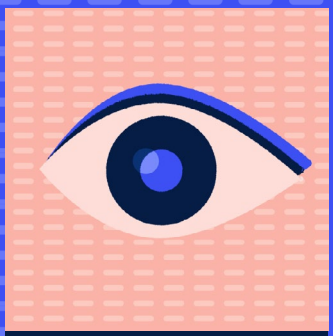


FUTURE DIGITAL THREATS TO DEMOCRACY

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.

Digital Threats to Democracy: A Double-Edged Sentence

M. Nina Miller, Technology for Global Security

WEAPONIZING INFORMATION IN DEMOCRATIC SOCIETIES

Digital communication speeds the spread of all information, true or otherwise. Increasingly, digital campaigns can have physical impacts by manipulating public opinion, eroding the distinction between truth and lie, and poisoning the forums for debating important ideas. Actors ranging from powerful countries to "lone wolves" can weaponize digital communications with novel technologies to change the course of an election or radicalize individuals to their cause.

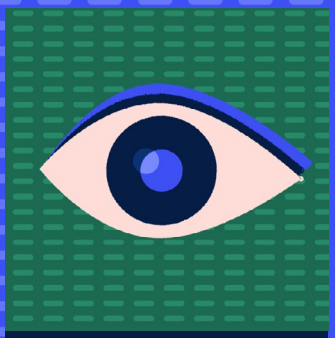
Democratic institutions and norms generally prioritize widespread communication, free access to information, and the liberty to hold distinct opinions. Widespread access to free online information gives a voice and new resources to previously marginalized groups, yet this openness can be a vulnerability that contributes to the weaponization of information. Civil society and governments rely on digital communications, which increase the attack surface. Malign actors exploit democratic values and institutions in three related ways:

- Filling public debate with disinformation and distraction—or "information flooding"—by abusing free speech and the purposefully open nature of the internet.
- Exploiting democratic values to disseminate misinformation and influence campaigns.
- Using open-source material, such as widely available code and other tools, for disinformation campaigns.

TECHNICAL DRIVERS BLUR TRUTH AND LIES

Lies and rumors have been spread for centuries, but technical development increases the reach and speed of malign actors spreading propaganda and confusion. Social media has changed how individuals communicate with each other and receive news, while new technologies are likely to make it even more difficult to identify lies among digital content. Three significant technical trends are:

- Artificial intelligence enables intelligent bots and automated spear phishing—when AI mines social media to gather information on friends and family and then impersonates them to extract important information.
- Deepfakes and video manipulation make false or manipulated political content more believable and influential.
- Augmented reality/virtual reality (AR/VR) is expected to worsen the trend of sophisticated digital propaganda because identifying false content that you can see, hear, and touch is near impossible.



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.

TECHNIQUES TO MANIPULATE ONLINE TARGETS

Malign actors employ sophisticated tactics and attack vectors that take advantage of cognitive biases and existing divides in society. As Samuel Woolley cautions, "No media tool, from a book to a virtual simulation, is a weapon in and of itself."

Digital propagandists are largely pragmatists—using cheap technology like automated accounts to astroturf and plant conspiracy theories that become widely adopted. Groups ranging from ISIS to Russian intelligence have deployed innovative influence campaigns. Based on digital platforms, these propaganda campaigns take advantage of hyper-personalized data available to target specific identities and interests. Elements of social media, particularly "trending" markers and personalized content algorithms, are valuable vectors to spread disinformation and hijack public conversations.

An Advanced Persistent Manipulator (APM) is a sophisticated type of digital propagandist that Clint Watts defines as "an actor or combination of actors perpetrating an extended, sophisticated, multi-platform, multi-media information attack on a specific target." Basic objectives of APMs include influencing audiences, discrediting adversaries, provoking conflict, and enlisting allies; yet, more sophisticated manipulators aim to distort reality itself. APM kill chains mobilize targets to act on their behalf through a multi-platform attack incorporating staging, reconnaissance, mimicry of popular accounts, and narrative amplification.

THE FUTURE IMPACT OF WEAPONIZED INFORMATION

While forecasting the exact future is impossible, several analysts have identified possible implications of this growing weaponization of information. As Robert Chesney and Danielle Keats Citron identify, deepfakes create a dangerous liar's dividend, where individuals could increasingly avoid accountability even when their wrongdoing is documented with video or photos. Joshua A. Tucker and colleagues caution that just as social media permits activists and marginalized populations to participate in democracy, these platforms can also aid anti-democratic extremists. As Zeynep Zufekci notes, the erosion of any and all credibility of online information is a new tool of censorship.

It has become a common refrain that a lie can travel halfway around the world while the truth is still putting its shoes on (ironically, frequently misattributed to Mark Twain). In this information environment, the truth needs a fighting chance.

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.