The Digital Revolution and the Demise of Democracy

Mitra V. Yazdi*

I. INTRODUCTION

Although Western society has long lauded democracy as the best form of governance for nation-states and the preservation of individual liberties, this system may have become outdated in the digital era. The fast-paced, viral nature of information in the digital age has outpaced the slow, bureaucratic nature of democracy. By contrast, authoritarian regimes have been able to capitalize on this new age of technology to reassert their dominance on a global scale. Without the many complications of a representative system, authoritarian regimes are able to address cyber incidents nearly as quickly as they occur. As developing countries struggle

* © 2021 Mitra V. Yazdi, J.D., Columbia Law School. Ms. Yazdi is an associate at White & Case, LLP in New York City, working in the Energy, Infrastructure, Project and Asset Finance division. Ms. Yazdi received her Juris Doctor in 2020 as a Harlan Fiske Stone Scholar, along with a Parker School Certificate for studies in International and Comparative Law. She served as the Editor-in-Chief of the *Columbia Journal of European Law* and worked briefly at the United States Court of International Trade while in law school. She has since focused on the implications of social media and technology law in a globalized economy and in particular on concepts of cyber governance and cyber warfare. Ms. Yazdi is highly involved in the Iranian-American community, and currently serves on the New York Planning Committee for the Iranian-American Women's Foundation and the New York Legal Committee of the National Iranian-American Council.

to come to terms with the impact they face from the Internet, many are desperately seeking governance solutions to reassert state control. Thus, the emergence of the cyber sphere has also provided global hegemons with a new battlefield, both for warfare and for influence.

This Article will seek to explore the viability of democracy in light of the challenges presented to it by the digital age. In particular, it will examine both the internal and external threats to sovereigns that have arisen as a result of the digital revolution. It will look at specific examples of domestic unrest caused by the lack of uniform online-content regulation as well as the proliferation of criminal activity resulting from anonymized Internet usage. In addition, it will demonstrate that the unclear bounds of the cyber sphere pose a unique threat to the exercise of national sovereignty and that the ubiquity of digital and Internet technologies has created a growing threat to national security. In light of these developing threats, this Article will look at the United States and other Western democracies in order to assess their ability to respond. It will show that such democratic systems are subtly eroding as a result of the digital revolution and have significantly expanded national security exceptions in order to have the flexibility necessary to compete with their authoritarian counterparts. As governance gaps have become ever more apparent, this Article will posit that authoritarian regimes, such as Russia and China, have risen to lead the charge in international fora. By advocating for cyber sovereignty and greater state control in the cyber sphere, these authoritarian powers have appealed to developing countries struggling to find their footing in this new world—offering them a set of tools with which to combat the threats unsettling them online. Ultimately, this analysis will demonstrate that the digital landscape has positioned authoritarian regimes to expand their global influence and will necessitate significant changes in the form and function of democracy going forward if it is to contend as a viable alternative.

II. INTERNAL THREATS—HATE SPEECH, ANONYMIZATION, AND UNDUE INFLUENCE

For thirteen consecutive years, Freedom House has documented "a decline in global freedom" as many countries have been trending towards "a new and more effective form of digital authoritarianism . . . [and]

digitally enabled social control."[1] Although in part this trend can be attributed to state actors, Pew Research polls showed that in fact a majority of people surveyed across thirty-eight countries (with the exception of Americans) were not in support of freedom of speech where such speech constituted hate speech against minorities or sexually explicit speech.[2] In response to increased instance of violence and misinformation online, "efforts to control speech and information [have been] accelerating, by both governments and private actors in the form of censorship, restrictions on access, and violent acts directed against those whose views or queries are seen as somehow dangerous or wrong."[3] Historically, the importance of freedom of speech has been recognized internationally as a fundamental right of individuals, to be preserved under Article 19 of the International Covenant on Civil and Political Rights (ICCPR),[4] as well as Article 19 of the Universal Declaration of Human Rights (UDHR).[5] However, it seems that today, the United States is alone in striving to maintain freedom of expression at all costs—"American law and judges are united, but all the cultural and social pressures around the world are in the opposite direction. The protections of the American Constitution and the demands of countries and consumers around the world are on a collision course."[6] As the consequences of completely liberated speech online continue to grow, the glaring regulatory gap does as well.

---

1. FREEDOM HOUSE, DEMOCRACY IN RETREAT: FREEDOM IN THE WORLD 2019 5 (2019), http://freedomhouse.org/sites/default/files/Feb2019_FH_FITW_2019_Report_ForWeb-compressed.pdf.

2. Richard Wike & Katie Simmons, *Global Support for Principle of Free Expression, but Opposition to Some Forms of Speech*, PEW RSCH. CTR. (Nov. 18, 2015), http://www.pewresearch.org/global/2015/11/18/global-support-for-principle-of-free-expression-but-opposition-to-some-forms-of-speech/.

3. *Free Speech*, HUM. RTS. WATCH, http://www.hrw.org/topic/free-speech# (last visited Apr. 12, 2021).

4. International Covenant on Civil and Political Rights art. 19(2), *opened for signature* Dec. 16, 1966, S. TREATY DOC. NO. 95-20 (1977), 999 U.N.T.S. 171 (entered into force Mar. 23, 1976) ("Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of [their] frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.").

5. Universal Declaration of Human Rights art. 19, G.A. Res. 217 (III), U.N. Doc. A/810, at 71 (Dec. 10, 1948) ("Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.").

6. Cecilia Kang, *It's U.S. vs. World as Big Tech Faces Specter of Limiting Speech Online*, N.Y. TIMES (Apr. 21, 2019), http://www.nytimes.com/2019/04/21/technology/facebook-zuckerberg-harmful-speech.html.

Although freedom of speech online has produced many goods, such as access to information and increased communication online, it has also produced significant harms that call into question the degree to which it should remain unbridled. The anonymity of speech online often "make[s] it easy for people to act antagonistically, unprofessionally, or unethically."[7] As a result, speech online behaves very differently than traditional forms of speech as it is somewhat detached from the speaker and is able to have a much greater impact as a result of the network effects spreading it quickly and extensively when viral. The proliferation of hate speech online demonstrates the dangers of online speech left to its own devices. The ability to participate in forums and social networks relatively anonymously not only emboldens extremists to voice their hateful opinions, but also gives them validation by creating echo chambers of confirmation bias online that reinforce their negative thoughts. Dangerous speech online ultimately translates into real world harm, as studies conducted found "a consistent positive association between Twitter hate speech targeting race and religion and offline racially and religiously aggravated offen[s]es."[8] As a result, many have struggled with finding the balance "between fighting hate speech on the one hand, and safeguarding freedom of speech on the other."[9] Calls for regulation of dangerous speech have largely sought to prevent violence by "inhibiting the speech, limiting its dissemination, undermining the credibility of the speaker, or 'inoculating' the audience against the speech so that they are less easily influenced by it."[10] However, such steps inherently require either a public or private body to determine what speech should be considered dangerous enough to merit such restraints. Thus far, the charge in Western democratic countries to limit hate speech has been led by private actors who have taken it upon themselves to develop policies defining hate speech and a means by which to enforce them. Tech giants such as Facebook, Google, Twitter, and Pinterest have all independently developed hate speech policies and begun monitoring and restricting content where they believe

7. Joe Dawson, *Who Is That? The Study of Anonymity and Behavior*, ASS'N FOR PSYCH. SCI. (Mar. 30, 2018), http://www.psychologicalscience.org/observer/who-is-that-the-study-of-anonymity-and-behavior.

8. Matthew L. Williams et al., *Hate in the Machine: Anti-Black and Anti-Muslim Social Media Posts as Predictors of Offline Racially and Religiously Aggravated Crime*, 60 BRIT. J. CRIMINOLOGY 93, 111 (2019).

9. *Hate Speech and Violence*, *European Commission Against Racism and Intolerance*, COUNCIL OF EUR., http://www.coe.int/en/web/european-commission-against-racism-and-intolerance/hate-speech-and-violence (last visited Apr. 12, 2021).

10. Peter Durand, *What Is Dangerous Speech?*, DANGEROUS SPEECH PROJECT, http://dangerousspeech.org/about-dangerous-speech/ (last visited Oct. 3, 2020).

such policies have been violated.[11] Facebook alone noted that in 2017, on average, the service "deleted around 66,000 posts reported as hate speech per week—that's around 288,000 posts a month globally . . . although it doesn't include posts reported for other reasons but deleted for hate speech."[12] However, this poses a problem for free speech in democratic nations as it allows private actors to restrict the speech of the public in impactful ways without requiring them to answer to state actors or the public itself.

The immense amount of power social media platforms have in shaping public discourse has been obviated by the treatment of politicized speech on Twitter. In the years following the election of President Trump, right wing groups increasingly claimed that Twitter and social media companies like it have chosen to utilize their monopoly over public speech in order to further their leadership's left-leaning agenda.[13] Beginning with the censorship of false information in the wake of the COVID-19 pandemic, Twitter radically altered its policy with regards to censorship of political speech and in particular the speech of public officials.[14] Originally having taken the stance that political officials should be exempt from censorship,[15] Twitter's sudden shift in tone seemed to verge on an

11. *See Hate Speech*, *Community Standards*, FACEBOOK, http://www.facebook.com/communitystandards/hate_speech/ (last visited Apr. 12, 2021) ("[W]e don't allow hate speech on Facebook. It creates an environment of intimidation and exclusion, and in some cases may promote offline violence."); *see also Community Guidelines,* GOOGLE, http://about.google/community-guidelines/ (last visited Apr. 12, 2021); *The Twitter Rules*, *Twitter Rules and Policies*, TWITTER, http://help.twitter.com/en/rules-and-policies/twitter-rules (last visited Apr. 12, 2021); *Community Guidelines*, PINTEREST, http://policy.pinterest.com/en/community-guidelines (last visited Apr. 12, 2021).

12. Richard Allan, *Hard Questions: Who Should Decide What Is Hate Speech in an Online Global Community?*, FACEBOOK: NEWSROOM (June 27, 2017), http://about.fb.com/news/2017/06/hard-questions-hate-speech/.

13. *Shannon Bond, Conservatives Flock To Mercer-Funded Parler, Claim Censorship On Facebook And Twitter*, NPR (Nov. 14, 2020, 6:38 PM), http://www.npr.org/2020/11/14/934833214/conservatives-flock-to-mercer-funded-parler-claim-censorship-on-facebook-and-twi.

14. Kim Lyons, *Twitter Removes Tweets by Brazil, Venezuela Presidents for Violating COVID-19 Content Rules*, THE VERGE (Mar. 30, 2020, 5:00 PM), http://www.theverge.com/2020/3/30/21199845/twitter-tweets-brazil-venezuela-presidents-covid-19-coronavirus-jair-bolsonaro-maduro.

15. Kenrick Cai, *Facebook Will Let Politicians Violate Its Rules on Speech, Taking a Page From Twitter*, FORBES (Sept. 24, 2019), http://www.forbes.com/sites/kenrickcai/2019/09/24/facebook-political-speech-community-standards-twitter/?sh=1ae1c9ba4e56 (discussing Twitter's statement in June 2019 that "it would not prohibit politicians' tweets that violated its rules, if the politician met certain criteria for noteworthiness. For Twitter-verified government officials with more than 100,000 followers, the company instead introduced a notice to preface these tweets that

attempt to control public discourse and shape the narrative of online speech.[16] The extension of censorship to former president, Donald Trump, perhaps symbolized Twitter's most inflammatory exercise in seeking to balance power and public responsibility "in an escalating row between Twitter and the White House," the company began by hiding Trump's tweets behind a warning that it violated the platform's rules about glorifying violence, but ultimately allowed the tweet to remain accessible, "in the public's interest."[17] Encouraged by activists and media outlets to exercise greater control over the channel of communication it provided for the President, Twitter ultimately removed President Trump's account from the platform following riots at the Capitol that were linked to his online activity.[18] Twitter's decision to not only censor, but ultimately suspend the President's right to speech on its platform makes explicit the amount of power that it has in public fora because it demonstrates the unilateral control that an unelected private actor can exercise at will over the most powerful democratically elected official.[19] Colloquially thought of as the most powerful man in the world, the former President of the United States was found to have little ground to stand on against the authority of a social media giant, raising the inevitable question of whether our legal doctrines are equipped to address, "highly concentrated, privately owned information infrastructure such as digital platforms."[20]

The business decisions of corporations like Facebook also have far-reaching ramifications for the property and civil liberty rights of consumers. Facebook, for example, collects an incredible amount of data on its users, developing profiles to later be utilized for advertising

---

states: 'The Twitter Rules about abusive behavior apply to this Tweet. However, Twitter has determined that it may be in the public's interest for the Tweet to remain available.'").

16. Justin Wise, *Appeals Court Rejects Claims that Facebook, Twitter Suppress Conservative Views*, THE HILL (May 27, 2020, 5:10 PM), http://thehill.com/policy/technology/499808-appeals-court-rejects-claim-facebook-twitter-suppress-conservative-views?rl=1.

17. Rory Cellan-Jones, *Twitter Hides Trump Tweet for "Glorifying Violence"*, BBC NEWS (May 29, 2020), http://www.bbc.com/news/technology-52846679.

18. Kate Conger & Mike Isaac, T*witter Permanently Bans Trump, Capping Online Revolt*, N.Y. TIMES (Jan. 12, 2021), http://www.nytimes.com/2021/01/08/technology/twitter-trump-suspended.html.

19. *Permanent Suspension of @realDonaldTrump*, TWITTER: BLOG (Jan. 8, 2021), http://blog.twitter.com/en_us/topics/company/2020/suspension.html (explaining the decision-making process at Twitter that led to the ultimate removal of the President's account).

20. Andrew Chung & Lawrence Hurley, *U.S. Supreme Court Brings End to Trump Twitter Fight*, REUTERS (Apr. 17, 2017, 9:14 AM), http://www.reuters.com/article/us-usa-court-trump-twitter/u-s-supreme-court-brings-end-to-trump-twitter-fight-idUSKBN2BS19X (quoting Biden v. Knight First Amendment Inst. at Columbia Univ., 141 S. Ct. 1220, 1221 (2021) (Thomas, J., concurring)).

purposes[21] Facebook user profiling allows advertisers to target individuals who might be more susceptible to purchasing their products and to exclude others; "affiliates once had to guess what kind of person might fall for their unsophisticated cons, targeting ads by age, geography, or interests. Now Facebook does that work for them."[22] This detailed profiling allows not only for greater targeting of legitimate advertising but also the growth of a multitude of Internet scams that prey on ignorant consumers— "[t]he social network tracks who clicks on the ad and who buys the pills, then starts targeting others whom its algorithm thinks are likely to buy . . . Because Facebook is so effective at vacuuming up people and information about them, anyone who lacks scruples and knows how to access the system can begin to wreak havoc or earn money at astonishing scale."[23] However, in addition to assisting in the dissemination of widespread fraud and marketing ploys, the profiling of consumers also facilitates discrimination among them, which can be especially problematic where sensitive areas such as housing and employment are concerned. Over the past year, Facebook has come under fire for violating the Fair Housing Act by "enabling discrimination in housing ads based on 'race, color, religion, sex, familial status, national origin and disability.'"[24] In filing an official complaint against the tech giant, the Department of Housing and Urban Development alleged that Facebook provided advertisers "with tools to define which users . . . the advertiser would like to see an ad . . . [and provided] drop-down menus and search boxes to exclude or include . . . people who share specified attributes . . . [and that Facebook] alone, not the advertiser, determine[d] which users [would] constitute the 'actual audience' for each ad."[25] Furthermore, the complaint alleged that the algorithmic software developed by Facebook to deliver targeted advertisements would "not show the ad to a diverse audience if the system consider[ed] users with particular characteristics most likely to engage

21. Caitlin Dewey, *98 Personal Data Points That Facebook Uses to Target Ads to You,* WASH. POST (Aug. 19, 2016, 9:13 AM), http://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/.

22. Zeke Faux, *How Facebook Helps Shady Advertisers Pollute the Internet*, BLOOMBERG (Mar. 27, 2018, 5:00 AM), http://www.bloomberg.com/news/features/2018-03-27/ad-scammers-need-suckers-and-facebook-helps-find-them.

23. *Id.*

24. Caroline Haskins, *Facebook Charged for Discriminatory Housing Ads by Department of Housing and Urban Development,* VICE (Mar. 28, 2019, 10:01 AM), http://www.vice.com/en_us/article/wjm399/department-of-housing-charges-facebook-for-discriminatory-housing-ads.

25. Charge of Discrimination at 4, Sec'y of U.S. Dep't of Hous. & Urb. Dev. v. Facebook, Inc., FHEO No. 01-18-0323-8 (Mar. 28, 2019).

with the ad . . . because [Facebook] structured its ad delivery system such that it generally will not deliver an ad to users whom the system determines are unlikely to engage with the ad, even if the advertiser explicitly wants to reach those users regardless."[26] Thus, the algorithm caused discriminatory advertisement even where advertisers might not have intended such disparate impact to take place. In response to such claims, Facebook purportedly has taken steps to remove many ad targeting options in order to prevent discriminatory effects, however it is unclear to what extent such changes have in fact been successful at eliminating machine learned biases in practice.[27]

Furthermore, Facebook is not alone in creating distortions in the marketplace that might contribute to discrimination among online users on the basis of race, sex, or other protected attributes. Technologies such as machine learning (ML) and artificial intelligence (AI) in particular have been linked to discrimination where they magnify structural patterns of bias that are learned out of context through human inputs. Although such disparate impacts can be observed in testing, prior to the release of an algorithm, often they are only realized after a harm is incurred. Amazon sought to develop a recruiting tool that would be able to review resumes "by observing patterns in resumes submitted to the company over a 10-year period. Most came from men, a reflection of male dominance across the tech industry."[28] The software developed by Amazon, however, was not able to distinguish the historical bias of male dominance from a legitimate correlate to positive job performance, and thus, "taught itself that male candidates were preferable" and "penalized resumes that included the word 'women's.'" [29] As a result, "Amazon edited the programs to make them neutral to these particular terms. But that was no guarantee that the machines would not devise other ways of sorting candidates that could prove discriminatory."[30] While Amazon was able to determine in this instance that biases were being magnified by its technology and isolate the cause, such subtle malfunctions often go

26. *Id.*

27. D. Lumb, *Facebook Removes 5,000 Ad Targeting Options to Prevent Discrimination*, ENGADGET (Aug. 21, 2018), http://www.engadget.com/2018/08/21/facebook-removes-5-000-ad-targeting-options-to-prevent-discrimin/.

28. Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women*, REUTERS (Oct. 10, 2018, 6:04 PM), http://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

29. *Id.*

30. *Id.*

unnoticed as the correlates involved in decision making become increasingly nuanced and complex. Predictive uses of ML and AI technology pose even greater risks of reinforcing harmful feedback loops because "where a problem exists, it will be worse and more durable" due to the scalability of algorithms.[31] "The ability of these algorithmic processes to scale, and therefore to influence decisions uniformly and comprehensively, magnifies any error or bias that they embody."[32] As a result, "instead of eliminating bias, too often these algorithms depend on biased assumptions or data that can actually reinforce discrimination against women and people of color," and in turn worsen such disparities by producing outputs that further influence the inputs they receive back from the outside world in the same direction.[33]

Without greater information about the data utilized in algorithmic decision-making processes, there is no way to distinguish how and why the biased effects from algorithmic decision making come about. While private companies do not currently owe the same level of fairness or due process to citizens as government agencies in their decision-making processes, algorithmic technology has given private actors the ability to have a much more severe impact on the livelihood and opportunities of their consumers than ever before, making them nearly as influential as their public counterparts, if not more. Technological redlining, a term used to describe the pattern of discrimination against protected classes as a result of algorithmic decision making, "occurs because we have no control over how data is used to profile us. If bias exists in the data, it is replicated in the outcome. Without enforceable mechanisms of transparency, auditing, and accountability, little can be known about how algorithmic decision-making limits or impedes civil rights."[34] Thus far, cases of documented discrimination and distorted information have been uncovered primarily by civil rights groups and journalists that have sought to test the bounds of technology where they stumbled upon anecdotal evidence indicating something may be amiss. Yet, reliance on such

31. Robert Brauneis & Ellen P. Goodman, *Algorithmic Transparency for the Smart City*, 20 YALE J.L. & TECH. 103, 129 (2018).

32. *Id.*

33. Adi Robertson, *A New Bill Would Force Companies to Check their Algorithms for Bias*, THE VERGE (Apr. 10, 2019, 3:52 PM), http://www.theverge.com/2019/4/10/18304960/congress-algorithmic-accountability-act-wyden-clarke-booker-bill-introduced-house-senate.

34. ROBYN CAPLAN ET AL., DATA & SOC'Y, ALGORITHMIC ACCOUNTABILITY: A PRIMER 7-8 (2018), http://datasociety.net/wp-content/uploads/2018/04/Data_Society_Algorithmic_Accountability_Primer_FINAL-4.pdf.

independent actors to serve as watchdogs is unsustainable at scale, where the proliferation of social media and technology platforms has resulted in private actors controlling the most critical information channels used by citizens today. "[R]estraint of speech [online]," where utilized to limit false information and prevent market distortions, "can come from governments forcing algorithmic changes, from organizations purchasing audiences on platforms, or from platform companies tweaking their algorithms for whatever reason they deem fit. Regardless, the opaque nature of this filtering presents a challenge to . . . democratic society."[35] Such important decisions, capable of swaying entire elections and impacting individuals' livelihoods, cannot and should not be left solely to the discretion of politically unaccountable corporate actors.

III. EXTERNAL THREATS—DISINFORMATION, DESTABILIZATION, AND THE CYBER WARFARE

The deanonymization of the Internet and ease of access with which it connects people from different countries also provides an opportunity for foreign persons to influence domestic affairs. In a democracy this effect can be particularly damaging as the governance system is heavily reliant on free and fair elections. Where foreign influence is present, the integrity of domestic elections may be called into questions, and by extension the legitimacy of the leadership ultimately elected. This threat of election interference was made ever more clear during the 2016 presidential election cycle, where the proliferation of "fake news" on social media was highlighted by many as a potentially significant determinant in the ultimate election of Donald J. Trump. Facebook's newsfeed in particular was isolated as the culprit largely responsible for propagating such stories by allowing for widespread sharing and promotion of fake headlines that may have influenced voters' perceptions of the candidates in the days leading up to the election.[36] Reports indicated that during the election cycle, falsified Russian backed Facebook posts had reached as many as 126 million Americans through the platform.[37] Even more damaging, Facebook's policies and technology were found to have allowed the

35. EMILY BELL & TAYLOR OWEN, THE PLATFORM PRESS: HOW SILICON VALLEY REENGINEERED JOURNALISM 83 (2017).

36. David Stockdale, *Why We Should Hold Facebook Responsible for Fake News,* CTR. FOR DIGIT. ETHICS & POL'Y (Mar. 22, 2017), http://www.digitalethics.org/essays/why-we-should-hold-facebook-responsible-fake-news.

37. Olivia Solon & Sabrina Siddiqui, *Russia-Backed Facebook Posts 'Reached 126m Americans' During U.S. Election*, THE GUARDIAN (Oct. 30, 2017, 9:26 PM), http://www.theguardian.com/technology/2017/oct/30/facebook-russia-fake-accounts-126-million.

political consulting firm Cambridge Analytica to take advantage of millions of users personal information and data to manipulate the information received by them throughout the election in order to influence their opinions of the candidates.[38] As a result of these incidents, Facebook has taken a number of steps to attempt to rectify their reputation and mitigate the potential for misinformation on their platform,[39] following the lead of other large tech companies like Google, by attempting to promote high quality content through algorithmic decision making that ranks pages in accordance with perceived markers of credibility and explicitly warning users where they believe the sources may be fake.[40]

In addition to the criticism Russia received for interfering in the U.S. Presidential Election, the Kremlin has also been accused of seeking "to influence voter behavior and, in some cases, suppress turnout," in European elections.[41] Furthermore, President Trump openly chastised the Chinese government for engaging in cyber espionage and misinformation tactics that sought to undermine him and destabilize the country.[42] The Coronavirus pandemic has only made the dangers of the proliferation of misinformation more abundantly clear. In countries all over the world, government authorities "say they've seen a flood of misinformation on WhatsApp [among other platforms] about the number of people affected by coronavirus, the way the illness is transmitted and the availability of

38. Julia Carrie Wong, *Facebook Acknowledges Concerns Over Cambridge Analytica Emerged Earlier Than Reported*, THE GUARDIAN (Mar. 21, 2019, 10:01 PM), http://www.theguardian.com/uk-news/2019/mar/21/facebook-knew-of-cambridge-analytica-data-misuse-earlier-than-reported-court-filing.

39. Adam Mosseri, *Working to Stop Misinformation and False News*, FACEBOOK: NEWSROOM (Apr. 6, 2017), http://www.facebook.com/facebookmedia/blog/working-to-stop-misinformation-and-false-news; Jacob Kastrenakes, *Facebook Will Punish Groups for Repeatedly Spreading Fake News*, THE VERGE (Apr. 10, 2019, 1:00 PM), http://www.theverge.com/2019/4/10/18304739/facebook-groups-reduce-misinformation-harmful-content-changes-messenger.

40. Salvador Rodriguez, *Facebook is Taking a Page Out of Google's Playbook to Stop Fake News from Going Viral*, CNBC (Apr. 10, 2019, 7:47 PM), http://www.cnbc.com/2019/04/10/facebook-click-gap-google-like-approach-to-stop-fake-news-going-viral.html.

41. Michael Birnbaum & Craig Timberg, *E.U.: Russians Interfered in Our Elections, Too*, WASH. POST (June 14, 2019, 3:18 PM), http://www.washingtonpost.com/technology/2019/06/14/eu-russians-interfered-our-elections-too/.

42. Ellen Nakashima & David J. Lynch, *Trump Administration to Condemn China Over Hacking and Economic Espionage, Escalating Tensions Between Superpowers*, WASH. POST (Dec. 11, 2018, 10:35 AM), http://www.washingtonpost.com/world/national-security/trump-administration-to-condemn-china-over-hacking-and-economic-espionage-escalating-tensions-between-superpowers/2018/12/11/699e375c-f985-11e8-8d64-4e79db33382f_story.html.

treatments."[43] In India, YouTube videos detailing conspiracy theories about the virus were able to rack up millions of views before Google even became aware of the misinformation and took them down.[44] Countries like Russia, with complicated histories of censorship, have received public criticism for seeking to censor false information about the virus where they believe it might "sow panic among the public and provoke public disturbance,"[45] however, by contrast, private actors have been criticized where they've failed to censor false information or haven't taken action quickly enough.[46] A European study on disinformation around the world with regards to the novel Coronavirus found that many conspiracy theories advocated in different parts of the world seemed to be politically motivated, and believed that much of the disinformation targeted at Europe was the product of Russian efforts to destabilize the region as it was "characteristic of the Kremlin's well-established strategy of using disinformation to amplify divisions, sow distrust and chaos, and exacerbate crisis situations and issues of public concern."[47]

Despite originally denying that its platform was capable of causing large-scale harm, Facebook and other social media platforms have now openly admitted that "algorithms and filters on social media have gravely limited the content people see. [I]t is where an astounding number of people get their news. Indeed, forty-four percent of the general population of the United States claimed to get news from the site."[48] Self-policing of such platforms has only begun to occur as a matter of public outrage, rather than as a legal requirement. Good faith attempts at regulating and restricting harmful content are far from comprehensive,

---

43. Tony Romm, *Fake Cures and Other Coronavirus Conspiracy Theories are Flooding WhatsApp, Leaving Governments and Users with a 'Sense of Panic'*, WASH. POST (Mar. 2, 2020, 9:58 AM), http://www.washingtonpost.com/technology/2020/03/02/whatsapp-coronavirus-misinformation/.

44. Ryan Broderick & Pranav Dixit, *India is in The Middle of a Coronavirus YouTube Frenzy, and It's Going to Get People Killed*, BUZZFEED NEWS (Feb. 19, 2020, 4:23 PM), http://www.buzzfeednews.com/article/ryanhatesthis/the-most-popular-youtube-videos-about-the-coronavirus-are.

45. *CPJ Calls on Russia To Stop Censoring News Outlets Reporting on COVID-19*, RADIOFREEEUROPE/RADIOLIBERTY (Mar. 25, 2020, 12:26 AM), http://www.rferl.org/a/cpj-calls-on-russia-to-stop-censoring-news-outlets-reporting-on-covid-19/30507738.html.

46. Casey Newton, *Tech Companies Are Getting More Aggressive to Fight COVID-19 Hoaxes*, THE VERGE (Mar. 5, 2020, 4:23 PM), http://www.theverge.com/interface/2020/3/5/21164683/covid-19-tech-response-facebook-google-twitter-microsoft-youtube-whatsapp.

47. *EEAS Special Report: Disinformation on the Coronavirus—Short Assessment of the Information Environment*, EUVSDISINFO (Mar. 19, 2020), http://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/?fbclid=IwAR1UVFvKFuku3xaTHyncX38Ud5i4Tl6Ko_OSZhGRJPBHZ6evMLk1qVNx5yY.

48. Stockdale, *supra* note 36.

only addressing some of the many ways that algorithmic information sharing can be manipulated to cause harm.[49] Social media companies are also wary to engage in widespread policing of disinformation as such actions could quickly devolve into broader censorship, thus they have taken a milder stance: "whether or not a Facebook post is accurate is not itself a reason to block it. Human rights law extends the same right to expression to those who wish to claim that the world is flat as to those who state that it is round—and so does Facebook. . . . And rather than blocking content for being untrue, [they] demote posts in the News Feed when rated false by fact-checkers and also point people to accurate articles on the same subject."[50] However, online propaganda still poses a serious threat to governments as it can "spread much faster and can reach more people in the target audience" than traditional offline propaganda and requires that authorities "react much more quickly and precisely when accusations start to spread via social media channels."[51] Most concerning, extremist posts and in particular those coming from the far right seem to garner the greatest amount of engagement from users, nearly double that of other political posts.[52] This phenomenon has been further exacerbated, and in some cases weaponized by government actors that have realized that utilizing cyber propaganda can serve as a valuable new tool in their arsenals and "[e]ven traditional bastions of [I]nternet freedom have deployed . . . 'informational tactics' to manipulate elections, meaning the coordinated use of hyperpartisan commentators, bots or news sites to disseminate false content, often with the backing of the government or a political party apparatus. The countries using those tactics over the past year included the United States, Australia, Hungary, and Italy."[53]

---

49. Ryan Mac, *Literally Just a Big List of Facebook's 2018 Scandals*, BUZZFEED NEWS (Dec. 20, 2018, 10:10 AM), http://www.buzzfeednews.com/article/ryanmac/literally-just-a-big-list-of-facebooks-2018-scandals.

50. Richard Allan, *Hard Questions: Where Do We Draw the Line On Free Expression?*, FACEBOOK: NEWSROOM (Aug. 9, 2018), http://about.fb.com/news/2018/08/hard-questions-free-expression/.

51. Gregor Kutzschbach, *Digital Propaganda and Cyber Threats: The Role of Politics and the State*, AM. INST. FOR CONTEMP. GERMAN STUD., JOHNS HOPKINS UNIV. (Sept. 26, 2018), http://www.aicgs.org/2018/09/digital-propaganda-and-cyber-threats-the-role-of-politics-and-the-state/.

52. Lateshia Beachum, *Far-Right Sources on Facebook Get More Engagement Than Any Other Political Posts, Study Finds*, WASH. POST (Mar. 4, 2021, 6:19 PM), http://www.washingtonpost.com/technology/2021/03/04/far-right-extreme-study-facebook/.

53. David Ingram, *More Governments than Ever are Using Social Media to Push Propaganda, Report Says*, NBC NEWS (Nov. 5, 2019 12:38 AM), http://www.nbcnews.com/tech/tech-news/more-governments-ever-are-using-social-media-push-propaganda-report-n1076301.

The cyber sphere has also presented a myriad of other threats to governments by presenting them with a new battlefield, albeit one with no existing rules. In 2017, the pharmaceutical giant Merck & Co. experienced a $1.3 billion cyberattack that was allegedly traced back to Russia, and has been argued as constituting an "an act of war," at least in civil trial.[54] Although not explicitly acknowledged as such by a government entity, this attack has been thought to follow in the steps of many other obfuscated state-sponsored hacks—"[n]ation-states for years have been developing digital tools to create chaos in a time of war: computer code that can shut down ports, tangle land transportation networks, and bring down the electrical grid. But increasingly those tools are being used in forms of conflict that defy categorization."[55] Cyber warfare, unlike traditional warfare, is less suited to peace agreements and bilateral treaties as "it is difficult to measure the relative strength of states in cyberspace; there is uncertainty regarding the military effects of cyber technology; the challenges of monitoring compliance; and difficulties with enforcement."[56] Furthermore, cyber threats may also take on the form of subtle espionage, often targeting or using corporations as proxies for nation-states.[57] Even when cyber attacks are directly aimed at nation-states, the complicated nature of these digital weapons is such that they may go unnoticed for long periods of time or be difficult to attribute to those responsible once discovered. The infamous 2010 Stuxnet attack on Iran's nuclear plants (allegedly by the United States and Israel) is considered by some to be "the world's first digital weapon."[58] The clever code, targeted Microsoft Windows machines and networks, repeatedly replicating itself. Then it sought out Siemens Step7 software . . . used to program industrial control systems that operate equipment, such as centrifuges. Finally, it compromised the programmable logic controllers. [Its] authors could thus spy on the industrial systems and even cause the fast-spinning centrifuges

54. David Voreacos et al., *Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?*, BLOOMBERG (Dec. 3, 2019, 4:03 PM), http://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war?sref=WdMLv1YI.

55. *Id.*

56. Erica D. Borghard & Shawn W. Lonergan, *Why Are There No Cyber Arms Control Agreements?*, COUNCIL ON FOREIGN RELS.: NET POLITICS BLOG (Jan. 16, 2018, 10:11 AM), http://www.cfr.org/blog/why-are-there-no-cyber-arms-control-agreements.

57. *See* Chris Bing, *Chinese Hackers Starting to Return Focus to U.S. Corporations*, CYBERSCOOP (Nov. 6, 2017), http://www.cyberscoop.com/keyboy-dde-pwc-microsoft-word-rtf/.

58. Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014, 6:30 AM), http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

to tear themselves apart, unbeknownst to the human operators at the plant.[59]

The even greater danger lurking in the use of such digital weaponry, however, is that once released "[t]hat malware is now out in the public spaces and can be reverse engineered" thus giving access to these incredibly powerful tools to both public and private actors that might be seeking to do harm.[60] In the United States, the SolarWinds hack demonstrated just how vulnerable government systems can be due to the interconnected nature of our technological infrastructure. Suspected as an attack by Russian intelligence, hackers were able to infiltrate American nuclear facilities as a result of malware planted "in a routine software upgrade from a Texas-based I.T. company called SolarWinds, which provides network-management," and gave the hackers access to such customers' networks for at least nine months before being detected.[61] The problem with cyber warfare thus is two-fold, in that the weapons deployed are increasingly dangerous, but they also call for defense mechanisms that run far beyond investment in solely government entities – "[m]any of the factors that make developing a centralized national cyber defense challenging lie outside of the government's direct control . . . . [E]conomic forces push technology companies to get their products to market quickly, which can lead them to take shortcuts that undermine security . . . . It's unreasonable to expect any U.S. company to be able to fend for itself against a foreign nation's cyberattack."[62]

It is thus not surprising that countries have increasingly sought to invest greater amounts of money in the development of national champions in the tech space such that they can compete on a global scale where necessary. The United States and China in particular have both spent a great deal of money seeking to limit each other's technological influence globally. The United States for example, which has viewed the Chinese tech giant Huawei as a growing threat in the 5G landscape,

---

59. David Kushner, *The Real Story of Stuxnet*, IEEE SPECTRUM (Feb. 26, 2013, 2:00 PM), http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

60. *Id.*

61. Sue Halpern, *After the SolarWinds Hack, We Have No Idea What Cyber Dangers We Face*, The New Yorker (Jan. 25, 2021), http://www.newyorker.com/news/daily-comment/after-the-solarwinds-hack-we-have-no-idea-what-cyber-dangers-we-face.

62. Terry Thompson, *The SolarWinds Hack Was All But Inevitable – Why National Cyber Defense is a 'Wicked' Problem and What Can Be Done About It*, THE CONVERSATION (Feb. 9, 2021, 8:31 AM), http://theconversation.com/the-solarwinds-hack-was-all-but-inevitable-why-national-cyber-defense-is-a-wicked-problem-and-what-can-be-done-about-it-153084.

established the United States International Development Finance Corporation (DFC) which, "plans to tap some of its $60 billion budget to help developing countries and businesses purchase equipment from other companies . . . [concerned that] Huawei and ZTE gear could be used for spying, an allegation the companies have denied."[63] The DFC, specifically charged with, "helping to advance U.S. foreign policy by countering the growing influence of authoritarian regimes,"[64] notes that, "China is also invested in the technology race through the spread of Internet access and development of 5G technology, which poses international security risks . . . [and] is a full-fledged soft power competitor throughout [Asia] and elsewhere."[65]

Although the United States has historically dominated the global tech industry, China's rise as a "cyber superpower" has called into question the status quo.[66] Furthermore, China has continued to expand its reach in the developing world through the Belt and Road Initiative and has specifically sought to enhance, "cooperation in areas of communication via enhanced technologies such as 5G networks . . . integration via modern technologies, and develop[] exchanges and cooperation with international media."[67] China has even gone so far as to invest in the critical resources necessary to develop new technologies. Cobalt, soon to be one of the world's most important natural resources, is a critical input in the manufacture of batteries—making it essential to manufacturers of technological hardware (such as smartphones, laptops, etc.).[68] Although the majority of the world's cobalt reserves are located in the Democratic Republic of Congo, the weak political climate has allowed China to develop a dominant position in the

---

63. Alistair Barr, *U.S. to Tap $60 Billion War Chest in Boon for Huawei Rivals*, BLOOMBERG (Dec. 3, 2019, 10:59 AM), http://www.bloomberg.com/news/articles/2019-12-03/u-s-to-tap-60-billion-war-chest-in-boon-for-huawei-rivals?cmpid=BBD120419_TRADE&utm_medium=email&utm_source=newsletter&utm_term=191204&utm_campaign=trade.

64. *Adam S. Boehler Confirmed as CEO of U.S. International Development Finance Corporation*, U.S. INT'L DEV. FIN. CORP. (Sept. 26, 2019), http://www.dfc.gov/media/press-releases/adam-s-boehler-confirmed-first-ceo-us-international-development-finance.

65. DANIEL F. RUNDE ET. AL., CTR. FOR STRATEGIC & INT'L STUD., STRATEGIC DIRECTIONS FOR THE UNITED STATES INTERNATIONAL DEVELOPMENT FINANCE CORPORATION (DFC) 7 (Sept. 2019), http://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190923_Runde BanduraMurphy_USDFC_WEB.pdf.

66. Adam Segal, *When China Rules the Web*, FOREIGN AFFS. (Sept./Oct. 2018), http://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web.

67. Cao Desheng, *Technology Cooperation Under Belt, Road Urged*, CHINA DAILY (Apr. 23, 2019), http://www.chinadaily.com.cn/a/201904/23/WS5cbe6598a3104842260b7a9c.html.

68. James Conca, *Blood Batteries – Cobalt and the Congo*, FORBES (Sept. 26, 2018, 6:00 AM), http://www.forbes.com/sites/jamesconca/2018/09/26/blood-batteries-cobalt-and-the-congo/#25af22abcc6e.

region and thus, "control one of the world's key sources" of cobalt through, 'dollar diplomacy,'" whereby the Chinese regime provides large sums of loans and investments to foreign countries in order to exert its influence in the region."[69] With such leverage, China can begin to exert the same kind of global influence that the United States and its Middle Eastern allies have sought to impose as a result of their domination in the oil and gas industries.

It should be noted that democracies are much more susceptible to the external threats discussed above than their authoritarian counterparts because they inherently separate the state and the economy, and impose checks and balances that prevent unilateral action in foreign affairs. As a result, even where democratic nations pour resources into supporting homegrown tech companies, they cannot dictate how such companies utilize their talents. For example, "some of the biggest names in [U.S.] technology have provided components, financing and know-how to China's multibillion-dollar surveillance industry."[70] Although China may find it advantageous to ensure the entry of its largest tech companies into foreign markets, it does so with the knowledge that it is both a financial stakeholder in the company as well as often a primary decision maker.[71] Thus, China, unlike the United States, can ensure that where its companies conduct economic activity abroad, they do so in its best interest and are willing to utilize whatever data they collect in the process to assist the Chinese government where required. The United States, by contrast, cannot even force its own tech companies to work within its military interests domestically. For example, where dissenting employees were uncomfortable working under a Department of Defense contract, Google issued guidelines saying it will not apply AI to "[w]eapons or other technologies whose principal purpose or implementation is to cause or directly facilitate injury to people," severely limiting its role in the

69. Frank Fang, *China Takes Control of Cobalt Mines as It Advances Its Battery Industry for Electric Vehicles*, THE EPOCH TIMES (Aug. 21, 2018), http://www.theepochtimes.com/china-takes-control-of-cobalt-mines-as-it-advances-its-battery-industry-for-electric-vehicles_2622794.html.

70. Liza Lin & Josh Chin, *U.S. Tech Companies Prop Up China's Vast Surveillance Network*, WALL ST. J. (Nov. 26, 2019, 11:47 AM), http://www.wsj.com/articles/u-s-tech-companies-prop-up-chinas-vast-surveillance-network-11574786846?mod=hp_lead_pos11.

71. Jennifer Hughes, *China's Communist Party Writes Itself into Company Law*, FIN. TIMES (Aug. 14, 2017), http://www.ft.com/content/a4b28218-80db-11e7-94e2-c5b903247afd ("China's Communist party is writing itself into the articles of association of many of the country's biggest companies . . . . New phrases . . . include describing the party as playing a core role in 'an organi[z]ed, institutionali[z]ed and concrete way' and 'providing direction and managing the overall situation.'").

project.[72] Democratic governments are also limited in their ability to restrain the influence of foreign states within their own borders. By contrast, studies have shown time and again that Chinese funding has been funneled into Western universities in order to pursue research that ultimately assists the People's Republic in maintaining an authoritarian state.[73] In addition, in a democracy such as that of the United States, war-making power is given to Congress, and the extent of the powers of the President as Commander in Chief outside of war times has long been debated.[74] Thus, where cyber warfare is obfuscated and covert, assessing what actions a democratic government is authorized to take and how becomes quite difficult and requires a novel approach to diplomacy in order to remain effective.[75]

IV. DEMOCRATIC RESPONSES—DEFICIENCIES OF SPEED, SCALE, AND SUSTAINABILITY

Despite private corporations and citizens advocating for states to take the reins on fleshing out standards for online content regulation, thus far many Western governments have been hesitant to tread into such territory, but where they have, their responses have been relatively weak.[76] In the European Union some rules for online content regulation have emerged

---

72. Sundar Pichal, *AI at Google: Our Principles*, GOOGLE: BLOG (June 7, 2018), http://www.blog.google/technology/ai/ai-principles/; *see also* Tom Simonite, *Google Sets Limits on Its Use of AI but Allows Defense Work*, WIRED (June 7, 2018, 4:17 PM), http://www.wired.com/story/google-sets-limits-on-its-use-of-ai-but-allows-defense-work/.

73. Ellen Barry, *U.S. Accuses Harvard Scientist of Concealing Chinese Funding*, N.Y. TIMES (Jan. 28, 2020), http://www.nytimes.com/2020/01/28/us/charles-lieber-harvard.html; Charles Rollet, *Western Academia Helps Build China's Automated Racism*, CODA (Aug. 6, 2019), http://www.codastory.com/authoritarian-tech/western-academia-china-automated-racism/.

74. *Power to Declare War*, HIST., ART & ARCHIVES, U.S. HOUSE OF REPRESENTATIVES, (first quoting U.S. CONST. art. I, § 8, cl. 1. ("The Congress shall have Power To . . . provide for the common Defence and general Welfare of the United States."); then citing LOUIS FISHER, PRESIDENTIAL WAR POWER 1-4 (1995)) ("The framers of the Constitution—reluctant to concentrate too much influence in the hands of too few—denied the office of the President the authority to go to war unilaterally. If America was going to survive as a republic, they reasoned, declarations of war required careful debate in open forums among the public's representatives.").

75. David P. Fidler, *Year in Review: The Trump Administration Disrupts U.S. Cyber Diplomacy*, COUNCIL ON FOREIGN RELS.: NET POLITICS BLOG (Dec. 18, 2017, 10:20 AM), http://www.cfr.org/blog/year-review-trump-administration-disrupts-us-cyber-diplomacy (describing the United States' efforts at passing legislation that would allow for greater oversight of cyber issues and reorganization under the State Department).

76. *Mark Zuckerberg Stands for Voice and Free Expression*, FACEBOOK: NEWSROOM (Oct. 17, 2019), http://about.fb.com/news/2019/10/mark-zuckerberg-stands-for-voice-and-free-expression/ (quoting Zuckerberg as stating, "in general, I don't think it's right for a private company to censor politicians or the news in a democracy. . . . [A]s a principle, in a democracy, I believe people should decide what is credible, not tech companies.").

(to be discussed in Section V), while in the United States, no such government policy has been enacted. Regulatory efforts in the United States with regard to algorithmic transparency and accountability have also been limited and largely restricted to public use cases of such technology. Criticisms of algorithmic software used in criminal trials, and sentencing in particular, have created cause for concern with regards to citizens' civil liberties.[77] Legal scholars have argued that "due process requires that those who deprive individuals of liberty interest do so without unwarranted bias or direct financial interest in the outcome," and have called for algorithmic decision-making to provide users with, "procedural data due process . . . [to] ensur[e] greater fairness with predictive analytics."[78] In the United States, the Supreme Court has held that the Constitution requires administrative agencies and government actors to provide due process where they risk causing an erroneous deprivation of rights through decision-making:

> due process generally requires consideration of three distinct factors: First, the private interest that will be affected by the official action; second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail.[79]

In algorithmic decision-making, the risk of erroneous deprivation can be extremely high as automated processes are often not properly understood or monitored by the human elements utilizing them. While utilization of algorithmic technology and automation eases the government's administrative burden, the private interest of individuals affected by such algorithmic decision-making is arguably of much greater import. This is made particularly evident in the case of software used in criminal adjudications and sentencing where a flawed algorithm can result

77. Caplan et al., *supra* note 34, at 6. For example, the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) system came under fire for delivering discriminatory results, "because of the bias embedded in the training data. Because black people have historically been arrested at a higher rate than white people, COMPAS learned to predict that a black person is more at risk of being re-arrested than a white person . . . injecting a source of racial bias into steps of the judicial process that come after arrest."

78. Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 127 (2014).

79. Mathews v. Eldridge, 424 U.S. 319, 335 (1976).

in false imprisonment.[80] By ceding such important tasks to algorithmic decision-making systems, "over time, deference to algorithms may weaken the decision-making capacity of government officials along with their sense of engagement and agency . . . undermin[ing] a person's sense of her own moral agency . . . [whereby] human dignity is eroded and individuals may consider themselves to be largely unaccountable for the consequences of their computer use." [81] Diminishing the agency of government officials and distancing them from accountability in turn erodes the confidence of the public in the governing body. This erosion of trust related to the provision of due process is incredibly harmful to democracy—as due process is a foundational aspect of the social contract ensuring the individual's freedom, without it the arbitrariness of the decision-making process begins to recall authoritarian rule.

In light of the significant liberty interest implicated, industry leaders and legal theorists have argued greater federal agency oversight of algorithmic technology is necessary in the United States. In particular, the majority have pushed for greater algorithmic transparency overseen and enforced by administrative government agencies. [82] However, the definition of algorithmic transparency and the degree to which corporations should be held accountable for harms caused by their algorithms is still a point of contention. "Government officials and tech executives have argued that too much transparency could imperil companies' intellectual property and dissuade [them] from working with governments."[83] Revealing the function and inputs of an algorithm could divulge proprietary information that, if leaked, would put technology companies at severe business risk. Furthermore, where an algorithm has caused an unintended harm to a consumer or bystander of such technology, it is unclear who, if anyone, should be held responsible for the

80. Lauren Kirchner, *Traces of Crime: How New York's DNA Techniques Became Tainted*, N.Y. TIMES (Sept. 4, 2017), http://www.nytimes.com/2017/09/04/nyregion/dna-analysis-evidence-new-york-disputed-techniques.html?_r=0.

81. Brauneis & Goodman, *supra* note 31, at 127.

82. JOSHUA NEW & DAVID CASTRO, CTR. FOR DATA INNOVATION, HOW POLICYMAKERS CAN FOSTER ALGORITHMIC ACCOUNTABILITY 8 (2018), http://www2.datainnovation.org/2018-algorithmic-accountability.pdf ("A Pew survey found that many technologists believe algorithmic transparency would be a good way to mitigate the risks of algorithms [and the FTC] has expressed support for algorithmic transparency—though it is unclear exactly how the FTC defines it.").

83. DJ Pangburn, *Washington Could be the First State to Rein in Automated Decision-Making*, FAST CO. (Feb. 8, 2019), http://www.fastcompany.com/90302465/washington-introduces-landmark-algorithmic-accountability-laws.

technological malfunction.[84] Many worry that holding technology companies, especially market newcomers, strictly liable for harms caused by their algorithmic innovations would place too high a financial burden on industry players and fail to take into account the "significant difference between mistakes that harm consumers due to maleficence, negligence, willful neglect, or ineptitude on the part of the company, and those that harm consumers as a result of a company striving to innovate and benefit society."[85] Furthermore, it is unclear to what extent intent should be factored in, "when an algorithm causes harm . . . to determine if an operator acted responsibly."[86] However, as capitalism and democracy often go hand in hand, the market economy repercussions of regulation cannot be taken lightly. Rather in a democratic system, any means of oversight must take into account not only the public's interest, but also that of the corporate actors it seeks to control.

In the European Union, attempts at regulating the cyber sphere have thus far resulted in the General Data Protection Regulation (hereinafter, GDPR), which provides citizens with a nearly direct right to due process where algorithmic decision-making is concerned. The GDPR requires data controllers to "implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision," if they are subjected to "a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[87] In addition, the GDPR focuses heavily on user's privacy and consent rights,[88] as well as data localization and

84. *See* Thomas Beardsworth & Nishant Kumar, *Who to Sue When a Robot Loses Your Fortune*, BLOOMBERG (May 5, 2019, 7:00 PM), http://www.bloomberg.com/news/articles/2019-05-06/who-to-sue-when-a-robot-loses-your-fortune; Kristin Houser, *Prosecutors: Uber Isn't Criminally Liable for Self-Driving Car Death*, FUTURISM (Mar. 7, 2019), http://futurism.com/uber-not-criminally-liable-self-driving-car-death (indicating that there is no established case law regarding liability where a machine is determined to be the primary cause of the harm incurred).

85. NEW & CASTRO, *supra* note 82.

86. *Id.*

87. Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, 46 [hereinafter GDPR]; *see also* GDPR, art. 16, 2016 O.J. (L 119) 1, 43.

88. *See* GDPR, art. 12-15, 2016 O.J. (L 119) 1, 39-43.

securitization. [89] However, measures focused primarily on ensuring informed consent risk falling prey to the consent fallacy whereby they place too great an emphasis on user knowledge in relation to practices that these users have no power to change. Rather, such measures may have the opposite of their desired effect, normalizing the existing manipulative practices by accepting them through notice and agreement instead of demanding change. Online consent thus carries little meaning when it, "is most often obtained by displaying a link to a privacy policy . . . and asking the user to accede to these terms and conditions by ticking a box [with] no chance to negotiate and little evidence that the majority of users either read, understand or truly consider these conditions, [making it] hard to see how this consent is either 'freely given, specific, informed and unambiguous' despite these being conditions for valid consent."[90] As a result, while such measures may make users aware of the type of personal data they are allowing companies to access, they fail to provide meaningful insight into how such data is used and do not seek to instill greater fairness in the technology's development from the start. Thus, while the GDPR takes a step in the right direction, it has been criticized for placing an outsize burden on many businesses.[91] Furthermore, it should be noted that the GDPR, while adopted by largely democratic societies, was imposed by the European Union's supranational governing body, which is much less concerned with electoral bias and election pandering. As a result, the passage of legislation at this level, while still representative in essence, is further from democracy than the direct system found in many of the nation states composing the Union.

Legislative efforts have also sought to address the external threats posed by the digital revolution through the expansion of national security. The invocation of national security has often provided a blunt tool by which executive powers may be expanded without concern for the checks and balances otherwise required in a democratic system. While national security exceptions are necessary in order to preserve the sovereign, the over-expansive interpretation of exigent circumstances threatens both the liberty interests of its subjects as well as the legitimacy of the democratic system. The Foreign Investment Risk Review and Modernization Act of

89. *See* GDPR, ch. 4 & 5, 2016 O.J. (L 119) 1, 47-65.

90. Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18, 66 (2017).

91. Frank Ready, *U.S. Companies Among Most GDPR Compliant, But Privacy Burden Grows*, LAW.COM (May 22, 2019 11:00 AM), http://www.law.com/legaltechnews/2019/05/22/us-companies-among-most-gdpr-compliant-but-privacy-burden-grows/?slreturn=20200417011558.

2018 (FIRRMA) and the Export Control Reform Act of 2018 (ECRA) are an example of such an expansion in the United States. Taken together, these acts provide the executive branch a great degree of oversight in trade and investment by establishing a broad category of industries and transactions that may be deemed critical to national security. Under FIRRMA, "national security" is read to "include those issues relating to 'homeland security,' including its application to critical infrastructure."[92] The amended Defense Production Act of 1950 (DPA) under FIRRMA gives the Committee on Foreign Investment in the United States (CFIUS) oversight broadly of "covered transactions," which extends not only to mergers, acquisitions and takeovers that result in foreign control of a U.S. business related to national security (as it did previously), but also the following transactions:

> (ii) . . . the purchase or lease by, or a concession to, a foreign person of private or public real estate that—(I) is located in the United States; (II)(aa) is, is located within, or will function as part of, an air or maritime port; or (bb)(AA) is in close proximity to a United States military installation or another facility or property of the United States Government that is sensitive for reasons relating to national security; (BB) could reasonably provide the foreign person the ability to collect intelligence on activities being conducted at such an installation, facility, or property; or (CC) could otherwise expose national security activities at such an installation, facility, or property to the risk of foreign surveillance; and (III) meets such other criteria as the Committee prescribes by regulation, except that such criteria may not expand the categories of real state to which this clause applies beyond the categories described in subclause (II). (iii) Any other investment . . . by a foreign person in any unaffiliated United States business that—(I) owns, operates, manufactures, supplies, or services critical infrastructure; (II) produces, designs, tests, manufactures, fabricates, or develops one or more *critical technologies*; or (III) maintains or collects sensitive personal data of United States citizens that may be exploited in a manner that threatens national security. (iv) any change in the rights that a foreign person has with respect to a United States business in which the foreign person has an investment, if that change could result in—(I) foreign control of the United States business; or (II) an investment described in clause (iii).[93]

The inclusion of "critical technologies" here is particularly noteworthy, as it expands the oversight of CFIUS to nearly all innovations

92. Foreign Investment Risk Review and Modernization Act of 2018, 50 U.S.C. § 4565(a)(1).

93. *See id.* § 4565(a)(4)(B) (emphasis added).

in the digital world by capturing "emerging and foundational technologies controlled pursuant to section [1758 of the Export Control Reform Act of 2018.]"[94] The referenced ECRA provision provides a statutory basis for the President to "establish and . . . as appropriate, lead, a regular, ongoing interagency process to identify emerging and foundational technologies that—(A) are essential to the national security of the United States; and (B) are not critical technologies described in [FIRRMA's definition of "critical technologies]."[95] As a result, the amendments to the DPA allow for a constantly fluctuating scope of technologies to be subject to review, and furthermore consolidate the discretion by which this scope may be determined in the hands of the executive (rather than requiring legislative agreement). Under the FIRRMA pilot program, the industry categories that were determined to constitute emerging and foundational technologies and would thus be subjected to greater scrutiny are as follows:

> aircraft manufacturing; aircraft engine and engine parts; alumina refining and primary aluminum production; ball and roller bearing manufacturing; computer storage device manufacturing; electronic computer manufacturing; guided missile and space vehicle manufacturing; guided missile and space vehicle propulsion unit and propulsion unit parts manufacturing; military armored vehicle, tank, and tank component manufacturing; nuclear electric power generation; optical instrument and lens manufacturing; other basic inorganic chemical manufacturing; other guided missile and space vehicle parts and auxiliary equipment manufacturing; petrochemical manufacturing; powder metallurgy part manufacturing; power, distribution, and specialty transformer manufacturing; primary battery manufacturing; radio and television broadcasting and wireless communications equipment manufacturing; research and development in nanotechnology; research and development in biotechnology; secondary smelting and alloying of aluminum; search, detection, navigation, guidance, aeronautical, and nautical system and instrument manufacturing; semiconductor and related device manufacturing; semiconductor machinery manufacturing; storage battery manufacturing; telephone apparatus manufacturing; turbine and turbine generator set units manufacturing.[96]

However, the ECRA imposed trade restrictions over an even broader swath of technologies considered emerging and foundational. It proposed

94. *See id.* § 4565 (a)(6)(A).
95. Export Control Reform Act of 2018, 50 U.S.C. § 4817(a)(1).
96. 31 C.F.R. pt. 801, Annex A.

to impose export controls to the following list of emerging technologies that are essential to the national security of the United States:

> (1) Biotechnology, such as: (i) Nanobiology; (ii) Synthetic biology; (iii) Genomic and genetic engineering; or (iv) Neurotech. (2) Artificial intelligence (AI) and machine learning technology, such as: (i) Neural networks and deep learning (e.g., brain modelling, time series prediction, classification); (ii) Evolution and genetic computation (e.g., genetic algorithms, genetic programming); (iii) Reinforcement learning; (iv) Computer vision (e.g., object recognition, image understanding); (v) Expert systems (e.g., decision support systems, teaching systems); (vi) Speech and audio processing (e.g., speech recognition and production); (vii) Natural language processing (e.g., machine translation); (viii) Planning (e.g., scheduling, game playing); (ix) Audio and video manipulation technologies (e.g., voice cloning, deepfakes); (x) AI cloud technologies; or (xi) AI chipsets. (3) Position, Navigation, and Timing (PNT) technology. (4) Microprocessor technology, such as: (i) Systems-on-Chip (SoC); or (ii) Stacked Memory on Chip. (5) Advanced computing technology, such as: (i) Memory-centric logic. (6) Data analytics technology, such as: (i) Visualization; (ii) Automated analysis algorithms; or (iii) Context-aware computing. (7) Quantum information and sensing technology, such as (i) Quantum computing; (ii) Quantum encryption; or (iii) Quantum sensing. (8) Logistics technology, such as: (i) Mobile electric power; (ii) Modeling and simulation; (iii) Total asset visibility; or (iv) Distribution-based Logistics Systems (DBLS). (9) Additive manufacturing (e.g., 3D printing); (10) Robotics such as: (i) Micro-drone and micro-robotic systems; (ii) Swarming technology; (iii) Self-assembling robots; (iv) Molecular robotics; (v) Robot compliers; or (vi) Smart Dust. (11) Brain-computer interfaces, such as (i) Neural-controlled interfaces; (ii) Mind-machine interfaces; (iii) Direct neural interfaces; or (iv) Brain-machine interfaces. (12) Hypersonics, such as: (i) Flight control algorithms; (ii) Propulsion technologies; (iii) Thermal protection systems; or (iv) Specialized materials (for structures, sensors, etc.). (13) Advanced Materials, such as: (i) Adaptive camouflage; (ii) Functional textiles (e.g., advanced fiber and fabric technology); or (iii) Biomaterials. (14) Advanced surveillance technologies, such as: Faceprint and voiceprint technologies.[97]

Even a cursory glance at this list of technologies demonstrates that the concerns of the United States when described as "essential to national security" are not solely related to traditional notions of security, as covered

97. Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201, 58,202 (Nov. 19, 2018) (to be codified at 15 C.F.R. pt. 744).

under Article XXI of the General Agreement on Tariffs and Trade (GATT).[98] Furthermore, the legislative proposal for FIRRMA specifically contains provisions regarding reporting of Chinese investments, [99] supporting the notion that national security measures are utilized by the United States to address political and economic threats in addition to military necessities. Security exceptions have generally been considered necessary, "in [a] time of war or other emergency in international relations. . . [or]. . .under the United Nations Charter for the maintenance of international peace and security."[100] However, the concerns of the United States with regards to "national security" have been significantly expanded to encompass potential as well as actual threats. Economic competitiveness, particularly in the technology sector, has clearly been incorporated into the terminology of "national security" in the United States. In the past year alone, these expansive provisions have been used to conduct reviews of social media apps such as TikTok and Musical.ly.[101] Such reviews demonstrate that data collection and aggregation in and of itself has become a national security threat, particularly where the government believes that such data may reach its enemies; "lawmakers raised concerns about TikTok's growing influence in the United States . . . the American government had evidence of the app sending data to China . . . [and had] been downloaded more than 750 million times [in the past twelve months]."[102] Some American lawmakers have gone so far as to seek to bar government employees of any kind from the ability to use such apps.[103] However, the United States is not alone in raising security concerns with regards to the use of foreign made social media applications,

98. General Agreement on Tariffs and Trade, Oct. 30, 1947, 61 Stat. A-11, 55 U.N.T.S. 154 [hereinafter GATT] (herein used as a baseline for what is internationally agreed upon as meriting a "national security" exception as it is the longest standing international agreement concerning such topic).

99. H.R. 5515, 115th Cong. (2018).

100. GATT, *supra* note 98, at art. XXI.

101. Greg Roumeliotis, Yingzhi Yang, Echo Wang & Alexandra Alper, *Exclusive: U.S. Opens National Security Investigation into TikTok—Sources*, REUTERS (Nov. 1, 2019, 10:21 AM), http://www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-u-s-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL.

102. Jack Nicas, Mike Isaac & Ana Swanson, *TikTok Said to be Under National Security Review*, N.Y. TIMES (Nov. 1, 2019), http://www.nytimes.com/2019/11/01/technology/tiktok-national-security-review.html.

103. No TikTok on Government Devices Act, S. 3455, 116th Cong. (2020) (noting that "no employee of the United States, officer of the United States, Member of Congress, congressional employee of officer or employee of a government corporation may download or use TikTok or any successor application developed by ByteDance or any entity owned by ByteDance on any device issued by the United States or a government corporation.").

nor are their concerns completely unfounded: "India's military . . . has prohibited personnel from installing Chinese social platform WeChat due to security concerns. The Australian armed forces have also banned WeChat. The Pentagon banned the military's use of geolocating fitness trackers in August 2018 after live GPS data was found on the public [I]nternet [making it possible for researchers] to track the location of troops on military bases and spies in safe houses."[104]

The additional scrutiny placed on foreign investments, however, raises issues of due process similar to those discussed with regards to algorithmic decision-making. By couching the review of such investments in terms of national security, the executive branch both broadens its reach and seeks to place its decisions beyond reproach from the legislative or judicial branch. The initial expansion of the DPA to give CFIUS greater review powers was constitutionally challenged in the United States in *Ralls Corp. v. Committee on Foreign Investments in the United States* on the grounds that it denied foreign persons due process under the Fifth Amendment of the United States Constitution.[105] Although the case was settled on appeal, in its latest amendments to the DPA, the legislature sought to address some of the due process concerns of the United States Court of Appeals for the District of Columbia Circuit in its ruling in *Ralls Corp.* by providing foreign persons the ability to pursue civil actions, although they are still unable to contest actual decisions made by the administrative body or have insight into the review process. Democracy thus battles itself when trying to compete in the cyber sphere as its governing mechanism is slow and burdensome, while the foe it faces is nimble and quick. In order to address the harms posed by online speech, it would have to re-evaluate its commitment to absolute freedom of speech. In order to remain competitive against its foreign enemies, it would have to cooperate to a greater degree with its national tech companies and move away from the laissez-faire capitalism of years past. In order to address the threats posed by cyber warfare, it would need to re-evaluate the role of the balance of powers and adequate due process in order to defend itself fully

104. Justin Sherman, *Unpacking TikTok, Mobile Apps and National Security Risks*, LAWFARE (Apr. 2, 2020, 10:06 AM), http://www.lawfareblog.com/unpacking-tiktok-mobile-apps-and-national-security-risks.

105. Ralls Corp. v. Comm. on Foreign Inv. in the U.S., 758 F. 3d 296, 320 (D.C. Cir. 2014) (wherein CFIUS review of a Chinese acquisition of land was reviewed and resulted in a Presidential Order requiring Ralls Corporation to divest itself of the purchase of a number of windfarms it had acquired two years prior.).

against the threats it faces both domestically and from abroad. As a result, rather than taking a primary role in governing online spaces, democratic governments have been forced to acquiesce to the norms imposed either by private actors or their more dominant and forceful authoritarian counterparts.

V. AUTHORITARIANISM, CYBER SOVEREIGNTY, AND REASSERTION OF STATE CONTROL

International law has generally recognized that, "sovereignty is perhaps the most fundamental [principle]. From [which] emerges, *inter alia*, notions of non-intervention; prescriptive, enforcement, and adjudicative jurisdiction; sovereign immunity; due diligence; and territorial integrity."[106] A sovereign state thus maintains the right "to conduct its affairs without outside interference. Between independent [s]tates, respect for territorial sovereignty is an essential foundation of international relations."[107] Extending this principal of independent sovereign control to the ephemeral territory of cyber space, Russia and China have actively advocated for cyber sovereignty—"the idea that states should be permitted to manage and contain their own [I]nternet without external interference."[108] Advocates of cyber sovereignty seek to control cyberspace within their perceived territoriality because they too understand "information as a weapon . . . [thereby making] censorship . . . a legitimate matter of national security . . . [and] [d]igital information warfare . . . a legible threat."[109] However, this is much easier said than done—"[w]hereas sovereignty is an inherently territorial concept, cyberspace connects states in ways that seem to dilute territoriality,"[110] making it difficult to draw boundaries on where one state's control should end and where another's begins.

The United States' stance on sovereignty in international law has been traditionally weak— holding that sovereignty, rather than being a

106. Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 47 YALE J. INT'L L. ONLINE 1, 4 (2017).

107. *Id.* at 5,7 (citing to the Nicaragua and Corfu Channel cases, respectively) (citations omitted).

108. Cate Cadell, *China's Xi Says Country Will Not Close Door to Global Internet*, REUTERS (Dec. 2, 2017, 8:57 PM) http://www.reuters.com/article/us-china-cyber/chinas-xi-says-country-will-not-close-door-to-global-internet-idUSKBN1DX01S.

109. Eduard Saakashvili, *The Global Rise of Internet Sovereignty*, CODA (Mar. 21, 2019) http://codastory.com/authoritarian-tech/global-rise-internet-sovereignty/.

110. Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace: Lex Lata Vel Non?*, 111 AJIL UNBOUND 213, 218 (2017).

primary rule of international law, is a foundational principal upheld through other codified rules of international law, such as non-intervention or the prohibition on use of force.[111] In a similar vein, it has refrained from applying sovereignty to cyberspace. Rather, as cyber territory has blurred borders, the United States has capitalized on its position as a technological superpower in order to export its political norms and maintain its position as a global hegemon. The United States' refusal to impose international limits on cyberspace has been motivated in large part by what some have dubbed the proliferation of "'data colonialism' by [W]estern companies and governments."[112] Furthermore, the United States and its global allies have taken a strong ideological stance against cyber sovereignty on the grounds that "[t]hese advances in authoritarian innovation should provoke concerns for democracies for reasons of security, human rights, and overall competitiveness." [113] However, this characterization of cyber sovereignty, or a lack thereof, makes it incredibly difficult to find a State guilty of violating another's sovereignty through cyber activity because it requires an internationally wrongful act to occur in violation of a more stringent primary rules.[114] Internationally wrongful acts are even more difficult to prove when respecting sovereignty is not deemed a primary rule in and of itself, as they consist of two elements: "[f]irst, there must be a breach of a State's legal obligation through either commission or omission. Second, the act in question must be attributable to the State

111. *Id.* at 214.

112. ARINDRAJIT BASU ET AL., THE LOCALISATION GAMBIT: UNPACKING POLICY MEASURES FOR SOVEREIGN CONTROL OF DATA IN INDIA, CTR. FOR INTERNET & SOC'Y, INDIA 4 (Mar. 19, 2019), http://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf.

113. SAMUEL BENDETT & ELSA KANIA, AUSTL. STRATEGIC POL'Y INST., POLICY BRIEF: A NEW SINO-RUSSIAN HIGH-TECH PARTNERSHIP 3 (Oct. 2019), http://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-10/A%20new%20Sino-Russian%20high-tech%20partnership_0.pdf?xAs9Tv5F.GwoKPiV9QpQ4H8uCOet6Lvh.

114. Eric T. Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 GEO. J. INT'L L. 735, 741 (2017). (Under the current international framework, as interpreted by [U.S.] proponents, "remote cyber activities that violate domestic law on espionage would not, in themselves, violate international law . . . election meddling by cyber-means would never amount to a violation of the target State's sovereignty, for only the breach of an obligation contained in a primary rule of international law [would qualify] as an internationally wrongful act."); *see also* Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AJIL UNBOUND 207, 211 (2017) (arguing that in order to defend the use of cyber operative tactics by the [United States] to fight terrorist activity abroad, "[w]hile the principle of sovereignty should factor into the conduct of any cyber operation, it does not itself establish a bar against individual or collective state cyber operations against all cyber infrastructure within infrastructure within another state.").

concerned pursuant to the law of State responsibility."[115] The cyber sphere complicates both the notion of obligation and attribution where the domain of the sovereign is unclear and the anonymization and complexity of cyber attacks allows attribution of actions to be obfuscated.

As the criticality of the cyber sphere to national infrastructure becomes more evident, however, the majority of U.N. Member States have moved away from the United States' point of view "generally agree[ing] that cyberspace is subject to the principles of sovereignty and jurisdiction as well as prohibitions on intervention in the affairs of other States and the use of force."[116] China was the first to champion cyber sovereignty in 2010, releasing a White Paper explaining the need to control the information exchanged within its borders as "an issue that concerns national economic prosperity and development, state security and social harmony, state sovereignty and dignity, and the basic interests of the people."[117] In large part, this was a response to U.S. dominance in cyberspace. As home to many of the largest tech corporations and the leader in developing new information technology, the United States has long been the most dominant power, utilizing "international law to maintain [its] superior position and to prevent other states from engaging in what it perceives to be disruptive activities. . . . The [United States] has consistently [sought] to resist the creation of new legal constraints—such as those proposed by the Chinese and the Russians—that [might] limit American cyber capabilities."[118] The United States has staunchly opposed the Sino-Russian view of cyber sovereignty, arguing that it is merely, "a way to justify practices deemed unacceptable in many democracies, such as tight control of [I]nternet gateways or the censorship of political content online."[119] The debate over cyber sovereignty thus ultimately evolved to represent "not merely an academic exercise in legal interpretation but

115. Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30, 33 (2018).

116. Cyrus Jabbari, *The Application of International Law in Cyberspace: State of Play*, UNITED NATIONS (Oct. 25, 2018), http://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/.

117. *Full Text: The Internet in China*, PEOPLE'S DAILY ONLINE (June 8, 2010, 1:05 PM), http://en.people.cn/90001/90776/90785/7017177.html.

118. Anders Henriksen, *The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace*, 5 J. CYBERSECURITY 1, 4 (2019), http://academic.oup.com/cybersecurity/article/5/1/tyy009/5298865.

119. Justin Sherman, *How Much Cyber Sovereignty is Too Much Cyber Sovereignty*, COUNCIL ON FOREIGN RELS.: NET POLITICS BLOG (Oct. 30, 2019), http://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty.

also—if not primarily—about trying to reconcile colliding strategic interests and clashing ideological worldviews."[120]

Russia and China have reinforced this dichotomy, maintaining that the debate around cyber sovereignty is the result of "balancing the benefits of globalization and the digital revolution between the developed and developing countries."[121] Their fear is that without the acceptance of cyber sovereignty as an international legal norm, nations with "the most advanced and original technology," such as the United States, are likely to, "intervene and control the cyber-territory of any other nation . . . [because they have] establish[ed] a more advanced electronic/cyber/virtual national sovereignty than . . . other, less-advanced nations."[122] As a result, "[t]he sovereignty debate has been most active in the realm of national security, where U.N. member states have for years debated norms governing cyberespionage and cyberwarfare."[123] Recognition of cyber sovereignty, as proposed by Russia and China, would thus require states to "refrain from using information and communication networks 'to interfere in the internal affairs of other States' . . . [to] ensure that other states cannot exploit a dominant position . . . [and] to undermine States' right to independent control of information and communications technology goods and services, or to threaten their political, economic and social security," and recognize that it may be deemed necessary by any state under its own mandate of sovereignty "to make certain restrictions . . . for the protection of national security or of public order . . . or of public health or morals."[124]

The Sino-Russian approach to cyber sovereignty provides a flexible solution to states seeking to assert control; "they argue that countries should be exercising [cyber sovereignty] but do not present a specific plan for how to do so . . . allow[ing] countries to pick a repressive toolbox that suits them best—ranging from draconian censorship laws to network

120. Henriksen, *supra* note 118.

121. Hao Yeli, *A Three-Perspective Theory of Cyber Sovereignty*, PRISM, http://cco.ndu.edu/PRISM-7-2/Article/1401954/a-three-perspective-theory-of-cyber-sovereignty/ (last visited Oct. 6, 2020).

122. Dr. Georgios Zekos, *Cyber-Territory and Jurisdiction of Nations*, 15 No. 12 J. INTERNET L. 3 (2012).

123. Ellen Nakashima, *The U.S. Is Urging a No Vote on a Russian-Led UN Resolution Calling for a Global Cybercrime Treaty*, WASH. POST (Nov. 19, 2019,11:03 AM), http://www.washingtonpost.com/national-security/the-us-is-urging-a-no-vote-on-a-russian-led-un-resolution-calling-for-a-global-cybercrime-treaty/2019/11/16/b4895e76-075e-11ea-818c-fcc65139e8c2_story.html.

124. Henriksen, *supra* note 118, at 5 (internal citations omitted).

shutdowns."[125] "In places like Russia, China and in many states in the Middle East, [where] an open cyberspace is (rightly) considered a threat to existing governing structures," such a broad based approach to cyber sovereignty is often characterized as an opportunity for abuse aimed at the political opposition, however, the sole motivation of the movement should not be equated with these repressive tendencies.[126] Although cyber sovereignty does in fact pose concerns of human rights violations with regards to freedom of expression, it also provides nations with the ability to combat the chaos arising within their borders as a result of social media and new information technologies. India provides one of the most notorious examples, where rumors spread through services such as WhatsApp and Facebook led to public lynchings and acts of extreme violence.[127] It is then unsurprising that the Indian government has been supportive of the push for cyber sovereignty and has drafted its own legislation aimed at restricting and tracking potentially disruptive information by "mak[ing] it mandatory for online platforms to 'proactively' deploy technology, which would enable a ferreting of content seen as 'unlawful,'" in hopes of preventing such occurrences in the future.[128]

China has led by example in its implementation of cyber sovereignty—putting in place a number of laws restricting freedom of speech and even notoriously blocking tech giants such as Facebook from accessing users in its territory.[129] Where social media companies have sought to successfully enter the Chinese market, they have been forced to comply with the state's standards of conduct. LinkedIn, for example, was only able to gain tacit approval from the government by demonstrating willingness to "play by Chinese rules on expression . . . [and] relinquish[ing] 7 percent of its local operation to two well-connected

125. *The Sinicization of Russia's Cyber Sovereignty Model*, COUNCIL ON FOREIGN RELS.: NET POLITICS BLOG (Apr. 1, 2020), http://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model.

126. Henriksen, *supra* note 118.

127. *Death by Fake News: Indian Authorities Blame 'Irresponsible and Explosive Messages' on WhatsApp for Lynchings*, S. CHINA MORNING POST (July 14, 2018, 3:51 PM), http://www.scmp.com/news/asia/south-asia/article/2155270/death-fake-news-indian-authorities-blame-irresponsible-and.

128. Seema Chishti, *Govt Moves to Access and Trace All 'Unlawful' Content Online*, INDIAN EXPRESS (Dec. 24, 2018, 10:26 AM), http://indianexpress.com/article/india/it-act-amendments-data-privacy-freedom-of-speech-fb-twitter-5506572/.

129. Paul Mozur & Carolyn Zhang, *Silicon Valley Giants Confront New Walls in China*, N.Y. TIMES (July 22, 2017), http://www.nytimes.com/2017/07/22/technology/in-china-silicon-valley-giants-confront-new-walls.html.

Chinese venture capital firms."[130] In 2015, China's National Security Law was adopted, "set[ting] an expansive definition of national security that outlaw[ed] threats to China's government, sovereignty and national unity as well as its economy, society and cyber and space interests."[131] Soon after, it adopted a controversial counterterrorism law restricting "the right of media to report on details of terror attacks, including a provision that media and social media cannot report on details of terror activities that might lead to imitation nor show scenes that are 'cruel and inhuman.'"[132] The law went so far as to impose additional proactive obligations "on telecommunications and Internet service operators . . . [requiring that] they . . . proactively monitor their networks for terrorism information and disclose such information to the authorities."[133] More recently, the Cyber Security Law adopted in 2017 expanded the institutions and legal tools at the government's disposal "to monitor and control information disseminated online."[134] In essence, the Chinese government has sought to ensure its domestic sovereignty against foreign actors by restricting access and censoring information wherever it is deemed to pose a threat—"no website or social media account is allowed to provide news service on the [I]nternet without the Cyberspace Administration of China's permission[, and] [I]nternet users are blocked from foreign search engines, news websites, and social media platforms by the Great Firewall."[135]

Russia in turn has expanded formal Internet censorship in the past few years, requiring "Russian [I]nternet service providers (ISPs) . . . to store six months of metadata and [imposing] laws forcing international

130. Paul Mozur & Vindu Goel, *To Reach China, LinkedIn Plays by Local Rules*, N.Y. TIMES (Oct. 5, 2014), http://www.nytimes.com/2014/10/06/technology/to-reach-china-linkedin-plays-by-local-rules.html.

131. Chun Han Wong, *China Adopts Sweeping National Security Law*, WALL ST. J. (July 1, 2015, 9:37 AM), http://www.wsj.com/articles/china-adopts-sweeping-national-security-law-1435757589.

132. Ben Blanchard, *China Passes Controversial Counter-Terrorism Law*, REUTERS (Dec. 27, 2015, 10:49 PM), http://www.reuters.com/article/us-china-security-idUSKBN0UA0722 0151228.

133. *China Enacts Broad Counter-Terrorism Law*, COVINGTON & BURLING LLP 2 (Jan. 5, 2016), http://www.cov.com/-/media/files/corporate/publications/2016/01/china_enacts_broad_ counter_terrorism_law.pdf.

134. Paul Triolo, Samm Saks, Graham Webster & Rogier Creemers, *China's Cybersecurity Law One Year On*, NEW AMERICA (Nov. 30, 2017), http://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-law-one-year/.

135. *10 Most Censored Countries*, COMM. TO PROTECT JOURNALISTS, http://cpj.org/ reports/2019/09/10-most-censored-eritrea-north-korea-turkmenistan-journalist.php (last visited Oct. 5, 2020).

companies to store Russian users data on Russian servers, so the government can have access to it if needed."[136] Some have gone so far as to say that, "Russia has actively mimicked China in its implementation of cyber sovereignty."[137] Similar to China, Russia has provided for an oversight body, Roskomnadzor,[138] to actively monitor and block media content that it finds disruptive as well as that regarded as demonstrating"'blatant disrespect' for the state, the authorities, the public, the Russian flag or the constitution."[139] In 2019, Russia further formalized its desire for censorship by putting in place a "fake news" and "[I]nternet insults" law that would "allow[] it to target individuals and websites for such nondescript crimes as spreading 'fake news' and 'disrespecting' state symbols or figures."[140] Later that year, the Kremlin put in place a Sovereign Internet law as well, "tightening state control over the global network . . . [and] aim[ing] to route Russian web traffic and data through points controlled by state authorities and to build a national Domain Name System to allow the Internet to continue working even if Russia [were to be] cut off from foreign infrastructure."[141] Most recently, the overbearing nature of Russia's expanding cyber controls has been felt in Moscow as a result of the Coronavirus pandemic. In response to threats of an exponential epidemic, the Kremlin imposed a digital tracking system that requires all residents of Moscow, fourteen years and older, to "register on a government website, download an app on their smartphones . . . declare a route and a purpose [if they want to go anywhere] and then [wait for] a QR code, which authorities can track . . . the app has access to the user's

136. Caleb Chen, *Thousands March in Moscow, Russia to Support Internet Freedom, Protest VPN Ban*, PRIV. INTERNET ACCESS (July 24, 2017), http://www.privateinternetaccess.com/blog/thousands-march-moscow-russia-support-internet-freedom-protest-vpn-ban/.

137. *The Sinicization of Russia's Cyber Sovereignty Model*, *supra* note 125.

138. Statute of Roskomnadzor, GOV'T OF THE RUSS. FED'N, (Mar. 16, 2009), http://eng.rkn.gov.ru/about/statute_of_roskomnadzor/.

139. Gabrielle Tetrault-Farber, *Russia Blocks Shutterstock Domain for 'Insulting State Symbols'*, REUTERS (Dec. 2, 2019, 1:42 PM), http://www.reuters.com/article/us-russia-shutterstock/russia-blocks-shutterstock-domain-for-insulting-state-symbols-idUSKBN1Y627M.

140. Caleb Chen, *Russia Doubles Down on Censorship with New 'Fake News' and 'Internet Insults' Law*, PRIV. NEWS ONLINE (Mar. 19, 2019), http://www.privateinternetaccess.com/blog/russia-doubles-down-on-censorship-with-new-fake-news-and-internet-insults-law/.

141. *Russia Enacts 'Sovereign Internet' Law; Free Speech Activists Cry Foul*, WASH. POST (Nov. 1, 2019, 6:03 PM), http://www.washingtonpost.com/world/russia-enacts-sovereign-internet-law-free-speech-activists-cry-foul/2019/11/01/a0654e3a-fcd4-11e9-8190-6be4deb56e01_story.html.

mobile information . . . includ[ing] calls, location, storage, camera, and network details."[142]

Developing nations, particularly those with authoritarian regimes, have largely followed in Russia and China's footsteps, imposing their own cyber governance measures in an attempt to regain control from foreign private actors in this domain. Even smaller countries such as Kazakhstan have passed legislation as a part of their National Security laws that allow "the government to shut down [I]nternet access and mobile connection during mass riots or anti-terrorist operations held in the country."[143] Additionally, this legislation "force[s] Internet service providers and mobile operators to block their services when an official order is issued."[144] India, which leads the world in the number of Internet shutdowns, has done so in large part because disinformation and fake news has led to public hysteria resulting in violence or riots in the country.[145] As a result, the government has "temporarily shut down mobile networks or blocked social media apps during riots and protests, claiming that the measures were necessary to halt the flow of disinformation and incitement to violence."[146] Sri Lanka similarly followed India's lead in March 2018 when "online rumors that Muslims were trying to sterilize Sinhalese Buddhists, led a group of Buddhist men to beat a Muslim man and set fire to his shop. [E]xtremists used Facebook to implore followers to 'rape without leaving an iota behind' and 'kill all Muslims' . . . ."[147] The Sri Lankan "[a]uthorities reacted by blocking four social media platforms that they said were amplifying hate speech."[148] In Vietnam, the government's new cybercrime legislation requires big tech "to store at least 36 months of local users' data in the country [and] bans the use of social networks to

142. JC Robles, *Moscow's Digital Tracking 'Cyber Gulag' Helps Enforcing Lockdown by Tracking People*, TECH TIMES (Apr. 14, 2020, 11:17 AM), http://www.techtimes.com/articles/248814/20200414/moscows-digital-tracking-cyber-gulag-helps-enforcing-lockdown-by-tracking-people.htm.

143. Dina Baidildayeva, *Internet Censorship in Kazakhstan: More Pervasive Than You May Think*, OPEN DEMOCRACY (Mar. 26, 2018) http://www.opendemocracy.net/en/odr/internet-censorship-in-kazakhstan/.

144. *Id.*

145. Tariq Ahmad, *Government Responses to Disinformation on Social Media Platforms: India*, LIBRARY OF CONG. (Sept. 2019), http://www.loc.gov/law/help/social-media-disinformation/india.php.

146. Adrian Shahbaz, *Fake News Data Collection and the Challenge to Democracy*, FREEDOM HOUSE, http://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism (last visited Oct. 4, 2020).

147. *Id.*

148. *Id.*

organize anti-state activities, spread false information or create difficulties for authorities."[149] In Egypt, the government has sought to repress fake news by not only passing legislation that allows the shutdown of websites "deemed to constitute a threat to national security or the economy,"[150] but will also consider, "social media accounts and blogs with over 5,000 followers . . . [as] media companies [that are] subject to stricter censorship requirements," and punish individuals found in violation of the law with jail time and monetary fines.[151] Where the government does not itself possess the ability to impose censorship, it may enlist the help of tech giants by enacting domestic laws that require them to remove certain content as a matter of compliance. For example, Facebook released a transparency report that denotes the number of items it censors in a given country where required by law, notably restricting access to "items in the UAE, all reported by the Telecommunications Regulatory Authority, a federal UAE government entity responsible for information technology."[152] The restricted content was "reported for hate speech and was attacking members of the royal family, which is against local laws."[153] However, many countries feel either that these companies do not go far enough in censoring and policing for false information, or take issue with the outsourcing of regulation of speech to a foreign private actor. Thus, increasingly, countries such as Singapore are considering "legislation to ensure technology companies rein in online fake news and [hold] those responsible" criminally liable.[154]

The need for cyber sovereignty as a means of national security and independence has even gained popularity in the West; "[r]emarkably, technological sovereignty is also of great appeal to countries that fashion themselves as cosmopolitan and internationalist alternatives to Trump's

---

149. John Boudreau & Xuan Quynh Nguyen, *Vietnam Says Google and Facebook May Have Year to Meet Cyber Law*, BLOOMBERG (Nov. 2, 2018, 10:56 PM), http://www.bloomberg.com/news/articles/2018-11-03/vietnam-says-google-and-facebook-may-have-year-to-meet-cyber-law.

150. *Egypt Internet: Sisi Ratifies Law Tightening Control Over Websites,* BBC NEWS (Aug. 18, 2018), http://www.bbc.com/news/world-middle-east-45237171.

151. Mack DeGeurin, *Egypt's 'Fake News' Laws are Being Used to Silence Online Dissent*, N.Y. MAG. (Oct.9, 2018), http://nymag.com/developing/2018/10/egypt-fake-news-laws-amal-fathy-mona-el-mazbouh-facebook.html.

152. Sam Biddle, *Sheryl Sandberg Misled Congress About Facebook's Conscience*, INTERCEPT (Sept. 9, 2018, 4:25 PM), http://theintercept.com/2018/09/05/facebook-senate-hearing-sheryl-sandberg/.

153. *Id.*

154. John Geddie & Aradhana Aravindan, *Singapore Panel Recommends Regulation of Tech Firms Over Fake News*, REUTERS (Sept. 20, 2018, 3:04 AM), http://www.reuters.com/article/us-singapore-politics-fakenews/singapore-panel-recommends-regulation-of-tech-firms-over-fake-news-idUSKCN1M011F.

nationalist project [such as] France and Germany."[155] Faced with growing internal and external threats online, "Western democracies are, like their authoritarian peers, seeking more control . . . merely converging with China and Russia on common fears. This leads to a shared affinity for something like . . . [a] 'paternalistic [I]nternet' . . . [a]nd of course, paternalism appeals to everybody."[156] The sudden rise of populist parties and hate speech in Europe led, "the French defence minister [to announce that] she want[ed] to 'lower [France's] exposure to [U.S.] components' . . . [and] an MP from President Macron's centrist party [asked] the government if it would establish a commission on digital sovereignty."[157] In Germany, content regulations went into effect with the NetzDG Regulation, passed in 2017, requiring ISPs to implement notice-and-action complaint procedures such that "obviously illegal" content would be deleted within twenty-four hours of notification.[158] Europe, as a whole, is now considering the passage of an EU-wide Digital Services Act that would force ISP providers to take on a more active role as intermediaries and assume some degree of liability and editorial responsibility to help minimize the spread of fake news.[159] In India, where the Constitution guarantees its citizens freedom of speech,[160] the government has struggled to strike a balance of preserving such rights and enacting regulations that can preserve both the integrity of their elections and public order, though it has been vocal that some form of regulation is necessary.[161] At its core, "sovereignty conveys rights on two distinct planes or spheres . . . first in [the State's] capacity as the entity entitled to exercise control over its territory and second in its capacity to act on the international plane,

155. Evgney Morozov, *Reasserting Cyber Sovereignty: How States are Taking Back Control*, THE GUARDIAN (Oct. 7, 2018, 3:59 PM), http://www.theguardian.com/technology/2018/oct/07/states-take-back-cyber-control-technological-sovereignty.

156. Saakashvili, *supra* note 109.

157. Morozov, *supra* note 155.

158. Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG), GERMAN L. ARCHIVE, http://germanlawarchive.iuscomp.org/?p=1245; *Germany Starts Enforcing Hate Speech Law*, BBC NEWS (Jan. 1, 2018) http://www.bbc.com/news/technology-42510868.

159. Mehreen Khan & Madhumita Murgia, *EU Draws Up Sweeping Rules to Curb Illegal Online Content*, FIN. TIMES (July 23, 2019) http://www.ft.com/content/e9aa1ed4-ad35-11e9-8030-530adfa879c2; Denisa Avram, *Towards an Enhanced Responsibility of Online Platforms: The EU Digital Services Act*, INLINE (July 31, 2019) http://www.inlinepolicy.com/blog/towards-an-enhanced-responsibility-of-online-platforms-the-eu-digital-services-act.

160. *See* India Const. art. 19.

161. Vindu Goel & Sheera Frenkel, *In India Election, False Posts and Hate Speech Flummox Facebook*, N.Y. TIMES (Apr. 1, 2019), http://www.nytimes.com/2019/04/01/technology/india-elections-facebook.html.

representing that territory and its people."[162] Although the Russian-Chinese push for cyber sovereignty likely originated in the states' desire to convey its rights with regards to the former capacity, as the threat to the latter has become clear through misinformation campaigns and cyber espionage, their coalition to advance such goals on an international stage has grown tremendously. As cyber speech and activities continue to echo even more loudly in real world actions, we are likely to see this call for state regulation to grow. While private actors, such as social media companies, have begun to regulate speech and monitor for misinformation to address the current gap, such entities are neither proper nor prepared to take on such a momentous task. Those that previously advocated against cyber sovereignty did so on the basis of promoting "globali[z]ation and open trade. Today, however, there are no governments that can convincingly preach further liberali[z]ation of trade in data, software or hardware. All governments, thus, are forced to choose between two options: reasserting technological sovereignty—or doing nothing."[163] As it has become abundantly clear that, for the sake of public order, action will be taken by those states that feel their national security is threatened, states that choose to do nothing risk abdicating their cyber sovereignty. Those that fail to govern themselves, will thus likely fall prey to foreign powers or private actors that step in to dictate the rules of the cyber space in their absence.

VI. CONCLUSION

In an increasingly technologically driven world, the war of global political influence has moved from the real world to online. Rather than having to invade a foreign nation in order to drastically alter its social or political landscape, such goals are now capable of being accomplished subtly through disinformation campaigns, cyber interference, and strategic investments. Over the course of the last decade, the proliferation of cyber legislation around the world has sought to enhance technological sovereignty and control, both by way of regulation and infrastructural capacity, in order to insulate States from the potential harms caused by both the internal and external threats described above. Although the United States still houses some of the world's most influential tech giants, its brand of democracy has been threatened by the innovations that they have

162. Eric Talbot Jensen, *Cyber Sovereignty: The Way Ahead*, 50 TEX. INT'L L.J. 275, 283 (2015).

163. Morozov, *supra* note 155.

introduced to the world. Just as Freedom House documented a decline in global freedom online, Pew Research Polls found that across the majority of the twenty-seven countries they surveyed, dissatisfaction with democracy and democratic institutions was on the rise.[164] Furthermore, the unavoidable realization that online speech unrestrained can easily result in real world harms has only furthered the cause of authoritarian regimes like China and Russia in leading "a cohort of countries [to move] toward digital authoritarianism by embracing . . . extensive censorship and automated surveillance systems."[165] While human rights groups have raised concerns that "efforts to control speech and information are accelerating, by both governments and private actors in the form of censorship, restrictions on access, and violent acts directed against those whose views or queries are seen as somehow dangerous or wrong,"[166] few, if any, better alternatives have been proposed by democratic governments. The decline of freedom online has been acknowledged as a threat, yet the solutions proposed by democratic governments have thus far been relatively vague and ineffectual, such as that proposed by Sweden—"[t]he solutions can only be found in discussions between all stakeholders—states, civil society and companies, as well as everyone who is dependent on the [I]nternet in their everyday lives and their work."[167] While such proposals may sound ideal, they are just that—idealistic, rather than pragmatic or capable of implementation. The emphasis in democracy on extensive deliberation and public input requires time and consideration, a luxury that the quick and dirty nature of the cyber sphere does not afford. Rather threats on the Internet require decisive action, speed, and flexibility in decision making—all attributes not characteristic of democratic society.

Without the expansive governmental powers of their authoritarian counterparts, democratic nations like the United States will not be able to maintain their position of global dominance much longer. Their attempts to compete thus far have threatened to erode the very foundations of their governing institutions—freedom of speech, a capitalist economy, and

164. Richard Wike, Laura Silver & Alexandra Castillo, *Many Across the Globe Are Dissatisfied with How Democracy Is Working*, PEW RSCH. CTR. (Apr. 29, 2019), http://www.pewresearch.org/global/2019/04/29/many-across-the-globe-are-dissatisfied-with-how-democracy-is-working/.

165. Shahbaz, *supra* note 146.

166. *Free Speech*, *supra* note 3.

167. Ministry for Foreign Affairs, *Internet Freedom in Decline—A Threat to Our Democracy*, GOV. OFFS. OF SWED. (June 11, 2019), http://www.government.se/opinion-pieces/2019/06/internet-freedom-in-decline--a-threat-to-our-democracy/.

balance of powers. As democracy seeks to evolve in time with the digital revolution, it is beginning to turn on itself—"the irony is that more democracy—ushered in by social media and the Internet, where information flows more freely than ever before—is what has unmoored [democratic] politics, and is leading us towards authoritarianism."[168] While some have described the erosion of trust in democratic institutions as a function of the rise of populism against elite institutions,[169] others have deemed it a function of online manipulation and misconduct.[170] Either way, the trend against democratic governance in the digital age is clear. Whether in response to domestic shortcomings or an inability to defend against foreign foes, democratic governments must either undergo serious change or bow out of the race for global hegemony, because without a strong cyber governance structure they will soon become obsolete in the digital age.

168. Rick Shenkman, *The Shocking Paper Predicting the End of Democracy*, POLITICO (Sept. 8, 2019), http://www.politico.com/magazine/story/2019/09/08/shawn-rosenberg-democracy-228045.

169. *Id.*

170. *The Rise of Digital Authoritarianism: Fake News, Data Collection and the Challenge to Democracy*, FREEDOM HOUSE (Oct. 31, 2018), http://freedomhouse.org/article/rise-digital-authoritarianism-fake-news-data-collection-and-challenge-democracy.