# MIND THE TECHNOLOGY GAP: THE IMPORTANCE OF TECHNOLOGICAL LITERACY AMID TRANSATLANTIC STRIFE

THOMAS HANLEY

The transatlantic alliance is showing unprecedented signs of cracking. Since President Donald Trump's election in 2016, it has been nearly impossible to find major policy priorities where Europe and the United States agree. Mr. Trump even questions why the United States is so closely aligned with Europe in the first place, and has named the European Union (EU) one of the United States' greatest "foes."[1] His disdain for the European Union is no secret, but his most consistent object of derision has been Germany. In response, German chancellor Angela Merkel has said that Europe can no longer "rely on the superpower of the United States,"[2] while German foreign minister Heiko Maas has pointed out that even the very foundation of the transatlantic alliance—a consensus on shared values—"has come off the rails."[3] Despite this cleavage, Germany and the United States continue to face similar threats. In looking to the next generation, one of the greatest challenges will be ensuring both American and European societies are aptly prepared for a world dominated by new technologies. Technology is at the heart of many challenges in the twenty-first century: confronting China, defending democracy from foreign influence, or even ensuring a basic civic trust within society. Technologies such as artificial intelligence (AI), deepfake videos, data mining, and 5G are only going to become more important in the future. Frighteningly enough, most legislators are not prepared to embrace this reality. In the United States, Senator Orrin Hatch became perhaps the most meme-worthy example of a pervasive technological illiteracy among policymakers when he asked Mark Zuckerberg, "How do you sustain a business model in which users don't pay for your service?"[4] In Germany, the recent debate over whether Chinese technology should be excluded from the country's 5G network has shown policymakers' inability to grasp the complexities of the technology in question. On both topics, German and American government officials desperately require technological assistance.

Yet this is only half the story. While policymakers in the West may be struggling to understand emerging technologies, countries like Russia and China are not. And they are increasingly exploiting these technologies to their advantage. Technological illiteracy is an internal vulnerability that has exacerbated external threats to Western democracies. This merits action. And while substantial transatlantic policy cooperation is unlikely considering the current state of the relationship, there is still plenty of room for lower-stake cooperation. Transatlantic enthusiasts would be wise to channel their efforts here. One such lower-stake solution would be to empower and deepen cooperation between government institutions devoted to promoting technological expertise among legislators, specifically offices of technology assessment. Cooperation on this front has an actual chance for success, and would ensure policymakers are appropriately informed to weigh the tough political dilemmas of tomorrow.

## Emerging Tech Threats

The role that technology plays and will continue to play in society necessitates that politicians adequately understand it. However, an even more pressing motivation is the fact that countries like Russia and China are well positioned to exploit this knowledge gap. In both countries, power is concentrated in a much smaller number of governing elites—and these elites are technologically astute.

Both countries have proven that they are quite capable of understanding technology's potential—and using it to their advantage.

In Russia, Vladimir Putin dominates the political landscape, directing both foreign and domestic policy. One of the ways he has been able to influence Western domestic politics is through disinformation campaigns. Putin was quick to recognize the dark potential of Western social media platforms. Disinformation operations were taking place within Russia as early as 2011, following anti-Putin protests.[5] Since then, the effort has been exported and has targeted every NATO member state.[6] In the United States, the 2016 presidential election was the apex of a targeted campaign by the Russian government to manipulate U.S. voters through Facebook, Instagram, Twitter, and Youtube. Its ultimate design was to polarize the American electorate by "spread[ing] sensationalist, conspiratorial, and other forms of junk political news and misinformation to voters across the political spectrum."[7] This is, of course, nothing new for Europe, particularly Germany. As early as 2014, Moscow was using social media networks and comment sections to peddle pro-Russian messaging throughout the German populace.[8] And in the lead up to the May elections for the European Parliament, Russian efforts on German social media have focused on bolstering support for EU-skeptic parties such as the Alternative for Germany (AfD),[9] while at the same time amplifying messages from left-wing anti-fascists to exacerbate internal tensions.[10] Yet these tactics have not been nearly as successful in Germany as they have been in the United States—partly because of the U.S.' inability to recognize what was happening. U.S. intelligence officials were aware that Russia had successfully used social media as a propaganda tool both domestically and in Ukraine, yet it took them at least two years to realize that similar efforts were being deployed in the United States.[11]

While Russia has shown a keen ability to exploit Western social media platforms, the more formidable threat comes from China. Recent concerns about the implications of including Chinese technology into Western supply chains is a case in point. Particular focus has been given to Western critical infrastructure technology, such as the technology used in 5G networks. The West's growing dependence on Chinese technology is a direct result of the Chinese government's "Made in China 2025" initiative, a concerted effort by the Chinese government to become a global high-tech leader. In combining technological innovation with subsidized pricing, Chinese technology has become a very attractive alternative to its Western competitors in the American and European market. The suspected predatory nature of such technology has to do with its security implications. In Africa, Chinese technology was used to build the computer network for the African Union. The network included a backdoor that allowed China to download and transfer confidential data back to Beijing for nearly five years.[12] Additionally, many in the West point to a 2017 Chinese intelligence law which stipulates that "all organizations and citizens shall, in accordance with the law, support, cooperate with, and collaborate in national intelligence work, and guard the secrecy of national intelligence work they are aware of."[13] Law or no law, every Chinese company and citizen is at the behest of the Chinese Communist Party (CCP) leadership. But the law conveniently provides written proof that Chinese technology could be used as a tool for the CCP to gain critical access to Western infrastructure, data, and information. And as China marches on toward 2025, its close relationship with its tech companies will ensure its leaders retain a technological literacy—because their relationship requires it. In the Chinese political system, Chinese technology companies are essentially arms of the government. These companies "are increasingly co-opted into national policy," and "have even been assigned roles in government strategy documents,"[14] which necessitates a deeper knowledge.

Both Russia and China have a dangerous acumen for utilizing technology as a geopolitical tool, and this constitutes a real challenge for transatlantic policymakers. Ultimately, open societies like Germany and the United States will always be more susceptible to external threats than countries like Russia and China. But openness and freedom have always been worth fighting for, making it critical that we are prepared to continually do so. Ensuring policymakers in the United States and

Germany possess a deep technological literacy is paramount to inspiring the informed political debate necessary to combat this challenge.

## Combatting Disinformation on Social Media

Western attempts to properly comprehend and subsequently regulate content on social media platforms have fallen flat. This is most glaring in the United States. The U.S. regulatory environment provided ideal conditions for the Russian campaign to succeed. The United States' 1996 amendment to the U.S. Communications Decency Act chose not to hold social media platforms responsible for content published by third parties (with exceptions for illegal content such as violence, child pornography, or copyright infringement). Third parties—such as public authorities—are the ones required to notify the social media platform of its content's illegality.[15] While the U.S. government could have hardly foreseen the vulnerability social media would constitute to open societies, its susceptibility to Russian disinformation is now clear and present. Yet little has been done to update the lax regulatory environment. Instead, the policy prescriptions to address Russian disinformation have presented real questions over whether policymakers understand the evolving nature of the disinformation threat.

The focus of the U.S. response has been on efforts to increase transparency over who buys political advertisements on social media platforms. The Russian Internet Research Agency (IRA), the Kremlin-backed troll factory weaponized in Russian disinformation campaigns,[16] was well known to have used ads on both Facebook and Google to advance its goals.[17] U.S. legislators believe that increasing transparency about those advertisements will help counter interference efforts. This legislation is entitled "The Honest Ads Act," a bipartisan bill which would require all digital platforms with 50 million or more monthly users to keep a public file containing the details of all election-related communication purchased by a group or entity that spends over $500 on the platform. Senator Amy Klobuchar, one of the bill's sponsors, released a statement arguing that the legislation is meant to "protect our democracy and prevent this kind of [foreign] interference from ever happening again."[18] Increased transparency is always a worthy endeavor, and the legislation will prove useful in pulling political advertising out of the dark. Yet its characterization as being a solution to curb foreign interference is indicative of an inability to understand how Russian actors' use of the technology is changing. The ads purchased during the run-up to the 2016 election were primarily bought from Russian IP addresses and paid for in Russian rubles.[19] The Honest Ads Act is meant to expose that behavior, and thus make it more difficult for disinformation campaigns to fool unsuspecting viewers.

Unfortunately Russian tactics are, again, ahead of U.S. policy prescriptions. Facebook has already indicated that since the 2016 election, the Russian IRA-linked accounts "have used VPNs to hide their locations and paid third parties to purchase ads on their behalf."[20] If Facebook cannot track those efforts, a public file is useless for countering Russian interference. Additionally, an extensive report from the University of Oxford on the IRA's use of social media in the United States demonstrated that "the most far reaching IRA activity is in organic posting, not advertisements," and showed that those efforts "increased substantially after the [2016] election."[21] Therefore, the U.S.' current legislative approach is not focusing on the crux of the problem. As Claire Wardle, executive director of First Draft, a nonprofit organization based at the Harvard Kennedy School that combats disinformation, has noted, "at a policy level, the conversation that people are having is based on what happened in 2016. The challenge is that politicians have almost no knowledge of how these platforms actually work."[22] It is a case of the regulatory dialectic, a term coined by Professor Edward Kane in the 1980s describing the way in which "financial institutions found innovative ways to circumvent regulations designed to restrict their behavior."[23] We are seeing this dialectic in action when it comes to attempts to regulate disinformation online: nefarious Russian actors are showing the same innovative spirit in their navigation of Western social media platforms. Without a better understanding of the platforms themselves, U.S. policymakers are doomed to always be one step behind.

## 5G

In Germany, no issue has divided Berlin and Washington more than the question of whether including Chinese technology into Western 5G networks constitutes a security risk. 5G will revolutionize everything from manufacturing to kitchen toasters, and enable other more complicated procedures that require instantaneous data transmissions—like self-driving cars and remote surgery operations. Some have gone so far as to liken the potential effect of 5G to that of electricity in enabling unseen levels of industrial productivity.[24] Securing the network is therefore critical. Yet, if Germany's risk assessment and subsequent debate has been indicative of anything, it is that government representatives do not adequately understand the technology they are attempting to secure.

Huawei, the main Chinese technology provider, has a distinct advantage in that Chinese technology is already deeply embedded in the main German telecommunication providers' 4G network infrastructure.[25] This means that upgrading to a 5G network with European or South Korean technology would first require removing the existing Chinese infrastructure from the 4G network in order to install the new infrastructure. This is widely believed to be a very expensive and time-intensive process. Which, combined with Huawei's subsidized pricing, provides clear financial incentive to continue using Chinese technology in Germany's 5G network. This point is central to the German government's rationale in allowing providers that rely on Huawei infrastructure to be included in the 5G auction.[26] Yet this point is devoid of any substantive technological understanding, because hard facts on the subject do not exist. To date, there has been no public government reporting outlining the costs and deployment delay of switching out Huawei technology. It may well prove to be more expensive and time-intensive, but it is thus far unclear and such an important decision cannot be made on mere speculation. In fact, globally this argument is almost exclusively substantiated with rather generic figures and vague time estimates compiled by the telecommunication firms themselves—which have every incentive to keep costs low by using their existing Huawei infrastructure in building Germany's 5G network.[27]

Yet the ultimate decision not to exclude Huawei is predicated on the belief that any security risks can be properly detected. This too presents a problem. Following the British White Lab model, the German Federal Office for Information Security (BSI) established a Huawei testing center in Bonn where Huawei works in conjunction with government officials from BSI to frequently test their technology for security vulnerabilities. BSI assesses the equipment used by conducting source-code reviews, which entails examining the programming language used to run network gear and screening for possible "backdoors" that would allow Chinese intelligence officials to gain covert access.[28] The German government has essentially agreed that this testing guarantees the necessary security to allow Huawei technology to be included in the German network. Yet this decision shows little understanding for the actual technology powering 5G. 5G will be much more dependent on software, compared to 4G, which was more reliant on traditional hardware. It expects to be the first "software-driven network architecture," as while software-defined networking, or SDN, has been around for years, "its real impact in terms of flexibility and range of services available won't be felt until 5G is more widely deployed."[29] Because of this, the functionality of the system is dependent upon its latest software update.

Therefore, the focus of any testing has to be on software as opposed to hardware. And that testing must continually remain ahead of software updates—which, considering the frequency of potential updates, would be very difficult to maintain. In the United Kingdom, testing centers have already proven to be inadequately prepared. The National Cyber Security Agency's latest report on the country's Huawei testing center has already noted that "software in Huawei equipment tested in [their testing center] doesn't always match software found in products on the market."[30] It would thus be nearly impossible to ensure that every software update is adequately vetted before deployment. Even if inspections did occur, they would take significant amounts of time and, most often, involve investigating benign updates merely meant to fix bugs. Therefore, the most likely solution would mean "patch inspection and testing would have to be done after deployment,"[31] which in layman's terms means that the authorities would be searching for an intruder after they'd already been through the house.

## Offices of Technology Assessment

In both U.S. efforts to rein in Russian disinformation on social media platforms as well as Germany's grappling over whether to include Chinese technology in its 5G network, questionable political decisions highlight a dangerous technological illiteracy. Both Germany and the United States desperately need experts present and available to provide apolitical, timely, fact-based reporting and advice for lawmakers. Traditionally, Offices of Technology Assessment in Europe and the United States have provided such expertise. In the United States, the office was originally set up as a congressional agency in 1972 before it was defunded in 1995 by then-Speaker of the House Newt Gingrich.[32] In Germany, the office has existed since 1990, but has been rather ineffective at providing the necessary expertise during critical technological debates. In reinstituting the U.S. Office of Technology Assessment, revitalizing Germany's Office of Technology Assessment, and deepening transatlantic cooperation between the two, transatlantic leaders would possess the necessary expertise to produce cutting-edge policy prescriptions for countering external technological threats, and subsequently be better able to defend their democracies.

In the United States, these efforts should begin with bringing back the Office of Technology Assessment. The purpose of the office was to produce neutral, objective scientific assessments for congressional committees when requested. These were written in close consultation with leaders from industry, policy, and academia "to help Members of Congress understand and plan for the short- and long-term consequences of the applications of technology."[33] Yet perhaps its most useful function was that its staffers were frequently on Capitol Hill engaging with lawmakers. The office went beyond mere assessment reports, guarding against technological illiteracy by frequently giving informal advice, testifying before Congress, and frequently commenting on legislation. This was critical, as "the oral communication that occurred between staffers and members of Congress was crucial for promulgating the contents of OTA's reports."[34] One such example of its influence was a 1984 report that questioned the reliability of polygraph tests. The report led Congress to enact limits on their use by employers.[35] Today, any U.S. government research regarding technology is currently housed within the Government Accountability Office (GAO), specifically in its Science, Technology Assessment, and Analytics (STAA) team. Yet STAA is part of a much larger mandate, housed within GAO, which gets about 800 requests from Congress a year (on a large range of topics) and gives priority to reviews mandated by law, conference reports, and then requests from congressional committee leadership.[36] This makes it very difficult to ensure that the pressing technological issues are getting the attention they deserve. For this reason, those suggesting reviving the OTA, like Rep. Mark Takano, have argued that the OTA would "be [better] responsive to immediate questions and the needs of members and staff,"[37] something that is desperately needed and unavailable within the current structure. Yet more importantly, restoring the OTA as its own congressional agency and untangling technological research from the web of GAO bureaucracy would be an important step toward recognizing the importance emerging technologies and technological literacy holds in an American future.

In Europe, it was not long before countries began taking notice of the United States' Office of Technology Assessment and copying the model to ensure their legislators were equally informed on pertinent technological developments. In Germany, the Office of Technology Assessment (TAB) at the German Bundestag was created in 1990 to independently advise lawmakers. TAB is operated by the Institute for Technology Assessment and Systems Analysis (ITAS) in the Karlsruhe Institute of Technology (KIT).[38] The office is composed mostly of academics and researchers,[39] and produces reports in accordance with an agenda set by the German Bundestag's committee for Education, Research, and Technology Assessment. The office has published over 160 reports since its founding, and most recently has completed studies on autonomous vehicles and energy storage systems.[40] Yet it has not always been as effective as it should. Its work on 5G is a perfect example. While the German debate has been starved of technological expertise, TAB's report on 5G is expected "at the earliest in 2020," that is, after the 5G auction has been completed, the technology providers have been selected, and the technology is already in use.[41] For this reason, Germany's Office of Technology Assessment is well in need of an update.

## Fostering Transatlantic Technological Literacy

In reinstating the U.S. OTA and updating Germany's TAB, these offices should prioritize three points in order to maximize their value. The first is to ensure they are maintaining a presence within the policymaking community. One thing that made the initial American venture so successful was its capacity to provide informal advice by being consistently present on Capitol Hill and engaging with lawmakers. Both offices should be much more than their reports. Cultivating relationships with legislators and their staffers is a necessity. One way to do this would be by giving the offices more say in the research agenda. While Congress and the Bundestag should continue directing the agenda of their respective technology assessment offices, the offices themselves should have an input in that agenda. If it can assumed that legislators do not adequately understand emerging technologies, they are unlikely to have a sense of which technologies merit closer consideration. This input should in no way supersede the direction of the legislators, but rather help ensure that the agenda stays ahead of impending technological dilemmas. It would help safeguard any potential for repeating the German 5G experience, where the debate is completed before the assessment from TAB arrives. It could also guarantee the offices are focusing on the necessary research questions. For Germany's 5G network, this would include an extensive analysis of the costs and delay associated with removing Huawei hardware. It would also provide a more extensive overview of the technology's most important elements, to ensure government security testing is adequately suited to 5G technology. Bringing office staffers into the agenda-making process would help build more substantive relationships with policymakers to ensure the effectiveness of these offices' advisory role and better position legislators to gauge technological developments.

Second, and perhaps most importantly, these offices should cultivate private partnerships. In the field of emerging technologies, when it comes to 5G and social media platforms, the experts are most often in the private sector. The West is not doing enough to cultivate these relationships. Google's decision to refuse to work with the Pentagon on artificial intelligence while concurrently building a Chinese search engine is indicative of this reality.[42] Foremost, there should be a concerted effort on both sides of the Atlantic to bring more actors with industry experience into these offices as staffers. The offices cannot be staffed exclusively with academics. Additionally, the offices should provide a much-needed bridge between government and the private sector. While the relationship between the two is increasingly rather sour, there is nevertheless an opportunity for increased collaboration. For instance, Mark Zuckerberg has asked regulators and governments to work closely with Facebook to ensure they have a more active role over controlling Internet content.[43] Yet, tech companies' chief complaint in prior attempts to do so has been that government officials do not fully understand the technology their companies operate. Relying on technology assessment offices to act as an intermediary would help alleviate that concern. Industry professionals would be talking to experts that understand their technology. And having cultivated relationships with the legislators, the offices could provide a trusted neutral platform for encouraging collaboration and understanding between private industry actors and government officials.

Last, despite transatlantic leaders' seeming inability to work with one another, encouraging collaboration between a newly reinstated American OTA, the German TAB, and other European technology assessment bodies would require little political capital and pay dividends. The current collaborating body is the European Parliamentary Technology Assessment Partners, which has twelve members (including Germany's TAB), and ten associate members (including the U.S.' STAA).[44] While there is an annual meeting, project collaboration is limited to a database collecting each country's published reports. This collaboration should increase. There should be a more robust exchange of best practices, particularly in how to effectively engage with policymakers in an advisory role. Additionally, more effective collaboration would involve conducting cooperative transatlantic projects addressing technologies that challenge Western democracies. One such idea would be a transatlantic report on Russian disinformation campaigns, focusing first on the technology driving social media platforms and how the Russian technological toolbox has developed in reaction to legislative proposals on both sides of the Atlantic. Considering the national security element to such a project, expanding the partnership to include NATO's Science and Technology Organization would provide the necessary security perspective. This would enhance assessment reports by ensuring research and expertise appreciates the security dimensions that new technologies continually present, and focusing in on transatlantic collaboration would foster cooperative responses to common threats.

## Conclusion

Ultimately, addressing the problems of the next generation will continue to be dependent upon understanding emerging technologies. And the future does not look brighter than the recent past. Ongoing efforts to comprehend artificial intelligence have not proven any more inspiring. In the U.S., continuing efforts to regulate biases in AI algorithms have been hampered by how few legislators possess "a deep enough technical grasp of data and machine learning to approach regulation in an appropriately nuanced manner."[45] And in Germany, experts have criticized the country's AI strategy, noting its "considerable need for further development,"[46] while the government ministries have failed to explain what the strategy's allocated funds will be used for.[47] These technological issues are not going away. It is thus imperative that lawmakers are technologically literate for the future. Russian and Chinese leadership already is, and transatlantic leaders cannot fall further behind. U.S. and European democracies need government institutions prepared to support this process. Reinstituting the Office of Technology Assessment (OTA) in the United States and revitalizing its German equivalent (TAB) will go a long way to guaranteeing American and German lawmakers are provided with the timely, informed analysis they require to face these challenges. And in deepening a transatlantic relationship between U.S. and European offices, policymakers will be better positioned to engage one another with a similar understanding of the technological intricacies fundamental to many analogous challenges.

But technological advice can only go so far. The focus of such an effort is ultimately to ensure informed debate. These dilemmas most often come down to addressing fundamental political questions. The decisions over how best to regulate content on social media platforms is closely tied to free speech. Equally, navigating the fine line between ensuring fair business competition and adequately mitigating security risks is something the government is meant to decide. No technological report or advice will supplant that reality. But legislators on both sides of the Atlantic will be ill-prepared to make the right decisions without an extensive understanding of the technology behind the issues they are meant to address. In a time of transatlantic strife, this is something both Europe and the United States can work together to guard against. And as technology increasingly reflects societal values,[48] perhaps a deeper understanding of technology will help remind transatlantic lawmakers that their values are not as far apart as the current rhetoric suggests.

## Notes

[1] “Trump calls European Union a ‘foe’ – ahead of Russia and China,” *The Guardian*, July 15, 2018, https://www.theguardian.com/us-news/2018/jul/15/donald-trump-vladimir-putin-helsinki-russia-indictments

[2] Morgan Gstalter, “Merkel: Germany can’t rely ‘on the superpower of the US’ anymore,” *The Hill*, July 20, 2018, https://thehill.com/policy/international/398025-merkel-we-cant-rely-on-the-superpower-of-the-us-anymore

[3] Federal Foreign Office, “Speech by Federal Foreign Minister Heiko Maas at the luncheon held by the American Council on Germany (ACG) on ‘Germany, Europe and the United States: A strategic partnership facing new challenges?’” April 1, 2019, https://www.auswaertiges-amt.de/en/newsroom/news/maas-american-council-on-germany/2205634

[4] “European Tech Insights 2019,” Center for the Governance of Chance, 2019, http://docs.ie.edu/cgc/European-Tech-Insights-2019.pdf

[5] Krishnadev Calamur, “What is the Internet Research Agency,” *The Atlantic,* February 16, 2018, https://www.theatlantic.com/international/archive/2018/02/russia-troll-farm/553616/

[6] Tim Mak, “Troll Factory Contributes to Russia’s Worldwide Interference,” *NPR*, December 12, 2018, https://www.npr.org/2018/12/12/675987838/russias-worldwide-interference

[7] “The IRA, Social Media and Political Polarization in the United States, 2012-2018,” Computational Propaganda Research Project, December 2018, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf

[8] Laura Rosenberger and Thomas Morley, “Russia’s Promotion of Illiberal Populism: Tools, Tactics, Networks,” Alliance to Secure Democracy, March 11, 2019, https://securingdemocracy.gmfus.org/russias-promotion-of-illiberal-populism-tools-tactics-networks/

[9] “EU intel: Russia is using social media to influence EU elections,” *DPA International*, April 13, 2019, http://www.dpa-international.com/topic/eu-intel-russia-using-social-media-influence-eu-elections-190413-99-808460

[10] Matt Apuzzo and Adam Satariano, “Russia is Targeting Europe’s Elections. So are Far-Right Copycats,” *The New York Times*, May 12, 2019, https://www.nytimes.com/2019/05/12/world/europe/russian-propaganda-influence-campaign-european-elections-far-right.html

[11] Amy Zegart and Michael Morell, “Spies, Lies, and Algorithms,” *Foreign Affairs*, April 16, 2018, https://www.foreignaffairs.com/ articles/2019-04-16/spies-lies-and-algorithms

[12] John Aglionby, “African Union accuses China of hacking headquarters,” *Financial Times*, January 29, 2018, https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5

[13] Danielle Cave, “Huawei highlights China’s expansion dilemma: espionage or profit?” *Aspi Strategist*, June 15, 2018, https://www.aspistrategist.org.au/huawei-highlights-chinas-expansion-dilemma-espionage-or-profit/

[14] Louise Lucas, “The Chinese Communist party entangles big tech,” *Financial Times*, July 19, 2018, https://www.ft.com/content/5d0af3c4-846c-11e8-a29d-73e3d454535d

[15] Konrad Niklewicz, “Weeding out Fake News,” Martens Centre, 2017, https://martenscentre.eu/sites/default/files/publication-files/mc-weeding_out_fake_news_v3_web.pdf

[16] Krishnadev Calamur, “What is the Internet Research Agency,” *The Atlantic*, February 16, 2018, https://www.theatlantic.com/international/archive/2018/02/russia-troll-farm/553616/

[17] Computational Propaganda Research Project, “The IRA, Social Media and Political Polarization in the United States, 2012-2018,” December 2018, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf

[18] Maggie Miller, “Bipartisan group of senators seeks to increase transparency of online political ads,” *The Hill*, May 8, 2019, https://thehill.com/homenews/senate/442598-bipartisan-group-of-senators-seek-to-increase-transparency-of-online.

[19] Issie Lapowsky, “Fake Facebook Accounts Are Getting Harder to Trace,” *Wired*, July 31, 2018, https://www.wired.com/story/facebook-uncovers-new-fake-accounts-ahead-of-midterm-elections/

[20] Ibid.

[21] “The IRA, Social Media and Political Polarization in the United States, 2012-2018,” Computational Propaganda Research Project, December 2018, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf

[22] Mark Scott, “Why we’re losing the battle against fake news,” *Politico*, October 7, 2018, https://www.politico.eu/article/fake-news-regulation-misinformation-europe-us-elections-midterms-bavaria/

[23] Robert Eisenbeis, “TNB and the Regulatory Dialectic,” Cumberland Advisors, December 13, 2018, https://www.cumber.com/tnb-and-the-regulatory-dialectic/

[24] Zheping Huang, “How 5G will unlock the industrial internet, driving another dimension of mobile connectivity,” *South China Morning Post*, May 2, 2019, https://www.scmp.com/tech/big-tech/article/3008594/how-5g-will-unlock-industrial-internet-driving-another-dimension

[25] “Warnungen vor Technik aus China kommen zu spat,” *t-online.de*, March 20, 2019, https://www.t-online.de/digital/sicherheit/.id_85435490/huawei-zte-und-co-warum-deutschland-nicht-mehr-auf-technik-aus-china-verzichten-kann.html

[27] “Vodafone says complete UK ban on Huawei would cost it millions of pounds,” *Reuters*, March 7, 2019, https://www.cnbc.com/2019/03/07/reuters-america-vodafone-says-complete-uk-ban-on-huawei-would-cost-it-millions-of-pounds.html

[28] Douglas Busvine, “Exclusive: China’s Huawei opens up to German scrutiny ahead of 5G auctions,” *Reuters*, October 23, 2018, https://www.reuters.com/article/us-germany-telecoms-huawei-exclusive/exclusive-chinas-huawei-opens-up-to-german-scrutiny-ahead-of-5g-auctions-idUSKCN1MX1VB

[29] Bob O’Donnell, “Opinion: The many paths and parts to 5G,” *Techspot*, September 11, 2018, https://www.techspot.com/news/76375-opinion-many-paths-parts-5g.html

[30] Lauren Cerulus, “UK intelligence finds ‘new risks’ linked to Huawei,” *Politico*, March 28, 2019, https://www.politico.eu/article/uk-intelligence-finds-new-risks-linked-to-huawei/

[31] Herb Lin, “Huawei and Managing 5G Risk,” *Lawfare Blog*, April 3, 2019, https://www.lawfareblog.com/huawei-and-managing-5g-risk

[32] Nancy Scola, “On Democrats’ wish list: Tech help for a clueless Congress,” *Politico*, December 29, 2018, https://www.politico.com/story/2018/12/29/democrats-technology-congress-1074187

[33] Jathan Sadowski, “Office of Technology Assessment: History, implementation, and participatory critique,” *Science Direct*, 2015, https://www.sciencedirect.com/science/article/pii/S0040162596001850

[34] Ibid.

[35] Celia Wexler, “Bring Back the Office of Technology Assessment,” *The New York Times*, May 28, 2015, https://www.nytimes.com/roomfordebate/2015/05/28/scientists-curbing-the-ethical-use-of-science/bring-back-the-office-of-technology-assessment

[36] Jory Heckman, “Freshman congressman: Axing Office of Tech Assessment made us ‘dumber as a nation,’” *Federal News Network*, April 5, 2019, https://federalnewsnetwork.com/technology-main/2019/04/freshman-congressman-axing-office-of-tech-assessment-made-us-dumber-as-a-nation/

[37] Ibid.

[38] Julia Hahn and Miltos Ladikas, “Constructing a Global Technology Assessment: Insights from Australia, China, Europe, Germany, India and Russia,” KIT Scientific Publishing, March 6, 2019, https://www.ksp.kit.edu/9783731508311

[39] Büro für Technikfolgen-Abschätzung Beim Deutschen Bundestag, “Team,” http://www.tab-beim-bundestag.de/de/team/index.html

[40] “Publikationen 2019,” ITAS, http://www.itas.kit.edu/pub/l/j/lit19.htm

[41]“Interview mit Peter Hensinger zum 5G-Projekt: Analysen zur digitalen Transformation,” *diagnose:funk*, March 17, 2019, https://www.diagnose-funk.org/publikationen/artikel/detail&newsid=1354

[42] Amy Zegart and Michael Morell, “Spies, Lies, and Algorithms,” *Foreign Affairs*, April 16, 2018, https://www.foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms

[43] "Mark Zuckerberg asks governments to help control internet content," *BBC News*, March 30, 2019, https://www.bbc.com/news/world-us-canada-47762091

[44] European Parliamentary Technology Assessment, https://eptanetwork.org/.

[45] Karen Hao, "Congress wants to protect you from biased algorithms, deepfakes, and other bad AI," *Technology Review*, April 15, 2019, https://www.technologyreview.com/s/613310/congress-wants-to-protect-you-from-biased-algorithms-deepfakes-and-other-bad-ai/

[46] Barbara Gillmann, "Keine Pläne für KI – Bundesregierung ist im "Tiefschlaf", sagen die Grünen," *Handelsblatt*, April 22, 2019, https://www.handelsblatt.com/politik/deutschland/kuenstliche-intelligenz-keine-plaene-fuer-ki-bundesregierung-ist-im-tiefschlaf-sagen-die-gruenen/24234870.html

[47] Ibid.

[48] Thomas Wright, "Democrats Need to Place China at the Center of Their Foreign Policy," *The Atlantic*, May 14, 2019, https://www.theatlantic.com/ideas/archive/2019/05/how-democrats-can-beat-trump-foreign-policy-2020/589360/