Digital Threats to Democracy: Divided Against Itself

M. Nina Miller, Technology for Global Security

Identity and ideology are multifaceted and complex. While polarization is often considered a question of binary extremes, most societies have multiple axes: racial, ethnic, economic, partisan, geographic, and linguistic diversity. These differences pre-date the digital threats discussed here, yet new technologies can amplify divisions and erode trust in public institutions.

FREE DIGITAL SPEECH

The wide reach and speed of online communication heightens the impacts of controversial content by preying upon basic psychological instincts. Social media platforms can amplify divisive voices and interfere with trust and attention that underlies public discussion in democracies. Zeynep Tufekci describes this psychological vulnerability to online divisiveness, "We are particularly susceptible to glimmers of novelty, messages of affirmation and belonging, and messages of outrage toward perceived enemies. These kinds of messages are to human community what salt, sugar, and fat are to the human appetite."

Digital propaganda dramatically heightens the impact that a lone actor or group can achieve by reaching more people, faster, with targeted content based on personal data. These propagandists seek to exploit societal divisions, erode trust in media and political institutions, and spread conspiracy theories. Little by little, this digital influence not only polarizes, but undermines popular faith in the ideological structures that previously tied citizens together.

Using false content, troves of user data, and inauthentic or synthetic accounts, well-resourced digital propagandists called Advanced Persistent Manipulators (APMs) can be especially influential. APMs use creative methods, such as arranging in-person meet ups and impersonating members of a targeted group to fracture consensus and increase polarization. This manipulation by unknown actors, facilitated by online anonymity, makes every interaction on social media a sort of masquerade ball. As Peter Pomerantsev posits, "more disconcerting is the idea that they know something about me that I hadn't realized myself, that I'm not who I think I am—one's complete dissipation into data that is now being manipulated by someone else."

In the future, online influence operations may increasingly employ AI-enabled "bots" and deepfakes to generate false and inflammatory content aimed at user biases, further fracturing ideologies and identities. Yet, a key point to remember is that humans, rather than bots, are responsible for amplifying and propagating false information online today.

FUTURE DIGITAL THREATS TO DEMOCRACY

This ongoing series from Technology for Global Security and the Center for a New American Security examines the elements and potential implications of digital threats to democracy over the next ten years.

UNEQUAL ACCESS

The use and abuse of digital communications is inherently linked to ongoing issues of unequal access to the tools of the 21st century. New digital technologies could further worsen urban-rural, economic, and social divides. For instance, the introduction of 5G infrastructure could widen the digital gap as rural communities are unlikely to see the same improvements in high-speed telecommunications systems as urban areas. Automation in the workplace is likely to cause socioeconomic shifts and could worsen income inequality without corresponding political adjustments. Many analysts have also identified key challenges, such as climate change, conflict, urbanization, demographic shifts, and mass migration, which will strain limited resources available to address digital threats to democracy.

The online mis/disinformation challenge is also a question of inequality. A small number of polarized individuals—particularly separated by age and partisanship—are the main consumers of "fake news" and refuse fact-checks. Andrew Guess, Brendan Nyhan, and Jason Reifler attribute this fact to selective exposure and indicate that the "echo chamber" is "narrow ... but deep." As such, digital propaganda has an outsized impact by targeting these influential individuals and groups who vote and amplify such content. This cycle contributes to a lack of consensus-forming in public conversations and distrust in both state and non-state institutions.

A DIVIDED FUTURE?

The growing trend of fractured ideologies and identities has the potential to undermine key democratic institutions in the future. Affective polarization is linked to reduced trust in government—particularly opposing party rule—so partisan divides could increasingly lead to cynicism and suspicion towards democratic processes in general. For civil society and the democratic public, fractured ideologies and identity is likely to contribute to another trend identified in this series: weakened media institutions. As polarization reduces trust in media institutions and journalists, this trend will also reduce the ability of populations in democracies to deliberate and reach consensus on important ideas.

In this future, elections increasingly may be seen as existential fights, and as Yoni Appelbaum notes, "democracy depends on the consent of the losers." Moreover, digital division is based on economic incentives. Some tech companies generate higher advertising revenue and thus benefit from increased polarization, because outrage drives engagement and increased use of online platforms. This trend seems intractable precisely because it takes advantage of base psychological tendencies, worsens existing societal divides, turns democratic free speech on its head, and chases market incentives at the expense of both national and individual well-being.

M. Nina Miller is a research analyst with Technology for Global Security. Before joining T4GS, Nina interned with the Nuclear Threat Initiative's Global Nuclear Policy Program and Scientific and Technical Affairs teams. She holds a B.A. (International Honours) from the Joint Degree Programme between the College of William & Mary and the University of St Andrews.

CNAS | TECHNOLOGY FOR GLOBAL SECURITY