Policy Brief:
Addressing the Misuse of Technology to Threaten Security and Human Rights

compiled by Nina Jankowicz, Global Fellow, The Wilson Center

Background

Technological advances in the past two decades have allowed democratic movements within and beyond the transatlantic space to reach new members, organize, and challenge repressive regimes, reinvigorating the democratic process. As they have empowered activism, so too have they enabled autocratic and authoritarian regimes to undermine democracies.

In the past five years alone democracies have been targets of disinformation, online influence, and election interference campaigns. Hacking, phishing, and cyberattacks have exposed the personal correspondence of politicians and government officials, while laying bare the personal information of private citizens.[1] These campaigns do not originate only in autocracies; Israeli company NSO Group has spied on dignitaries' and US diplomats' private communications through its Pegasus spyware.[2] Meanwhile, democratic activists who once turned to the internet as a critical tool in their outreach and organizing are now finding themselves technology's victims as authoritarian states such as Belarus, Russia, and China use technological developments for surveillance and restrictions on freedom of expression such as internet shutdowns.

Finally, democracies also have domestic forces with which to contend; online microtargeted advertising allows political campaigns and other groups to target antidemocratic, violent, or hateful messages to vulnerable populations, sometimes resulting in offline action, such as the January 6 insurrection at the U.S. Capitol. Furthermore, due to a lack of adequate oversight and content moderation enforcement, social media platforms have given purchase to an environment in which women and marginalized groups participating in online public discourse are subject to vitriolic and violent attacks on the basis of their gender, sex, or race; these attacks often spill offline and affect these groups' participation in the democratic process.[3]

This brief will outline potential responses to some of these challenges. It is not meant to be exhaustive, but to spark conversation and creativity; it is sorely needed in responding to the technological challenges democracies now face.

[1] For a list of more than 600 authoritarian influence incidents in the transatlantic community and beyond, see the Alliance for Securing Democracy's Authoritarian Influence Tracker.

[2] See Craig Timberg et al, "Pegasus spyware used to hack U.S. diplomats working abroad," *The Washington Post*, 3 December 2021.

[3] See Nina Jankowicz et al, "Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online," The Wilson Center, January 2021.

Potential Responses

Responding to Authoritarian and Autocratic Technological Misuse

- Democratic allies might pursue **targeted sanctions** addressing the funding or leadership of harmful technology projects. In Russia, US sanctions targeting Prigozhin and various parts of the Internet Research Agency seem to have had little impact on the IRA's activities. Such sanctions might be rendered more powerful if coordinated with allied governments (see next bullet). Similarly, **cyber disruptions**, such as the USG's shutdown of the IRA during the 2018 Midterm Elections, could be considered;[4] however, governments should remember that for disinformation campaigns, in particular, Election Day is an inflection point, not a start or end point.

- **Coordination between allied governments** is critical when levying economic, informational, or diplomatic responses to the misuse of technology. Such actions "could be molded in the image of the solidarity achieved in the wake of the Kremlin's poisoning of the former Russian military officer Sergei Skripal in the United Kingdom in 2018; for this explicit and gross violation of British sovereignty, British allies around the world coordinated the expulsion of hundreds of Russian diplomats from their countries. These countries also worked together to respond to the corresponding disinformation campaign the Kremlin launched to deny that it had poisoned Skripal with a military-grade nerve agent; the United Kingdom distributed fact sheets to allies and foreign policy and media influencers to use in their communications. This was the first such campaign to respond to foreign interference in a synchronized multilateral fashion," and it rendered the Kremlin's corresponding disinformation campaign much less effective.[5]

- This coordination could be pursued through a **democratic bloc** against election interference or online influence campaigns, for instance. Allies might prioritize such activities as: "sharing analysis and assessments to understand and counter threats; developing ongoing joint strategic communications to engage hostile states' target audiences; joint exercising of contingencies; and creating issue-specific plurilateral groups allowing partners to respond or put pressure on adversaries in specific regions or on specific topics, such as a wildlife commission into wet markets."[6] Furthermore, allies would benefit from much greater coordination of assistance programs related to technological misuse provided to burgeoning democracies. Currently, programs are duplicative and many do not reflect best practices in the growing field. When facing formidable adversaries such as Russia and China, who are willing to "flood the zone"

[4] Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *The Washington Post*, 27 February 2019.

[5] Nina Jankowicz, "How Disinformation Corrodes Democracy," *Foreign Affairs*, 30 November 2021.

[6] Nina Jankowicz and Henry Collis, "Enduring Information Vigilance: Government after COVID-19," Parameters 50, no. 3 (2020).

with misleading information, coordinating and maximizing allied resources is all the more important.

Regulatory Responses to Challenge the Infrastructure of Technological Misuse

Even if autocrats halted their misuse of technology tomorrow, democracies would still encounter antidemocratic behavior online due to the infrastructure governing popular social media platforms. Below are principles for democracies to consider in their pursuit of technological and electoral regulation.

- Similar to allied coordination to counter antidemocratic tech campaigns, a democratic internet requires **coordination on regulation**, not patchwork legislation affording users different democratic rights when they cross borders. As Europe pursues its Digital Services Act, set to be the broadest legislation governing social media in the world, while the UK debates its Online Safety Bill and the United States weighs many regulatory options with varying degrees of seriousness, tech companies continue to put revenue above democratic principles of equality and freedom of expression. This engenders not only an environment in which adversaries can manipulate societal fissures to the detriment of democracies, but democratic disinformers can exacerbate polarization and exploit the vulnerable. The aforementioned democratic counter-disinformation/tech abuse bloc could serve as a convener for negotiations on democratic regulation of tech platforms that protects freedom of expression and other democratic values.

- Similarly, allies should consider the broad adoption of **election integrity pledges**, similar to the "Pledge for Election Integrity spearheaded by the pro-democracy nonprofit Alliance of Democracies in 2019. Signatories promise to "not fabricate, use or spread falsified, fabricated, doxed, or stolen data or materials for disinformation or propaganda purposes; avoid the dissemination of doctored media that impersonate other candidates, including deep-fake videos;" practice good cyber-hygiene (ensuring that candidates, campaigns, and data about supporters are all safe from hacking operations); not use astroturfing to attack opponents; and maintain transparency in campaign funding."[7] These would encourage the adherence to democratic values in domestic campaigning, provide a signpost for voters and election observers regarding a candidate or party's integrity, and inform local election oversight bodies.

[7] Jankowicz, "How Disinformation Corrodes Democracy."