CONFRONTING DIGITAL EXTREMISM

An Introduction and How-To Guide

Curated by Dr. Stephen C. Rea (Colorado School of Mines) and Colin Bernatzky (UC Irvine)

Purpose

The University of California, Irvine's Office of Inclusive Excellence launched "Confronting Extremism" in 2017 as "a year-long campus initiative dedicated to understanding the ideas and behaviors advocated far outside of alignment to the campus values for social justice and equity in today's society as a means to identify pathways for building positive campus and democratic communities" (see https://inclusion.uci.edu/confronting-extremism/). As part of this broader university initiative, we have developed six teaching modules on the topic of digital extremism that are designed to help raise awareness about different modes of extremist activity in online environments and propose effective means of confronting them. Two related concerns motivate our project: the proliferation of disinformation through social media and other online platforms around the 2016 US Presidential election and the 2020 COVID-19 global pandemic; and the growing visibility of far-right extremist hate groups and violence, especially in the wake of August 2017's "Unite the Right" rally in Charlottesville, Virginia. While neither coordinated media manipulation nor far-right political extremism are new phenomena in American society, the ways in which disinformation campaigners and hate-based ideologues have exploited the digital media ecosystem's technological affordances present clear threats to the ideals of democratic communities that demand critical attention and understanding if they are to be confronted. University campuses are far from immune to these threats; college students who are participating in the political process for the first time are exposed to mis- and disinformation campaigns through their social media activities, and there is abundant evidence that far-right groups are targeting college students for recruitment.

In what follows, we introduce the six teaching modules and their components, and suggest best practices for integrating them into your own courses. Although we believe that these tools are helpful for the "Confronting Extremism" initiative's goals, there are also some potential risks that necessitate having preventive guardrails in place.

The Modules

Each module includes five components: 1) a video lecture (between 15 and 17 minutes long); 2) 3-4 readings; 3) a short video from a third-party source related to the topic; 4) a classroom activity; and 5) a list of recommended readings. The modules are organized around the following topics:

Case Studies in Disinformation: This module defines three types of media manipulation—propaganda, misinformation, and disinformation—and briefly summarizes three contemporary examples of coordinated disinformation through digital media channels: Russian military intelligence operations in the Ukraine in 2014; the Duterte campaign's social media strategy during the 2016 Philippines Presidential election; and the Internet Research Agency's use of fake Facebook groups during the 2016 US Presidential election.

Trolls & Extremists: This module compares the activities of so-called Internet "trolls" with those of digital extremists, defined as both disinformation campaigners and political extremists (focusing specifically on far-right, hate-based extremism). In particular, it identifies similar strategies and techniques that are employed by both groups in their online activities, such as the use of image-centric memes, leaderless mobilization, and targeted harassment. The circumstances surrounding #GamerGate in 2014 afford a window into online trolling's convergence more overtly political extremism.

Algorithmic Exploitation: This module closely examines some of the techniques that digital extremists use to exploit algorithmic processes on social media platforms and with respect to search engines. It highlights three specific techniques using real-world examples: how automated social media accounts called "bots" helped drive narratives and engagement around specific topics or stories during the 2016 US Presidential campaign; how Russia's Internet Research Agency used fake Facebook groups and Facebook's targeted advertising services to coordinate voter suppression in the same election; and how a white supremacist group exploited "data voids" in online searches to promote its hate-based ideology and, indirectly, influence a 2015 mass shooting.

Toward a New Digital Civics: This module proposes lessons for "a new digital civics," that is, a curriculum that addresses the affordances and hazards of participation in the digital media ecosystem. Going beyond media literacy and fact-checking efforts, new digital civics examine the technological capacities of social media platforms, search engines, and other aspects of digital media, how extremists have exploited those capacities to further their own messages and agendas, and practical strategies for confronting digital extremism. Three such strategies are introduced, targeted at different stakeholders: learning how to interpret and react to social media metadata; practicing "strategic silence" in news media coverage of digital extremists; and incentivizing the digital media ecosystem's gatekeepers to use their powerful positions to nullify extremists' ability to engage in exploitation and manipulation.

Racialization of COVID-19: This module examines how pandemics and similar crises have historically fueled processes of racialization, othering, and stigmatization, exploring how these processes have been both enabled and constrained through social media in the age of COVID-19. Strategies to counter online hate during the pandemic are identified, including responses by social media platforms, institutions and grassroots activists.

The Infodemic: This module assesses the increasing cross-pollination between white supremacists, science denialists, militia groups, and other factions that have been thrust together both online and in person by the pandemic, contributing to a flood of misinformation that has been described by the World Health Organization as an "infodemic". It outlines the basis and appeal of conspiracies that arise in uncertain times, as well as the role that social media plays in facilitating the spread of COVID-19 conspiracies and misinformation. Finally, efforts to mitigate the infodemic and restore our digital ecosystem are considered.

How to Use the Modules

As the name implies, we have designed these modules to be used separately and flexibly in your own courses. They are deliberately interdisciplinary as well; each module could just as easily be integrated with a communications course as they could with a course in political science, sociology, social informatics, literature, and so on. And although they complement each other, no single module relies on the others in order to make sense or be useful. Moreover, there is no requirement that every one of the module's five components must be used. You may find that the readings and video lecture are helpful, but that the classroom activity is unfeasible for your specific class. Or you may want to use the recommended readings for help in constructing your syllabus, but are not interested in screening the video lectures. Finally, while we have attempted to make the modules as accessible and approachable as possible, you may find that certain readings, activities, or video lectures are either too difficult or not advanced enough for your learning goals. Generally speaking, we imagine that they will be most applicable in upper-level undergraduate courses or as supplementary material for some graduate courses.

There are also some caveats to be aware of. Since the modules use examples of violent and disturbing incidents from recent history, these materials may be more experience-near for some students than for others, and so content warnings are advised. While we believe that it is important to examine topics and issues that make us uncomfortable, it is also important to avoid provoking additional trauma in students who have been on the receiving end of digital extremism. By that same token, the classroom activities have been designed to minimize potential risks to students that could come from being identified by extremists. We discourage in the strongest possible terms including any assignments that require students to participate directly in online extremist spaces. Whenever possible, use of tools such as private/anonymous web browsing, virtual private networks (VPNs), and "dummy accounts," i.e., accounts created for the sole purpose of doing an activity, are recommended.

On a related note, there may be some students in your classes who are more vulnerable to digital extremists' persuasion than others. A useful lesson in this regard comes from sociologist Jessie Daniels in her 2009 book *Cyber Racism: White Supremacy Online and the New Attack on Civil Rights*. Daniels relates a story about teaching a course titled "Race and Ethnicity" in the fall of 1998 at a predominantly white, suburban university, in which students were encouraged to use the Internet for research on their chosen topics and to develop websites as part of their final class projects. In the course of doing their independent research, two students inadvertently found their way to extremist websites, one to the official page for the Knights of the Ku Klux Klan, and the other to a "cloaked website"—i.e., a site published by an individual or group who has intentionally concealed their authorship in order to hide an underlying political agenda—that appeared to provide biographical information about Dr. Martin Luther King, Jr., but was in fact a front for white supremacist propaganda. Elsewhere in the book, Daniels also describes how extremists are adept at "[initiating] innocuous threads to encourage people to join the conversation," which she notes is "a reliable strategy for getting 'lurkers' to move from passive to active engagement" (2009, 106). Without the proper contextual framing and careful monitoring of student research, those who are most susceptible to extremist messaging may be drawn in by these manipulation strategies.

Acknowledgements

This project would not have been possible without the generous support from UC Irvine's Office of Inclusive Excellence, and the efforts of researchers on digital extremism whose publications were invaluable resources. In particular, Dr. Joan Donovan, Director of the Technology and Social Change Research Project at Harvard Kennedy's Shorenstein Center, was instrumental in helping us conceptualize the modules and providing advice about topics and resources. We are also grateful for Sion Avakian's excellent work as an undergraduate research assistant in designing modules 5 and 6.