16/02/2023

IN FOCUS

Digital Authoritarianism: How Digital Technologies Can Empower Authoritarianism and Weaken Democracy

Digital technologies have expanded the means by which states – both authoritarian and democratic – can exert societal control, thus helping to consolidate authoritarian rule and eroding democratic norms. Safeguarding against the abuses of digital authoritarianism will be a key challenge for 21st century democracy.

Federico Mantellassi
Research and Project Officer in Global and Emerging Risks, Geneva Centre for Security Policy

From their inception, digital information technologies were predominantly expected to lead to a global wave of democratisation. To many, the start of the Arab Spring in 2011 seemed to validate the role that these technologies could play in galvanising democratic uprisings against authoritarian governments. Greater connectivity would mean the end of authoritarian control over populations, who now would have the means to organise themselves and find and share information online, circumventing regimes' capacity for repression and control. Since then, we have woken to the reality that digital technologies such as social media, AI-powered surveillance systems, and big data collection and analysis capabilities enable "digital authoritarianism", because they have expanded the tools at a nation's disposal for repression and social control. Furthermore, they are enabling the decay of the online information ecosystem, a foundational aspect of 21st century democratic governance.

A global reality: AI-powered surveillance

Digital authoritarianism can be loosely defined as states' utilisation of digital information technologies for purposes of social control, repression, and surveillance and to otherwise reinforce their rule. Digital technologies (such as AI, facial recognition systems and social media) have substantially deepened the toolkit available for social control. Ubiquitous data collection systems, advanced biometrics, and advanced AI data-processing systems allow for accurate and broad tracking and profiling of citizens through the mass collection, analysis, and sorting of data, allowing governments to achieve both *granularity* and *scale* in their surveillance operations. Armed with this capacity, authoritarian regimes can more easily stem offline and online dissent and target surveillance at specific groups. Governments such as the ones in Russia and China have been particularly adept at leveraging these technologies to reinforce their rule, and stem dissent and democratic challenges to their power. They have also provided a global blueprint for how digital technologies can be utilised to these ends. For example, while China's much touted "social credit system" is often misunderstood and mis-characterised as a truly nation-wide centralised high-tech system for social control, the presence of smaller scale versions of such a system in some cities, particularly in the Xinjiang region of China, shows both a desire to leverage these digital tools for these purposes and their efficiency. Additionally, authoritarian regimes have weaponised the fact that political deliberations and organisation in the 21st century take place largely online. As such, they can more easily control narratives through censorship and by curbing internet freedoms, or with outright internet shutdowns –

which have become a popular tool for digital repression worldwide.

The capacity for digital technologies to undermine and degrade democracy and bolster authoritarianism is a global phenomenon that is not strictly confined to authoritarian regimes, but also affects democratic ones. Indeed, much of the technology that enables digital authoritarianism is Western in origin, and is widely used by democratic states. Countries such as France, the United States, Germany and Japan are, for example, both sellers and users of such technology, deeply involving the West in digital authoritarianism and putting even advanced democracies at risk of abuses. The COVID-19 pandemic, for example, sparked debates surrounding COVID tracing apps. These revolved around how, without appropriate legislative safeguards, they eroded privacy rights and the extent to which they normalised and extended a government's surveillance of its citizens. Similarly, NGOs in democracies such as the UK have long campaigned against the use of facial recognition technology in policing. Surveillance is not inherently unlawful. However, the scale, granularity, and types of data that these new technologies allow governments to collect – often without proper guardrails – greatly expands their snooping powers beyond what is traditionally needed for security and what is normatively acceptable. By allowing for and incentivising broad, automated, constant, cost-effective, invasive and targeted surveillance, these technologies increase the likelihood that states use them in ways that do not conform with democratic, privacy and human rights standards. For example, while it was not used for social control, the 2013 Snowden leaks revealed the full extent of the United States' problematic domestic and international digitally enabled surveillance apparatus.

Additionally, the rise of social media companies and a new business model based on relentless data collection to feed ever-more accurate AI-powered advertisement targeting has led to what amounts to widespread corporate surveillance and the emergence of "surveillance capitalism". While corporate surveillance does not equate to digital authoritarianism, surveillance capitalism does mean that citizens worldwide have little control over and knowledge of what sort of data is collected about them and for what purposes. The capacity for these companies to influence consumer behaviour through targeted advertisement and "nudges" has extended into the political sphere, with devastating effects on democracy. Technology giants' unprecedented and unrestricted access to our personal data has given private, unaccountable, and unrepresentative corporation unprecedented power over our socio-political lives, and influence during elections.

Eroding the information ecosystem

Democracy depends – among other pillars – on the free flow of reliable and factually accurate information. Today, this free flow of ideas largely takes place online, mainly on social media platforms, which have truly become the backbone of our digital democratic infrastructure. 2016 was a year of system shock for democracy, as the power of content echo chambers and online disinformation in influencing election results was in full display in the US elections and UK Brexit vote. Since then these dynamics have become commonplace, and almost a feature of 21st century democracy. This is symptomatic of the fact that digital technologies can be used to degrade democratic systems by polluting and diluting the information ecosystem – which is a key element of democratic governance.

This has been done in concerted efforts to destabilise democracies through disinformation campaigns, sometimes powered by troll farms paid to create, spread and amplify false narratives online. This disinformation epidemic is largely enabled by the algorithmic dynamics upon which social-media content recommendation relies, which prioritise emotional content more likely to capture users' attention, in turn promoting sensational, often erroneous political messaging while simultaneously locking users into content echo chambers. This has flooded digital spaces with false information and ensured that users are rarely exposed to competing viewpoints, while reinforcing their pre-existing beliefs. In this eroded information ecosystem (where citizens often do not share the same baseline understanding of what is factual), mistrust, political polarisation and real-world violence have

hijacked democratic deliberations. By enabling the creation of ever-more-realistic digitally created media and increasing the immersivity of digital experiences, emerging technologies such as deepfakes and metaverses will only accelerate this trend. Saving the information environment from decay should be a priority of security policy in order to reverse the global authoritarian trend. Facts and informed political deliberations fuel democracy, while conspiracy theories and lies fuel autocracy.

Conclusion

2022 marked the 16th consecutive year of global democratic decline. While by far not the only factor contributing to this trend, it is impossible to ignore the role that digital technologies, both old and new, have played in this decline. By expanding the repression toolkit available to governments, enabling the erosion of the information ecosystem vital to democratic governance, and massively empowering private technology firms, digital technologies have predominantly empowered authoritarianism and made democracy increasingly more fragile. Understanding this tension and ensuring that digital technologies are leveraged in ways that advance democratic norms and values should be a priority for the international community to start reversing the trend of global democratic decline.

Geneva Centre for Security Policy

www.gcsp.ch/publications
info@gcsp.ch