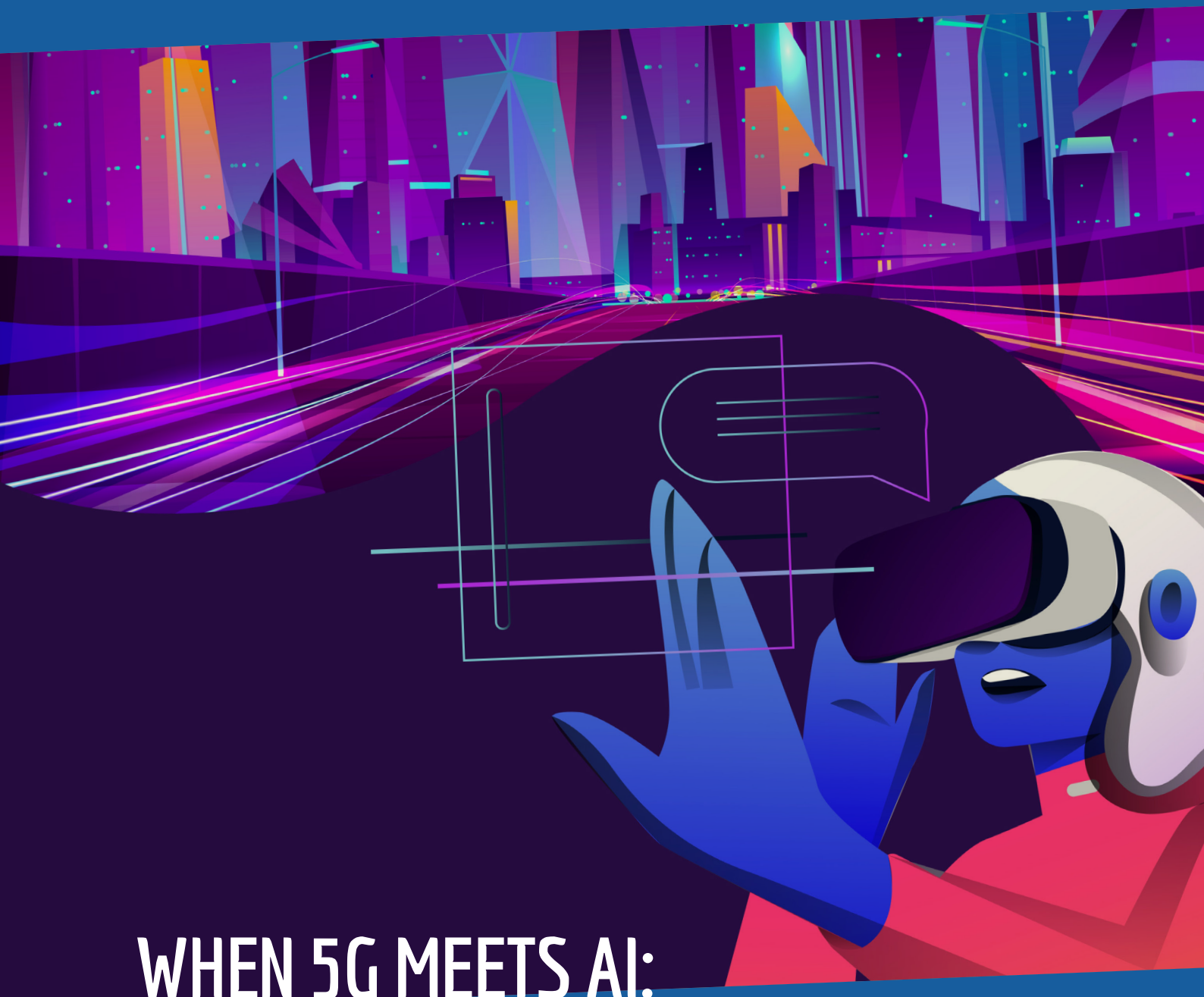
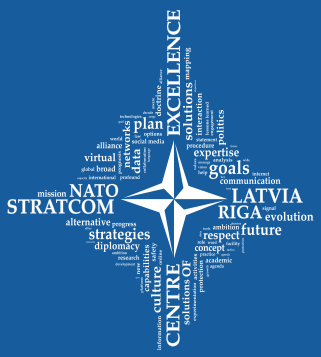
ISBN: 978-9934-619-04-5



WHEN 5G MEETS AI:
NEXT GENERATION OF COMMUNICATION AND INFORMATION SHARING

Published by the
NATO Strategic Communications
Centre of Excellence



Digital: 978-9934-619-04-5
Print: 978-9934-619-03-8

Author: Katarina Kertysova
Contributors: Gundars Bergmanis-Korāts and Gabriella Gricius
Copy Editing: Leonie Haiden
Design: Linda Curika

Author's Acknowledgments: The author is grateful to Eline Chivot, Christopher Painter, Sir Graham Stacey, Robert Strayer, and NATO StratCom CoE staff for their input and review of earlier versions of this study. Any errors and omissions are the sole responsibility of the author.

Riga, February 2021
NATO STRATCOM COE
11b Kalnciema Iela
Riga LV1048, Latvia
www.stratcomcoe.org
Facebook/stratcomcoe
Twitter: @stratcomcoe

TABLE OF CONTENTS

INTRODUCTION

The adoption of fifth generation (5G) wireless technology will touch nearly every aspect of our lives. While changes brought by 5G will primarily affect sectors that depend on smooth wireless connection – such as transportation, healthcare, or manufacturing – they will also alter the realm of (strategic) communications. In the coming decade, 5G and edge computing will generate new opportunities for how humans interact with each other and experience the world.[1] Greater connectivity and access to information enabled by 5G also promise to bridge the digital divide, improving democratic participation and citizen mobilization.

At the same time, there will be more opportunities for misuse of this technology. Events of the last ten years have demonstrated the impact that digital transformation is having on democracy and political life. Consider the role that social media has played in key political events such as the Arab Spring or how the advent of e-voting and e-political participation changed the outcome of some elections throughout the pandemic. The emergence and accelerated adoption of new technologies has seen a concurrent rise in digital repression and disinformation operations. While (online) disinformation is not a new phenomenon, rapid advances in information technologies have altered the ways in which information (and disinformation) can be produced and disseminated.[2] Data capture, speed, and connectivity offered by 5G will equip both state and non-state actors with more effective tools to tighten information control, repress political opponents, and manipulate public opinion online.

In recent years, both 5G and AI have received considerable attention. However, there has been little focus on the complexities presented by AI and 5G operating together in the context of communications and information operations. This study will cover this gap. Many studies of 5G highlight the technical risks posed by Chinese companies manufacturing 5G equipment. In contrast, this paper seeks to answer the following questions: *How are NATO Allies impacted by the 5G/AI revolution? How will 5G transform the information environment, including the nature of disinformation campaigns?*

To do so, this paper first examines the ways in which 5G-enabled applications alter the realm of communications: not only how we communicate, but also how we consume and share information. It then briefly identifies implications 5G can have for democracy and political life in general. Next, it outlines broader systemic threats and negative impacts of 5G rollout on political participation. The paper concludes with a set of recommendations.

5G AND THE NEXT GENERATION OF COMMUNICATION AND INFORMATION SHARING

As 5G continues to expand, it is altering not only how we communicate and connect with others, but also how we consume and share information. The connectivity benefits of 5G are giving consumers access to more information than ever before. With 5G, download speeds and data transfer are much faster – as much as ten times faster than the current 4G LTE. Since data can be transferred faster, the volume of information that can be exchanged in the same amount of time is higher too.[3] The available bandwidth makes it possible for 5G to handle many more connected devices and users than previous networks.[4] Put simply: no more network congestion in crowded areas. 5G is also designed to significantly reduce latency. Latency is the amount of time it takes for a mobile phone (or other connected device) to make a request to a server and receive a response. This allows machines to communicate and exchange data almost in real-time.[5]

What are the applications of this – apart from better gaming and other super-fast streaming services? First, 5G is enhancing **video-calling applications**. The first wave of video calls over 5G has been on phones. In the long run, 5G will be able to support high-definition (HD), 4K, and even 5K video streams to be exchanged between 5G-enabled augmented reality (AR) and virtual reality (VR) devices in real time.[6] In addition to improved video and voice calls, 5G networks will shift communication from 2D to 3D, enabling users to talk with a **hologram** of another person in real time. Holographic projection technology has already been tested in videoconferencing, museums, as well as to 'holoport' musicians in different geographic locations onto a virtual stage, or to replace wild animals with 3D projections in circuses. In the military realm, this technology is already helping military planning and training by simulating combat or transmitting 3D maps of battlefields. It can also be used for explosives disposal purposes, post-blast IED forensics, and weapon system modelling.[7] As 5G continues to improve, interactions will not feature delays, and voice, movement, and expression will become more vivid and natural. Researchers from MIT have already begun experimenting with deep learning to accelerate computer-generated holography, enabling real-time generation.[8] Although weaponization of this technology is not quite as developed, the idea of the 'Face of Allah weapon' – a hologram of God that could be projected onto a battlefield to raise fear – attests to the fact that holograms could theoretically also be used as a tool of war.[9]

In addition, 5G is expected to enable new applications such as **extended reality** (XR) – a generic term that encompasses all immersive technologies (VR, AR, and mixed reality). From improved training and situational awareness, through logistics support and combat readiness, to medical training and treatment of trauma, extended reality offers the military considerable opportunities. The Latvian National Armed Forces, for example, have recently set up a 5G military test site to explore applications such as VR/AR simulated medical training, support for unmanned aerial vehicles, and virtual training for military personnel.[10] While already advanced, current AR and VR applications face a variety of limitations including latency, slow communication speeds, and lack of full immersion – all of which will be solved with 5G.

5G rollout will also enable new kinds of **mobile video production**. Live streaming from smartphones is already popular and widely used for applications such as TikTok and Instagram. With 5G-enabled cameras and multiple audio channels, anyone will be able to download, upload, capture, and stream more media – in HD and faster.[11] Such content will then be experienced on the screens of phones, tablets, and TVs or on VR and AR headsets. With more immersive tools, addiction to smartphones and social media is set to increase, too.[12]

5G also promises to revolutionize **digital journalism**, transforming the way news is produced, distributed, and consumed. With 5G, the production and delivery of breaking news stories and other live events will change significantly. First, higher and faster bandwidth is transforming the way journalists gather their news, by enhancing their ability to capture and immediately transfer high-resolution media back to the newsroom at a decreased cost.[13] Second, 5G will unlock new ways for news organizations to deliver more dynamic storytelling formats (in an immersive 3D format) and enable readers to experience such reporting in extraordinary detail.[14]

As well as aiding professional journalists, 5G will enhance the potential and impact of **citizen journalism**. With stable connectivity, especially in areas with heavy network traffic that experience congestion issues on 4G, users will be able to share on-the-ground content with their followers or directly with a news team in near real-time and with higher quality.[15] While news organizations will be able to (and possibly come under increasing pressure to) source user-generated content faster than before, they will potentially have less time to verify sources. Not just news, but also disinformation that journalists must sift through will travel faster and spread more widely in the era of 5G. Today's oversaturation of the Internet with information, however, begs the question whether 5G will have a sizable impact on our (in)ability to evaluate the veracity of news and assess every piece of information we come across critically.

Several communications and media companies have teamed up with 5G developers to test this technology and showcase its potential applications. In 2019, for instance, the New York Times in collaboration with Verizon launched a 5G Journalism Lab to explore the future of 5G and journalism. One creation of

> *Today's oversaturation of the Internet with information, however, begs the question whether 5G will have a sizable impact on our (in)ability to evaluate the veracity of news and assess every piece of information we come across critically.*

the 5G Journalism Lab is *Beam*, a photography app that allows journalists instantaneous interaction with their editors back in the newsroom with nothing but their smartphone and camera.[16] With *Beam*, journalists can move from one site to another as events unfold, capture and immediately transfer high-resolution media to the newsroom without having to stop and open their laptops. Another outcome of this collaborative initiative has been the reconstruction of journalistic scenes in 3D, using a technique called *environmental photogrammetry.*[17] This fully immersive experience enables readers to move through a whole space as if they were there – not dissimilar to moving around in a video game.

As a 'network of networks', 5G can also include satellites. With 5G we will be able to do all satellite communications and remote sensing in real-time. This will help militaries and the civilian sector alike to optimize their logistics and situational awareness.[18] Domain awareness is set to improve, too. 5G, AI, and edge computing will enable real-time processing of more data from numerous sensors (like aircraft, ships, ground-based radars, and satellites), integrating systems across all domains. With Joint All-Domain Command and Control (JADC2), commanders should be able to make better-informed decisions by collecting data from all the military services, turning that data into actionable information using AI algorithms, identifying targets, and then recommending the optimal weapon (both kinetic and non-kinetic) to engage the target.[19] Under the oversight of US aerospace and weapons manufacturer Lockheed Martin, 5G capabilities are also being built to connect and remotely control weapons from low-earth orbiting (LEO) satellites as well as to advance space exploration, which has historically been hindered by difficulties in processing large amounts of data.[20]

DEMOCRATIZING POWER OF 5G

The effects of 5G rollout on democracies will be significant. In the words of Rumana Ahmed et al.: 'any 5G-backed technology promises to increase the scope and scale of its democratizing power to influence information spaces, civic participation, and human rights'.[21] First, 5G can use more of the radio spectrum than earlier networks – even low-band spectrum that previously has been used to deliver services such as TV broadcasting. A benefit of the low-band is that in this frequency range data can move at rates up to several times faster than 4G. This will allow people in underserved communities, who previously had no reception with 4G, to now have a reliable, fast broadband service at home.[22] Second, OneWeb's satellite communication network is being developed to interoperate within a 5G architecture. 5G-enabled satellites promise to deliver fibre-like connectivity to rural and hard-to-reach areas that are not covered by small cells.[23]

With improved connectivity, marginalized communities will gain greater access to information, educational tools, and other societal benefits.[24] Where governments are committed to delivering the right infrastructure (such as broadband connectivity and good mobile coverage) to rural areas, 5G promises to bridge the growing digital divide that particularly affects women, persons with disabilities, and rural communities.

Because 5G enables greater connectivity and access to digital technologies, it offers a great potential to support activism, civil mobilization, and the dissemination of information. When it comes to electoral processes, it is expected that 5G will push e-voting and widen political participation, especially in socially and geographically marginalized areas.[25] Should increased e-voting and, in tandem, increased access to 5G be implemented, higher voting activity could be possible. Digitizing elections will also enable real-time and more accurate voting statistics.

Regarding education, 5G promises to enhance the quality of the entire learning experience. From improved interaction between students and teachers through the integration of immersive technologies into classrooms, to personalized learning that reflects the unique needs of each student, 5G is set to transform both teaching and learning.[26] Perhaps most importantly, 5G could level the playing field by democratizing access to quality education for low-income students and under-resourced classrooms.

This would, however, be subject to students' ability to access 5G networks in the first place and, by extension, the availability of (state) funding to equip all students with the necessary digital devices for home learning. In August this year, Verizon Innovative Learning launched a free online education portal, leveraging 5G-enabled AI, VR, and AR to address issues such as lack of student engagement, teachers' expertise, and the need for more immersive and targeted support for students with special needs.[27] This project, which presents a good roadmap for future experiments with 5G and education, was being implemented in 511 schools across the United States at the time of writing this report.

The COVID-19 pandemic is believed to have changed education forever by having forced a sudden transition to online teaching.[28] In the event of future pandemics, 5G technology could help both students and teachers to better cope with remote learning. Particularly in densely populated urban areas, greater bandwidth, which 5G can deliver, will be needed to handle many more connected devices and users.

BROADER SYSTEMIC THREATS AND NEGATIVE IMPACTS ON DEMOCRACY AND CIVIC PARTICIPATION

Digital repression

While 5G can expand information access and bolster democracy, it can also be used to tighten information control and fuel digital repression. Digital repression can be defined as 'the use of information and communications technology to surveil, coerce, or manipulate individuals or groups in order to deter specific activities or beliefs that challenge the state'.[29] Because of its speed, connectivity, and ability to gather larger quantities of user data, 5G might well enhance existing abilities of authoritarian regimes to exercise digital control today. These include, but are not limited to, techniques such as surveillance, online censorship, social manipulation, disinformation, internet shutdowns, and targeted persecution of online users.[30] As Rumana Ahmed et al. observe, '5G adoption in a country inclined toward authoritarianism makes autocrats more effective and efficient […] in expanding the scope and scale of illiberal capabilities'.[31]

5G is also expected to augment future AI-enabled information warfare. Influencing information to exert power and control is not a novel phenomenon. For hundreds of years, states and state-sponsored actors have deployed strategies to control information and shift public opinion in their favour. With the advent of the internet and social media, traditional techniques (i.e., print media, radio, television, and movies) extended into the digital realm, resulting in a qualitatively different landscape of persuasion and mass manipulation.[32] New technologies – particularly the use of algorithms, automation, and AI – are giving a further boost to the scale, scope, efficiency, and sophistication of manipulation of public opinion online.[33] Looking ahead, 5G-enabled AI applications and real-time citizen information may enable autocrats to deploy subversive disinformation campaigns with greater reach to provoke fear, fuel polarization and political disengagement, or to influence

voters. However, it remains to be seen whether the quantitative shift brought about by 5G will translate into seismic qualitative changes, ushering in another major communications revolution.

Mass surveillance

With 5G, the amount of data that will be collected, transferred, and stored – and the speed with which that data can be used – will increase exponentially. This will benefit AI systems, which need large training datasets to improve in accuracy and performance.[34]

According to the AI Global Surveillance (AIGS) Index of the *Carnegie Endowment for International Peace*, at least 75 countries currently employ AI technologies for surveillance purposes.[35] Such technologies include smart policing, smart city platforms, and facial recognition systems. On the one hand, deployment and integration of surveillance technologies such as sensors and biometric data collection systems can help law enforcement agencies as well as governments to deliver services and make cities smarter. On the other, the same technologies can be used for espionage purposes and illicit activities – such as spying on political opponents, civil society activists, and independent journalists, locating citizens without warrants, intimidating those who challenge the state into silence, or engineering crackdowns against targeted populations. The Chinese crackdown on the Uighur minority is exemplary of the extent to which mass surveillance, enabled by AI, can fuel discrimination and racial profiling, and exacerbate human rights abuses.[36] Together, 5G and AI will dangerously increase the scale to which governments can extend mass surveillance by combining edge computing and 5G networks. Rumana Ahmed et al. warn that when such technologies are exported, China's model of data governance could 'further empower autocracies and threaten civil society, journalists, and activists who work towards inclusive and responsive democracies'.[37]

It is important to note that while AI technologies directly support surveillance objectives, 5G can be classified as an 'enabling technology' that is critical to AI functioning but not directly responsible for surveillance programs.[38]

Enhanced user profiling and micro-targeting

As previously mentioned, 5G will make it easier to extract, store, and transfer more personal data than was possible with earlier generations of networks. In addition, it will enable automatic collection of *new kinds* of user data, like more precise localization, biometric, and sensorial data that could be used for nefarious purposes

Thanks to 5G, marketers and (political) advertisers will also be able to gather larger quantities of consumer data than ever before and subsequently target a greater number of individuals with relevant and hyper-personalized messages. Eventually, they might be able to reach their target audiences in real-time, at a greater scale, and drive conversations as well as engagement in ways that were previously impossible. AR and VR further promise to revolutionize political campaigning by creating

more meaningful and immersive experiences.[39] 5G will significantly improve such applications. Political messaging will be more effective and the potential to reach and engage with large voter masses will increase considerably.[40] Just like the advertisers, malign actors will be equipped with better tools to target with maximum effectiveness those who are most vulnerable to influence. Depending on where this occurs, different data protection regulations and privacy laws may apply.

While user profiling and micro-targeting are not new in political campaigns, the Brexit vote and the Cambridge Analytica scandal, which rocked the 2016 US presidential election, revealed the role that targeted political advertising can play in fomenting polarization.[41] 5G-enabled AI can take psychometric profiling to the next level in terms of data availability, processing speeds, and personalization.

Regardless of what 5G can and cannot do, because it is so prevalent in the current imagination, it is, and will be, a strong tool for political campaigns. According to a 2020 report by the Reuters Institute for the Study of Journalism at the University of Oxford, high-level politicians, celebrities, and other public figures account for 20 percent of all disinformation about 5G, attracting high levels of engagement on various social media platforms.[42]

Privacy risks

5G-enabled data capture, transfer speed, and reliability come with privacy concerns. These include proliferation of user data, increased data harvesting, and telecom providers' responsibilities in handling user data.[43] Once collected, such data may be stripped of its original purpose(s) and be used for objectives the individual is largely unaware of, which is problematic from a privacy and personal data protection point of view.[44]

The EU has attempted to regulate the ways in which user data is collected, stored, and used through its flagship data protection legislation, the General Data Protection Regulation (GDPR). In particular, Article 22 of the GDPR governs automated decision-making including detection models, assessment, and automated profiling. This gives users the right not to be subject to a decision solely based on automated processing, including profiling (the so-called opt-out option). EU policymakers have argued that under the privacy law's requirements, personal data processed through automated decision-making cannot be used in political targeting.[45] In addition, Article 5 of the GDPR requires organizations to minimize the amount of data collected, and to restrict its use to its original intended purpose. Also noteworthy are Articles 13 and 15, according to which data subjects have a right to 'meaningful information about the logic involved' and 'the significance and the envisaged consequences' of automated decision-making.[46] In short, the GDPR requires consent of the data subject, transparency of any processing, limited duration of personal data conservation, anonymization, and purpose limitation.

The GDPR allows the transfer of personal data only if a country has an 'adequate level of protection', with the European Commission

Because of its speed, connectivity, and ability to gather larger quantities of user data, 5G might well enhance existing abilities of authoritarian regimes to exercise digital control today.

having confirmed Israel, Switzerland, and Japan (among others) as qualifying third countries.[47] China, which is not on the EU's third party list, must therefore ensure adequate data protection levels as well as 'enforceable rights and legal remedies' in order for its companies to be certified by the EU under GDPR. This creates a tension between GDPR and EU member states that want to continue using telecom equipment manufactured in China in their 5G networks. By providing network access to Huawei, European governments are potentially putting the data of over 500 million EU citizens at risk.[48]

Deepfakes

The application of AI to audio and video production presents an even bigger challenge. So-called 'deepfakes' – digitally manipulated audio or visual material that is highly realistic and virtually indistinguishable from real material – were initially used in the film industry for entertainment purposes. In late 2017, they first appeared on the Internet. At the beginning of 2019, Amsterdam-based cybersecurity firm DeepTrace identified 7,964 deepfake videos online. In under a year, this number had almost doubled to nearly 15,000 and rose to over 50,000 by July 2020.[49] Because this technology is improving and becoming widely accessible – with commercial and even free software already available on the open market – fake audio-visual content continues to proliferate. Almost anyone with a computer and Internet access can create such footage. With 5G-backed AI capabilities, deepfakes will have higher resolution, look more realistic, and will be easier to produce.[50] Malign actors – acting alone, collectively, or on behalf of states – will be able to manipulate audio-visual content in real time by applying deepfake technology to live video calls and conferences, as well as to live TV and other video streaming services.[51]

While the vast majority of deepfakes (96 percent)[52] are pornographic in nature, the greatest worry concerns the potential use of deepfake technology for harmful political purposes. Deceptively realistic but completely fabricated depictions of public officials doing

> *The ability to manipulate public opinion, with implications for democracy, is certainly there, just like it was with 4G. With 5G, however, the lack of trust in its architecture, alongside uncertainties about how the infrastructure operates, heightens some of those concerns.*

or saying things they never said or did could enter public discourse on a larger scale. Such deepfakes might undermine government institutions, exacerbate existing divisions in society, incite violence and civil unrest, erode voters' confidence in candidates and, crucially, influence the outcome of elections.[53] Consider the repercussions of a fake video of a government representative announcing the closure of polling places on the eve of an election, or of a president of a nuclear-armed state ordering a missile strike that goes viral before it can be explained. Although big tech companies are already investing resources and adopting policies to address deepfakes on their platforms, they continue to present real concerns for the future development of disinformation.

In the **military realm**, deepfake technology could disrupt effective military communication by producing false but convincing signal chatter on a massive scale or mimicking key individuals in the chain of command giving voice orders.[54] Also consider the implications of high-quality insurgent propaganda video for asymmetric warfare. Creating policies to address this security risk is key for NATO and its allies, as it moves forward in the realm of cyber defense.

Deepfakes make it possible for malign actors to deny the truth in two ways: not only may fake videos be passed off as real to create doubt, but authentic information can be passed off as fake.[55] This happened in 2018 in Gabon, when opponents of president Ali Bongo, who had not been seen in public for months, claimed that a video of him produced by the administration was fake, suggesting instead that he was incapacitated or dead. This speculation spread and the military attempted a coup a week later.[56]

Despite these potential dangers, a recent primer on deepfakes, published by the NATO Strategic Communications Centre of Excellence in Riga, concluded that while the threat from deepfakes is real, it is only one tool among many in the hands of malign actors. The risk posed by deepfakes is narrower than commonly suggested and may distract from

other deployments of machine learning by disinformation perpetrators that may be as, if not more, impactful than deepfakes.[57]

Cyber (in)security

5G is generally considered more secure than previous networks (2G, 3G, 4G LTE) due to better encryption[58] and the ability for network slicing, which makes potential breaches less likely and less damaging.[59] Since 5G is an evolution of 4G LTE, developers of this technology have been able to deal with weaknesses and vulnerabilities in previous networks and build security improvements into the protocol to ensure that 5G is more secure. However, that potential for extra security may not be delivered by the service providers for cost reasons. Despite increasing risk, not all manufacturers prioritize cybersecurity. Perhaps the greatest risk concerns extension of the attack surface. As connected devices proliferate in a 5G environment, the threat potential as well as new points of attack increase. Put simply, any system is only as strong as its weakest link: billions of interconnected devices with varied security also mean billions of possible breach points.[60] Given 5G's edge computing potential, this is a concern for the creators of 5G infrastructure and networks across Europe.

Most of the attention surrounding the cybersecurity of 5G networks has focused on supply **chain challenges.** Chinese companies currently lead in 5G development and Huawei dominates the global market for telecommunications equipment. In 2019, two-thirds of 5G networks outside China relied on telecom equipment manufactured in China.[61] On top of reported security vulnerabilities – such as software code deficiencies or poor oversight of its supplier networks – which could be exploited by any malign actor, concerns have also been voiced about Huawei's ties to the Chinese government and the potential risk that China might use 5G infrastructure for espionage or illicit actions (such as intellectual property theft, company sabotage, or fraud).[62] The Chinese State Security Law obliges companies to 'provide assistance with work related to state security'.[63] If critical communications, including Internet voting, come to depend on 5G networks, this will create a level of insecurity since the Chinese regime might gain access to and eventually manipulate such processes.[64] The ability to manipulate public opinion, with implications for democracy, is certainly there, just like it was with 4G. With 5G, however, the lack of trust in its architecture, alongside uncertainties about how the infrastructure operates, heightens some of those concerns.

In addition to user profiling and political micro-targeting, with the roll-out of 5G, an increase in the volume and speed of data theft is expected.[65] As confirmed by the US Cybersecurity and Infrastructure Security Agency (CISA), 5G networks will constitute 'an attractive target for criminals and foreign adversaries to exploit for valuable information and intelligence'.[66]

CONCLUSIONS & RECOMMENDATIONS

As this paper demonstrates, the development of 5G is a double-edged sword for democratic societies. On the one hand, 5G will enable greater connectivity and access to information, which promises to improve democratic participation, activism, and citizen mobilization. On the other hand, it can be used by governments to tighten information control, repress political opponents, and manipulate public opinion. The technology itself is inherently neutral; it is only what we, users, do with it that determines its impact.

Though widespread adoption will not be realized for a few years, once fully adopted, 5G will allow us to communicate ideas instantly, redefine audience engagement, and deliver unprecedented targeting capabilities. It will also change the way we interact with (political) advertising. 5G will bring to life new applications and usages: moving communication from a 2D to a 3D holographic format, enhancing video and voice calls, AR and VR, and providing richer and more interactive experiences. High-resolution audio and visual material will enable users to interact in ways that 4G does not come close to.[67]

5G has the potential to fill the gaps left unaddressed by previous technological revolutions. The changes that come with the implementation of 5G technology have the potential to considerably accelerate machine-to-machine interaction, but it remains to be seen how exactly it will impact human-to-human communication. While 5G is unlikely to usher in another major communications revolution, it would be naive to assume that nothing will change.[68]

Especially regarding disinformation campaigns, 5G will not only introduce new risks but also aggravate existing ones. First, a feature unique to 5G is its ability to collect new kinds of user data (such as more precise localization, biometric, and sensorial data), which can be used for more effective user profiling and (psychometric) targeting of those who are most vulnerable to influence. Second, 5G-backed AI capabilities will make it possible to manipulate audio-visual content in real time, making deepfakes more convincing. At the same time, because of its speed and connectivity, 5G will enhance all the problems we have been grappling with for the past decade. Not just the news, but also disinformation that journalists must sift through will travel faster and spread more widely in the era of 5G. As put by the Belfer Center for Science and International Affairs at Harvard: 'the weaponization of information through speedier channels could pose a threat to knowledge and information integrity'.[69] If even more information about a person's environment

becomes accessible, the potential for misuse expands too. Problems caused by previous technological breakthroughs plaguing social media today have not been solved. 5G and AI are evolving at such a quick pace that existing problems are likely to permeate, and intensify, in the 5G era.

Recommendations

1. **Address the potential for data misuse.** The first challenge lies in ensuring that personal data is secure – a challenge that is not unique to 5G networks. This necessitates both technological and regulatory solutions. On the technological side, privacy by design solutions and disclosure measures, i.e. getting companies to disclose how personal data is collected and what it is being used for, could minimize the risk of data misuse. On the regulatory side, improved law enforcement in 5G networks and adequate state policies that set out requirements for privacy regulations are needed. Such national strategies and policies should be harmonized across the Alliance. As tech companies such as Meta (previously Facebook), which have come under intense scrutiny for the mishandling of user data, turn to 5G to roll out new applications, it is crucial to promote greater accountability and address existing issues surrounding algorithmic transparency. In addressing these challenges, governments should ensure that regulation does not inhibit innovation and that democratic societies are not outpaced by their adversaries when it comes to technological advancement.

2. **Address supply chain and network security issues.** Modern militaries are going to become increasingly reliant on 5G for a wide variety of capabilities, from situational awareness, through military command and control (C2) and communications, to logistics. As connected devices proliferate, cybersecurity and resilience of 5G networks are crucial. Software supply chain efforts can address open-source vulnerabilities. To ensure the integrity of supply chains, technology vendors are increasingly adopting a zero trust network design. In May 2021, the Biden administration issued an executive order on zero trust architecture.[70] While disruptive for companies, this authentication system makes cyberattacks much less effective. Another important step in this regard was the adoption of the EU Toolbox for 5G Security in January 2020, which allows only 'trusted suppliers' into EU member states' networks. On the procurement side, it would be prudent for NATO to investigate the technologies that are being used in its systems and the civilian infrastructure that the military relies on, as well as their origins. To that end, NATO should develop common criteria to evaluate the trustworthiness of 5G vendors, technology, and infrastructure.

3. **Adopt cyber and technology standards.** With a long and successful track record as a standard-setter, NATO should be at the forefront of developing an ethical framework to drive the development and implementation of emerging and disruptive technologies, including 5G and AI.[71] This

would help offset China taking the lead in global standard setting. NATO recently launched an AI strategy which will set ethical guidelines around how to govern AI systems, and it is also exploring the potential of 5G for military applications.[72] NATO's baseline requirements for resilience already cover telecommunications, but Alliance-wide military-grade criteria to secure public and private 5G networks are yet to be developed.[73] To avoid duplication of effort, as a first step, NATO should take stock of what already exists and collaborate with Allied standard-setting bodies. Even with non-Chinese suppliers, the armed forces of NATO member states will largely rely on networks and equipment that are available commercially, which presents additional risks and vulnerabilities. Security requirements for military communications, such as the need to avoid being geo-localized and jammed by an adversary, exceed those offered by commercial 5G service providers, which have different security concerns and needs.[74] In addition to setting standards and technical specifications, Allied militaries should strive to secure high quality support and engineering, and closely cooperate with the industry to ensure that military-specific requirements are taken into consideration.

4. **Media and digital literacy.** In the fight against disinformation, technological solutions are not enough to combat the problem. As Dr. Alexander Klimburg, Head of the Centre for Cybersecurity at the World Economic Forum, puts it, 'attacking the body of cyber (the technical layers) is just a detour to attacking the mind (the human being)'.[75] Responses should therefore go beyond the technical and focus on the psychological dimension. Ultimately, the reason why disinformation works is because there is an audience for it. Increasing media and digital literacy may be one of the most efficient and powerful tools to restore a healthy relationship to information and increase the resilience of our democracies to online disinformation. Making end users aware of the potential risks that they may be facing in engaging with 5G and AI through campaigns, workshops, conferences, or online courses would go a long way. In the words of Tim Hwang, Director of the Harvard-MIT Ethics and Governance of AI Initiative, 'ultimately, resilience against online disinformation will depend not only on the ability to harness technology, but the ability to harness social and psychological forces, as well'.[76]

5. **Identify, verify, and correct social media content.** The use of highly realistic synthetic content is set to increase, which will present new challenges to content verification. With the proliferation of 3D storytelling formats, current assessment methods and tools will need to adapt and be able to process more complex types of data. In addition to the necessary education and digital literacy, it is equally important to equip journalists and fact-checkers with better tools to identify and verify the truthfulness and origins of obtained information, as well as to tackle false content.

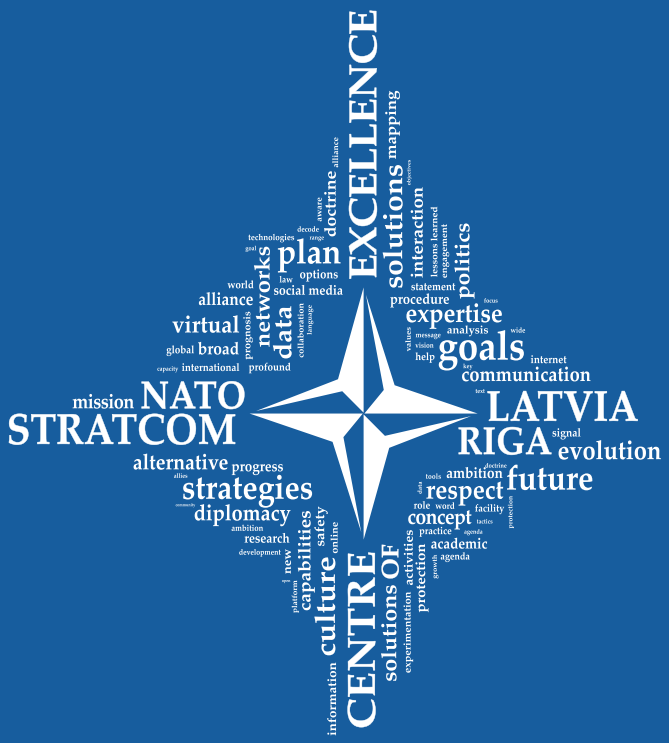
BOOKMARKS

1. Emily Vicker, 'Verizon Innovative Learning launches first ever 5G EdTech Challenge calling for solutions to challenges in under-resourced classrooms', Verizon, 9 November 2018, (accessed 22 December 2021).
2. Naja Bentzen, 'Computational Propaganda Techniques', European Parliamentary Research Service (EPRS), October 2018.
3. The Impact of the 5G Revolution on the Data Center,' 4 Data, 16 September 2020, (acccessed 13 January 2022).
4. Clare Duffy, 'What is 5G? Your Questions Answered,' CNN, 6 March 2021, (accessed 13 January 2022).
5. Ibid.
6. Jamie Carter, 'Discover 10 ways 5G can change how we communicate,' 5G Radar, 22 July 2020, (accessed 13 January 2022).
7. William Welsh, 'Holograms offer military better view of battlefield,' Defense Systems, 6 December 2010, (accessed 13 January 2022).
8. Daniel Ackerman, 'MIT Artificial Intelligence Tech can generate 3D holograms in real-time,' Big Think, 11 May 2021, (accessed 13 January 2022).
9. Sharon Weinberger, 'The Face of Allah Weapon Returns,' Wired, 13 May 2008, (accessed 13 Jauary 2022).
10. Latvia launches first 5G military test site in Europe,' LSM.lv, 13 November 2020, (accessed 13 January 2022).
11. User-Generated News: Can professional and citizen journalists work together?', SONY, (accessed 13 January 2022).
12. Raian Ali et al., 'Digital addiction: how technology keeps us hooked', The Conversation, 12 June 2018, (accessed 13 January 2022).
13. "How the New York Times Uses New Journalistic Tools Developed for 5G', The New York Times Company, (accessed 13 January 2022).
14. Aharon Wasserman, Serena Parr, and Joseph Kenol, 'Exploring the Future of 5G and Journalism', The New York Times, 11 April 2019, (accessed 13 January 2022).
15. 'User-Generated News'.
16. 'How the New York Times Uses New Journalistic Tools Developed for 5G'.
17. Mint Boonyapanachoti et al., 'R&D - Reconstructing Journalistic Scenes in 3D', The New York Times R&D, 27 July 2020, (accessed 13 January 2022).
18. Interview with Ján Lukačevič, The Czech Academy of Sciences, Institute of Atmospheric Physics at the Department of Space Physics, 10 November 2021.
19. 'Joint All-Domain Command and Control: Background and Issues for Congress', Congressional Research Service, 12 August 2021.

20. James Blackman, 'Lockheed Martin preps IoT and AI for space flights, satellite 5G for global weaponry', Expertise IoT Insights, 2 March 2021, (accessed 14 January 2022).
21. Rumana Ahmed et. al., '5G and the Future Internet: Implications for Developing Democracies and Human Rights', National Democratic Institute (NDI), July 2021, p. 9.
22. 'How 5G Will Bring High-Speed Internet to Underserved Communities', Forbes, 9 April 2021, (accessed 14 January 2022).
23. '5G from space - The role of satellites in 5G', Nokia, (accessed 14 January 2022).
24. Ibid.
25. Samuel Dominioni, 'Will 5G Push Internet Voting?', ISPI, 18 September 2020, (accessed 14 January 2022).
26. Sheila Jagannathan, 'How can 5G make a difference to education?', World Bank Blogs, 8 July 2021, (accessed 14 January 2022).
27. Emily Vicker, 'Verizon Innovative Learning launches first ever 5G EdTech Challenge calling for solutions to challenges in under-resourced classrooms', Verizon, 9 November 2018, (accessed 14 January 2022); 'Verizon scales edtech resources to over 3 million teachers in effort to leave no students behind', Verizon, 9 August 2021, (accessed 15 January 2022).
28. 'The COVID-19 pandemic has changed education forever. This is how', World Economic Forum, 29 April 2020, (accessed 15 January 2022).
29. Steven Feldstein, The Rise of Digital Repression: How Technology is Reshaping Power, Politics and Resistance (Oxford University Press, 2021, e-book).
30. Ibid.
31. Rumana Ahmed et al., '5G and the Future Internet: Implications for Developing Democracies and Human Rights', National Democratic Institute (NDI), July 2021, p. 9.
32. Rand Waltzman, 'The Weaponization of Information: The Need for Cognitive Security', RAND, 27 April 2017, (accessed 15 January 2022).
33. Naja Bentzen, 'Computational Propaganda Techniques', European Parliamentary Research Service (EPRS), October 2018, (accessed 15 January 2022).
34. Access to relevant data is key for the development and (re-)training of AI/ML models.
35. Steven Feldstein, 'The Global Expansion of AI Surveillance', Carnegie Endowment for International Peace, 17 September 2019, (accessed 15 January 2022).
36. Paul Mozur, 'One Month, 500 000 Face Scans: How China is Using A.I. to Profile a Minority', The New York Times, 14 April 2019, (accessed 15 January 2022).
37. Rumana Ahmed et al., '5G and the Future Internet: Implications for Developing Democracies and Human Rights', National Democratic Institute (NDI), July 2021, p. 13.
38. Feldstein, 'Global Expansion of AI Surveillance'.
39. Amit Agrawal, 'How Augmented Reality Can Revolutionize Political Campaigning', Forbes, 12 August 2020, (accessed 15 January 2022).
40. Marianne Barland, 'Elections, Technology and Political Influencing', Teknologirådet, 24 June 2019, (accessed 15 January 2022).
41. Silvia Milano, Brent Mittelstadt, and Sandra Wachter, 'Targeted ads isolate and divide us even when they're not political', The Conversation, 13 July 2021, (accessed 15 January 2022).

42. J. Scott Brennen et al., 'Types, sources, and claims of COVID-19 misinformation', Reuters Institute, University of Oxford, 7 April 2020, (accessed 15 January 2022).
43. Hugo Yen, David Simpson, and Lindsay Gorman, 'Tech Factsheets for Policymakers: 5G', Belfer Center for Science and International Affairs, Harvard Kennedy School, Spring 2020 Series, (accessed 15 January 2022).
44. See Katarina Kertysova, 'Artificial Intelligence and Disinformation: How AI changes the way disinformation is produced, disseminated, and can be countered', Security and Human Rights Volume 29 (2018): 55-81.
45. Gabriela Bodea et al., 'Automated Decision-Making on the Basis of Personal Data That Has Been Transferred from the EU to Companies Certified under the EU-U.S. Privacy Shield', European Commission, Directorate-General for Justice and Consumers, October 2018.
46. 'Article 13: EU GDPR', PrivazyPlan, 2018; 'Article 15: EU GDPR', PrivazyPlan, 2018.
47. 'GDPR: Third Countries', Intersoft Consulting, GDPR Info, (accessed 15 January 2022).
48. Carisa Nietsche and Bolton Smith, 'Why EU won't combat Huawei's Trojan Tech', The National Interest, 2 October 2019, (accessed 15 January 2022).
49. Rob Toews, 'Deepfakes are going to wreak havoc on society. We are not prepared', Forbes, 25 May 2020, (accessed 15 January 2022); Matthew F. Ferraro, 'Decoding Deepfakes', NSI Backgrounder, National Security Institute, December 2020, (accessed 15 January 2022).
50. Rumana Ahmed et al., '5G and the Future Internet: Implications for Developing Democracies and Human Rights', National Democratic Institute (NDI), July 2021.
51. Panel for the Future of Science and Technology, 'Tackling Deepfakes in European policy', European Parliament, (EPRS: July 2021).
52. Toews, "Deepfakes are going to wreak havoc on society'.
53. Robert Chesney and Danielle K. Citron, 'Disinformation on Steroids: The Threat of Deep Fakes', Council on Foreign Relations (CFR), 16 October 2018.
54. Keir Giles et al., 'The Role of Deepfakes in Malign Influence Campaigns' (Riga: NATO Strategic Communications Centre of Excellence, August 2019).
55. Paul Chadwick, 'The Liar's Dividend and Other Challenges of Deep-Fake News', The Guardian, 22 July 2018, (accessed 15 January 2022).
56. Janosch Delcker, 'Welcome to the Age of Uncertainty', Politico, 17 December 2019, (accessed 15 January 2022).
57. Tim Hwang, 'Deepfakes - Primer and Forecast' (Riga: NATO Strategic Communications Centre of Excellence, 3 June 2020).
58. Although calls and messages are encrypted in 4G, the user's metadata (location and identity) is not. 5G network equipment delivers improved security. It encrypts metadata that could otherwise be used to track a user and compromise their privacy. See for example: '5G SIM, Security and Privacy for IMSIS', Thales, 26 May 2021, (accessed 15 January 2022).
59. Ken Briodagh, '5G and GDPR can be boon to cybercriminals, Says GlobalData', IoT Evolution, 11 October 2018, (accessed 15 January 2022).
60. 'Is 5G Technology Dangerous – Pros and Cons of 5G Network', Kaspersky, (accessed 15 January 2022).

61. Rita Liao, 'Huawei says two-thirds of 5G networks outside China now use its gear', TechCrunch+, 26 June 2019, (accessed 15 January 2022).
62. '5G Explained – Part Three: National Security', Foreign Policy, 31 March 2020, (updated 23 February 2021), (accessed 15 January 2022).
63. Samuel Stolton, 'Huawei admit Chinese law obliges companies to work with government', Euractiv, 11 April 2019, (accessed 15 January 2022).
64. Interview results, 8 September 2021.
65. Saheli Choudhury, 'Automated hacking, deepfakes are going to be major cybersecurity threats in 2020', CNBC, 17 December 2019, (accessed 15 January 2022).
66. CISA, 'Potential Threat Vectors to 5G Infrastructure', 2021, (accessed 15 January 2022).
67. Jamie Carter, 'Discover 10 ways 5G can change how we communicate', 5G Radar, 22 July 2020.
68. Interview with Giorgio Bertoli, NATO StratCom CoE, 17 November, 2021.
69. Yen at al., 'Tech Factsheets for Policymakers: 5G'.
70. The White House, 'Executive Order on Improving the Nation's Cybersecurity', Briefing Room: 12 May 2021, (accessed 15 January 2022).
71. 'NATO 2030: Embrace the Change, Guard the Values', NATO 2030 Young Leaders Report, 2021.
72. 'NATO Tech Agency Explores the Potential of 5G for the Alliance', NCI Agency, 28 January 2021, (accessed 15 January 2022).
73. 'NATO needs a multinational effort to secure 5G networks', CCDCOE News, 9 June 2021, (accessed 15 January 2022).
74. Piret Pernik et al., 'Research Report: Supply Chain and Network Security for Military 5G Networks', (Tallinn: NATO CCDCOE, 2021).
75. Alexander Klimburg, The Darkening Web: The War for Cyberspace (New York: Penguin Books, 2017), p. 55.
76. Tim Hwang, 'Deepfakes - Primer and Forecast'.



Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

Operating since 2014, we have carried out significant research enhancing NATO nations' situational awareness of the information environment and have contributed to exercises and trainings with subject matter expertise.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org