant companies to either adjust their strategies to a new reality, or to give in and accept a decreased market share.

The author of the term „disruptive innovation," Clayton Christensen, differentiated between „low-end" and „new-market" innovations capable of profoundly affecting the structure of the market and the behavior of incumbents. In the former case, introduction of an innovation allowed to win a relatively small number of clients or buyers from the competition. The product associated with a low-end disruptive innovation is going to have similar features, but because of other important factors, such as smart marketing and potential impact on consumption patterns, it is nonetheless likely to cause a headache to the erstwhile leaders in the longer term. In the latter case—a „new-market" disruptive innovation—a newcomer to the market is able to broaden the client base, i.e. to increase the demand side.

„New-market" innovations are not uncommon and often have to do with the ability to successfully combine products or services from two or more different sectors. Think of a company that principally offers courses in computer programming and leadership development, but decides to do so in English, turning an ordinary foreign language course into a tool for general skills development. By positioning itself as a language school, it can now reach new clients for its core products. „Traditional" langauge schools will be affected, whereas our innovators will open the market to those who so far were interested only in mastering the knowledge of a foreign language. It takes only a little effort and imagination to grasp how such micro changes, happening on the level of individual companies, affect the macro picture, i.e. whole industry sectors and the mindsets of both producers and consumers.

This „two in one” philosophy can be especially effective for someone with little time on their hands. Perhaps crucially, however, this example shows that a disruptive innovation does not have to do with the introduction of a new technology, or with technological progress. It might just as well have to do with correctly identifying the direction in which the market is likely to develop and being the first to respond to demand.

Does the concept of disruptive innovation offer any useful lessons for the world of politics, and international politics in particular? A politician able to woe heretofore passive, disinterested citizens into going to the polls could be credited with coming up with a „new-market” innovation: a fresh agenda, e.g. shunning traditional divisions between left and right, liberal and conservative; or a promise of a new approach to policymaking. A „low-end” innovation would mean that without offering anything new, he was still able to win the votes from an opponent, simply because he accurately sensed the voters’ desire either for a change of guard, or to send a warning signal to the incumbents.

In another words, charismatic leaders could be defined as a very distinct group of disruptive innovators. More often, however, decision makers are confronted with the need to react to technological or merely management change. Otherwise, they risk missing important developments that can affect their political fate, or simply the ability to shape events in line with their priorities. Three distinct issues—„3Is”—merit special attention.

First, technological progress can bring about increased **interdependence** among states. Complex, high-tech products may require access to scarce mineral resources, such as rare-earth elements. Supply chains of such products may rarely be confined to a single state, or a group of states whose political priorities are aligned or compatible. What follows is additional layers of interactions and interests which affect the decision making process. Vulnerabilities—or additional opportunities to exert influence—emerge, thus necessitating trade-offs. The challenge is not to imperil one priority over the other.

Second, technological progress can mount a challenge to **inclusiveness** and social cohesion. In another words, if the benefits of an innovation will be available only for the selection few, e.g. because of high price, progress can in fact amplify existing social and economic discrepancies and tensions. Think of access to healthcare on the national level, or agricultural competition on an international scale. Developing countries rely on food production and exports to a greater degree than industrialized ones, yet may be deprived of access e.g. to the latest advancements in ensuring the livability of crops simply because such solutions are too expensive. As a result, they are less likely to compete with producers from developed countries. Thus if not properly managed—if insufficiently inclusive—technological progress can do more harm than good.

Finally, technological progress puts new demands on how we understand **ingenuity**. It goes without saying that technological advancements requires new skills, and down the road also the rethinking of the shape of the education system. A single country may not be able to properly equip a cadre of specialists whose work will be necessary to wield the whole potential of technological change and innovation. Thus the quest for the redefinition of ingenuity requires greater openness to international cooperation—and this is where the „3Is” become a coherent whole. For openness and interdependence are the two sides of the same coin. Fortunately, unlike when blind fate decides the „winning” side of the coin, it is possible to have it both ways—to accept the costs associated with interdependence and to embrace greater openness.

Aspen Institute Germany

Aspen Transatlantic Workshop

„Present at the New Creation? Tech. Power. Democracy.”

September 27 – September 29, 2018

Essays

The Aspen Institute Germany thanks its generous supporters:

LOTTO STIFTUNG BERLIN

VOLKSWAGEN
AKTIENGESELLSCHAFT

Estonian Embassy
in Berlin