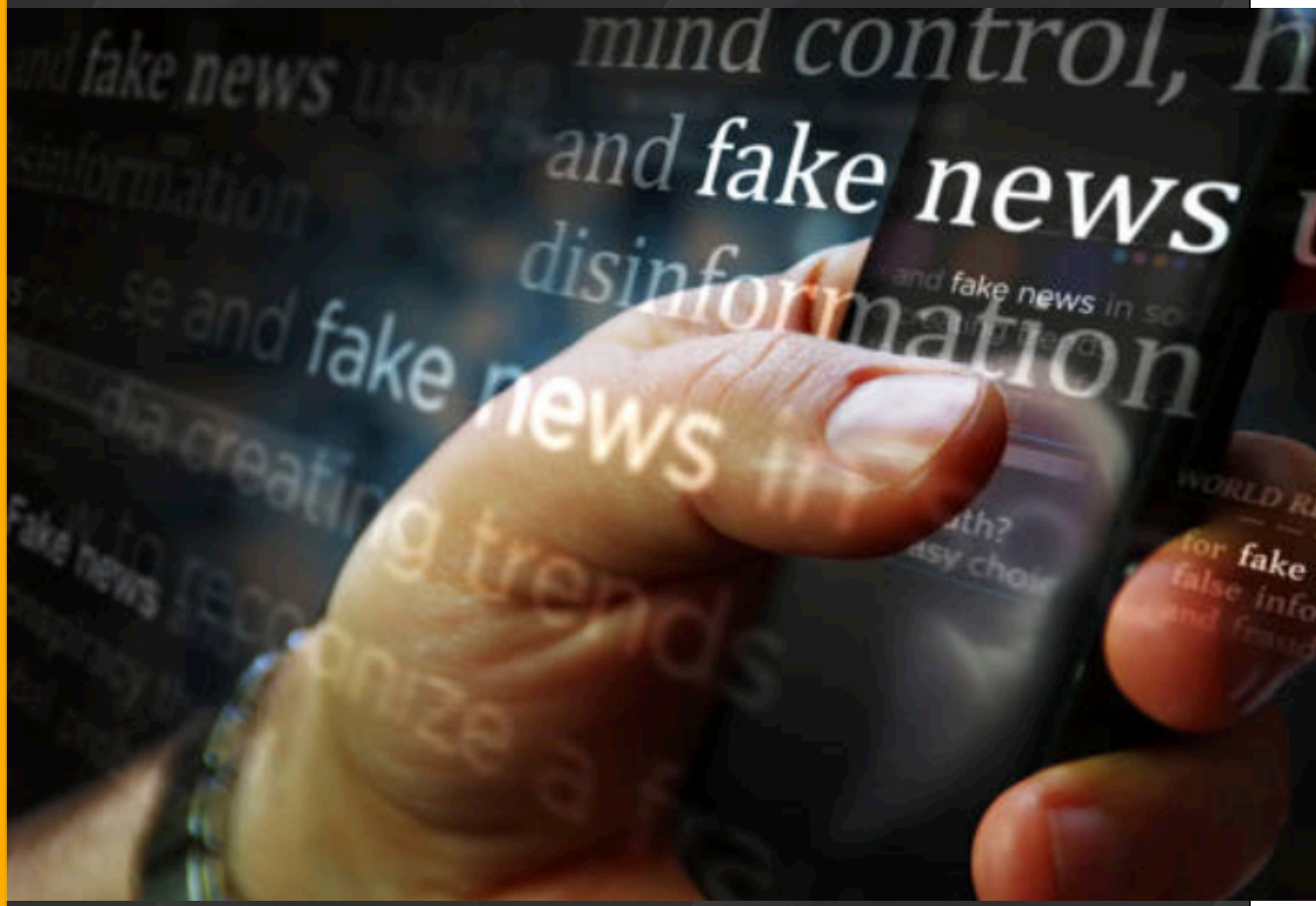
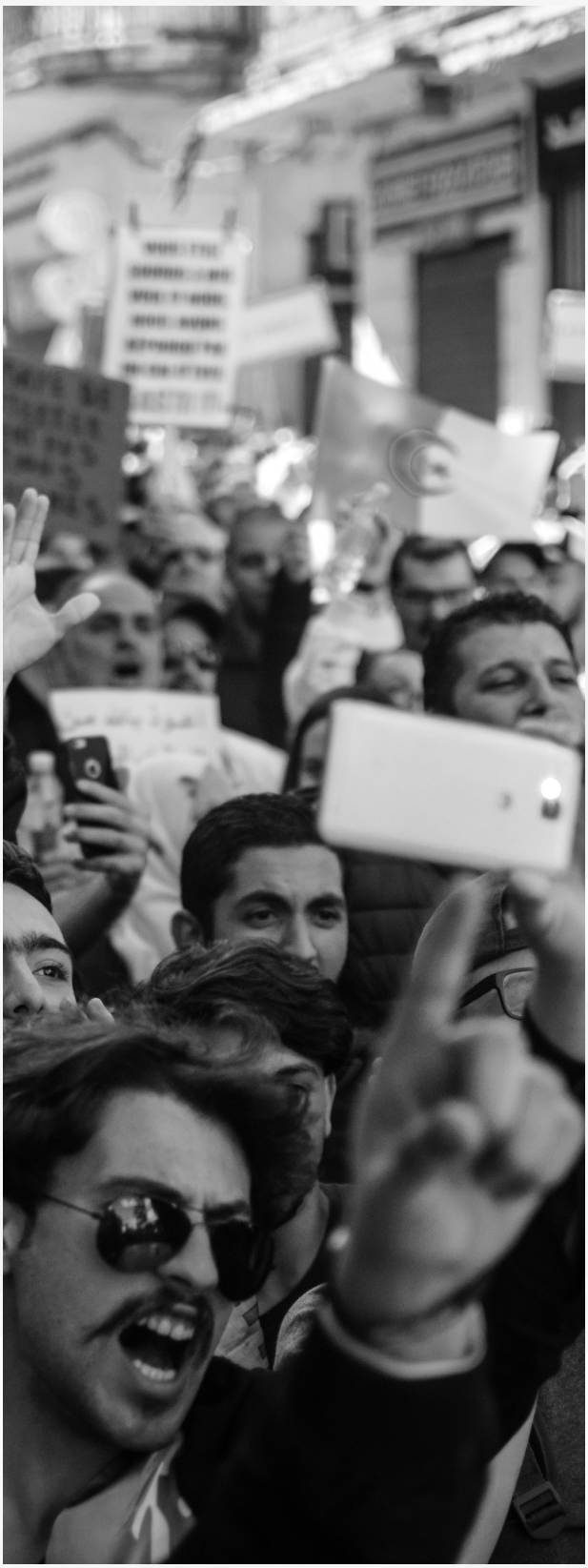
Global Insights

How Technology can Undermine Democracy



Across the world, political systems are being upended by technological developments. In this report, we examine how existing and emerging technologies can undermine democracy, along with the associated risks for businesses and political stability.

Introduction



This report delves into the multifaceted ways in which existing and emerging technologies can potentially undermine democracy, with a specific emphasis on the risks posed to national stability and businesses in light of recent developments. While technology has brought about significant advancements and opportunities, it has also ushered in an array of challenges that can erode the foundations of democratic systems. Technology has rapidly transformed the global landscape, providing unparalleled access to information, communication, and connectivity. These technological advancements, ranging from social media to artificial intelligence, also introduce various threats to the democratic system, which carry significant implications for national stability and businesses. These threats encompass issues such as disinformation, cyberattacks, privacy violations, and surveillance, all of which have the potential to undermine democratic processes and institutions.

In light of recent events both in the developed Western world and in fragile democracies, democracy and the rule of law appear to be universally under threat. After decades of liberalisation, the world has now witnessed a 17-year period of democratic decline (as per the World Freedom House). This has enabled the rise of 'strongman leaders' and military coups, partially fuelled by the disruptive societal forces of technological change.

These events can have profound implications not only for society but also for businesses. Social media can be swiftly employed to organise mass demonstrations, resulting in disrupted company supply chains, all the while being orchestrated around a misinformation campaign curated by artificial intelligence and micro-targeted to citizens based on data obtained through privacy violations or surveillance efforts. The extent and consequences of technology's politicisation will continue to be studied for many years, but it has already contributed to a more fractured and divided society, which is more prone to unrest, violence, and instability. All of these developments not only undermine business confidence and personal safety but also steer the world further away from prosperity and harmony.

Means of Disruption

Disinformation and Misinformation:
In our increasingly interconnected world, one of the paramount challenges engendered by technology is the propagation of disinformation and misinformation through online platforms. This has been seen in several elections across the democratic spectrum, from the UK to the US. The proliferation of false narratives, deepfakes, and fabricated news stories has the potential to manipulate public opinion, distorting the very essence of the democratic decision-making process. Foreign and domestic actors exploit these tools to foment discord, influence elections, and destabilise nations.

Cyberattacks:
The menace of cyberattacks, both those sponsored by states and those orchestrated by non-state actors, looms large over democratic systems. Elections, critical infrastructure, and government institutions have become ever at risk to hacking and a plethora of other cyber threats. These attacks can wreak havoc by disrupting essential services, undermining public trust, and inciting chaos on election days. This is of even greater threat in systems of digital democracy.

Privacy Violations:
The extensive gathering and commercialisation of personal data by technology companies give rise to concerns regarding individual privacy. The potentially intrusive nature of data collection, which includes surveillance, tracking, and profiling, poses a threat to citizens' trust in democratic systems. It also paves the way for highly effective micro-targeting and the formation of echo chambers within political campaigns. Such data can enable the precise targeting of individuals who are most susceptible to political rhetoric aimed at fostering divisions and instability.

Surveillance:
Governments, be they democratic or authoritarian, are increasingly harnessing technology for extensive surveillance, a practice criticised for the imposition of control over their citizens. This not only undermines individual freedoms and human rights but also represents a menace to businesses operating within these countries. Corporations face pressure to collaborate with such regimes, often leading to compromises in ethical standards and potentially tarnishing their international reputation, all of this occurs at the expense of democratic rights and norms and facilitated by elected officials.

Foreign State Involvement:
The aforementioned risks are increasingly carried out by malicious actors operating from outside the established political systems or democratic nations. Western democracies have consistently expressed concerns regarding the methods and potential for foreign state interference in their elections. This concern has received strong backing from intelligence agencies, which have underscored the capacity of nations like Russia to influence foreign political landscapes. Advancements in technology have ushered in a new global order where democratic boundaries no longer align neatly with geographical borders. While passports are still necessary for international travel, information, including tweets and other digital content flows freely across the globe. Consequently, technology's role in creating a more interconnected world has blurred the connection between physical location and the dissemination of information and political campaigning, thereby amplifying the possibility of increased foreign state interference.

Case Study – US Capitol Riots

The events of January 6, 2021, marked a pivotal moment in American democratic history while the causes and consequences of the attack are multifaceted and remain divisive, this case study delves only into the role of technology, particularly social media platforms, in the lead-up to the attack and its aftermath. Highlighting the ability of technology to facilitate disruptions in democratic systems.

Throughout and after the 2020 US presidential election, social media, emerged as a hub for echo chambers across the political divide. This has facilitated a more divided and fractured political landscape, with left-wing liberals only vocalising with those of a similar mindset, and the same occurring for the conservative right. Psychologists have studied how echo chambers can increase extremist voices and drive the polarisation we see around the world today. Throughout the 2020 campaign, the US witnessed new levels of polarisation as social media acted as a facilitator of division rather than information. However, the platforms have also revealed vulnerability to coordinated inauthentic behaviour as bots and disinformation campaigns have been shown to have spread falsehoods surrounding the 2020 elections. Researchers have since uncovered patterns of manipulation and coordinated influence campaigns on Twitter, Facebook, and Parler, shedding light on their contribution to the sentiment displayed in the January 6th attack.

This intertwined relationship between social media platforms and efforts to undermine democratic institutions is a key concern. Protestors in the January 6th riots were not spontaneous; the viral popularity of the #StoptheSteal campaign and the events on the day of January 6, where social media was used to broadcast, communicate, and at times organise the riot, are clear examples of the role technology can play in undermining the rule of law and political stability.

This case study illustrates the pivotal role technology, particularly social media platforms, played in the events leading up to the January 6th riots. Throughout the political campaign, the micro-targeting of individuals by networks of autonomous social media bots drove political polarisation, misinformation, and echo chambers. While not entirely clear, this likely involved the funding and campaigning by non-domestic actors and contributed to the divisions of society and political instability. The case study also notes the role of technology on the day of the riots in broadcasting, communicating, and organising the events.

As the United States approaches the 2024 presidential election, the road ahead is fraught with challenges. The divides in society have only deepened, and law enforcement must better understand the impact of technology on the events of January 6 to safeguard the integrity of the future democratic process. The study serves as just one example of the ability of technology to shape political discourse and mobilise movements in a destabilising manner.

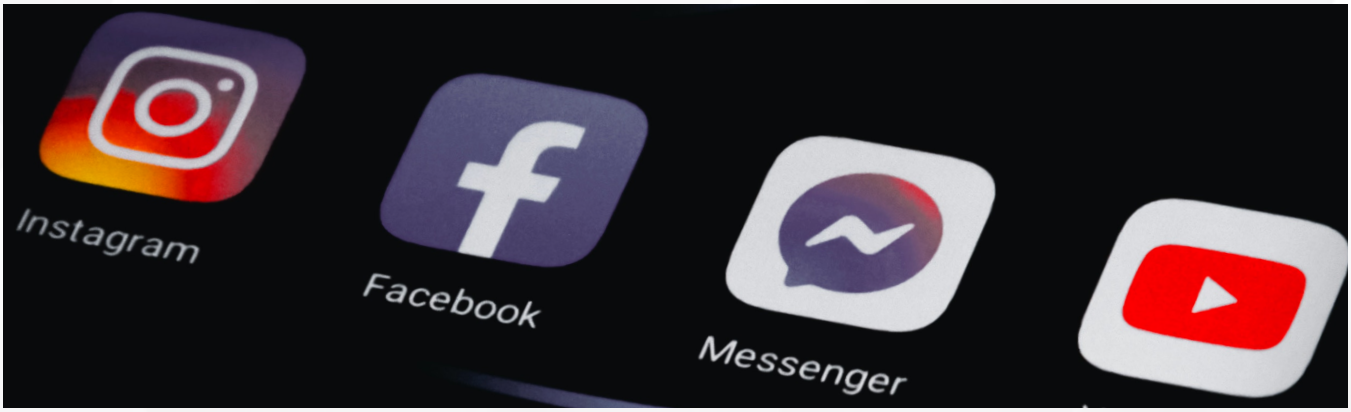
Conclusion

In conclusion, this report highlights the significant security implications that emerging technologies pose for democratic systems. The rapid advancement of technology has brought about unprecedented opportunities for connectivity and information access, but it has also ushered in a host of challenges that threaten the stability of nations and thus the operations of businesses. While this report exclusively highlights the risks of technology, this is of course one sided and for each flaw the new and emerging technologies have bought a range of benefits throughout society. We therefore stress that this is not a technologically pessimistic report, but rather its objective is to highlight the new risks and challenges we must now overcome.

The erosion of democracy with the rise of 'strongman leaders' and military coups in recent years, is at least partly driven by the disruptive forces of technological change. In this report we have highlighted how technological change can pose a direct threat to democracy. This is just one mechanism of technology's impact and technological change has to driven changes in societal structures from workplaces to perceptions of place, which have later influenced political outcomes and arguably created a climate of uncertainty and instability. This political climate can have profound consequences for businesses as they grapple with disrupted supply chains resulting from mass demonstrations organised via social media and deal with misinformation campaigns directed about there production techniques or environmental impact in part orchestrated by artificial intelligence. These developments not only undermine business confidence but also in an ever more polarised society endanger the personal safety of employees.

The means of disruption discussed in this report, including disinformation and misinformation, cyberattacks, privacy violations, and surveillance, have the potential to distort democratic decision-making processes, undermine public trust, and incite chaos. Furthermore, the involvement of foreign states in these disruptions, amplified by the interconnected nature of our digital world, poses a unique challenge to safeguarding the integrity of national democratic systems.

As we approach future elections and navigate the complex landscape of technology's impact on democracy, it is crucial for businesses to be vigilant about potential disruptions to their operations and travellers to be aware of the potential risks associated with political instability. Governments, corporations, and individuals must work together to address the security implications posed by technology, develop strategies to combat disinformation and cyber threats, and safeguard democratic processes. In doing so, we can better protect both the stability of nations and the interests of businesses in an increasingly interconnected and technologically driven world.



Contact

For more information on our full range of services including:

- Security Assessments
- Evacuation Planning
- Travel Risk Assessments
- Bespoke reporting

Please contact our Intelligence Research Team
irt@sps-global.com

This report was edited by: Oliver Maund, Lead Intelligence Analyst

Based in the Global Response Centre in Hereford, Oliver Maund is SPS's Lead Intelligence Analyst. Before joining SPS, he achieved a first-class honours degree in a joint Politics and Economics bachelor's program from the Exeter University.

Propriety Information