Chapter 11

Exploring Cybersecurity, Misinformation, and Interference in Voting and Elections Through Cyberspace

S. Raschid Muller
https://orcid.org/0000-0002-1742-7575
Arizona State University, USA

Darrell Norman Burrell
https://orcid.org/0000-0002-4675-9544
Marymount University, USA

Calvin Nobles
https://orcid.org/0000-0003-4002-1108
Illinois Institute of Technology, USA

Horace C. Mingo
https://orcid.org/0000-0002-2395-2990
Marymount University, USA

Andreas Vassilakos
Illinois Institute of Technology, USA

ABSTRACT

Interference in the election process from both abroad and within the United States has produced chaos and confusion in business markets, communities, and among voters. Elections have become less reliable as a result of misleading statements. Election deniers are actively working to undermine confidence in our elections and suppress turnout, particularly among voters of color and other communities that have historically been marginalized. The false information spread, which includes lies about the voting process and election workers, has the potential to have significant repercussions for people's abilities to vote and their faith in our elections. Election misinformation poses a threat to democratic processes in the United States. Sixty-four percent of election officials reported in 2022 that spreading false information had made their jobs more dangerous. This chapter uses emerging content from extant literature to discuss cyberpsychology and the complex dynamics of these issues with a primary focus on finding solutions to these problems.

DOI: 10.4018/978-1-6684-9018-1.ch011

INTRODUCTION

The United States elections officials faced extreme pressure in 2020 to safeguard the presidential election process (Vanderwalker, 2020). According to a Collaborative Multi-Racial Political Study, Sanchez et al. (2022) found that 64% of the American public feels that U.S. democracy is in crisis and at risk of crumbling. In a Quinnipiac University study, Sanchez found that more than half of Americans anticipate that political tensions will worsen rather than improve throughout their lifetime. Tenove, Bffie, McKay, and Moscrop (2018) suggested profound threats to fair political participation and that these threats may affect some groups disproportionately.

Vladimir Putin's administration has waged an unrelenting campaign to undermine the democratic process and the rule of law in Europe and the United States for many years. Military incursions, cyberattacks, disinformation, support for extreme political factions, the weaponization of natural resources, organized crime, and corruption are all part of the Kremlin's arsenal (Taylor, 2019). Digital communication technologies are being used to interfere in democracy and elections unprecedentedly (Anderson & Raine, 2020).

Cybersecurity risks and misinformation have become significant threats in the U.S. and globally (Anderson & Raine, 2020; Vanderwalker, 2020). Government interference in cyberspace can raise concerns about privacy, freedom of expression, and the potential for abuse of power. Government interference in cyberspace refers to actions taken by governments to regulate, control, or otherwise influence the use of the Internet and other digital technologies within their borders. This interference can take many forms, such as censorship, surveillance, and implementing laws and regulations related to online activity. Governments may engage in these activities for various reasons, including protecting national security, enforcing laws and regulations, and promoting particular political or ideological agendas. Klepper (2022) posits that political misinformation often focuses on immigration, crime, public health, geopolitics, disasters, education, or mass shootings. Klepper fund that claims about the security of mail ballots has increased, as have baseless rumors about noncitizens voting. That is in addition to claims about dead people casting ballots, moving ballot drop boxes, or wild stories about voting machines (Klepper, 2022).

Disinformation can take many forms, including false or misleading claims about candidates, voter suppression tactics, and attempts to manipulate the outcome of elections. Republican candidate Donald Trump assailed the election's validity even before he lost. He then refused to accept, disseminating falsehoods about the election that spurred the deadly attack on the U.S. Capitol on January 6, 2021. His attorney general, William Barr, denied his claim in over 60 court decisions (Klepper, 2022). The proliferation of intentionally misleading material intended to disrupt the democratic process has contributed to the erosion of public faith in the political system (Sanchez et al., 2022). President Trump reaffirmed that the deception of the 2020 election results enhanced Russian efforts and had long-lasting consequences on voter faith in election outcomes (Sanchez et al., 2022).

State and municipal election officials are concerned about electoral fraud claims, which include misleading assertions about the 2020 presidential election and this month's California recall process (Vasilogambros, 2021). The commonwealth is increasingly alleging voter fraud. Some election officials worry about verbal and physical attacks due to electoral system misinformation. This summer, the Justice Department launched a law enforcement task force to address election officials and volunteer threats (Vasilogambros, 2021).

The COVID-19 pandemic created new challenges for election officials who were forced to make emergency changes to the voting process, typically with rapidly scarce resources (Vanderwalker, 2020).