Social media is said to be the quintessential disruptive technology of the 21st century. Social media can play a crucial role in uniting societal forces in opposition to dictatorial rule. It can also help buttress civil society as a foundation of stable democracy, supporting or even replacing traditional forms of civic engagement. But social media can also fragment and degrade reasoned discourse about politics, undermine the legitimacy of democracy, and promote left and right-wing radicalism. The 2016 Presidential election underscored the danger of the weaponization of information by foreign actors. This weaponization of information was used again by American groups and organizations in the 2020 Presidential election. What is the proper course for government as to whether and how social media platforms should be regulated? What values and considerations should determine U.S. policy toward this disruptive technology? How might disruptive technology exacerbate or alleviate domestic political polarization and what will the impact be on foreign policy? Will social media strengthen populist movements in the United States, deepening political discord? How can the United States respond to safeguard its institutions and maintain public trust in the integrity of the political system? Looking abroad, how can the United States protect the interests and values of its allies, from the Baltic states to South Korea, from the disinformation and malign narrative strategies of China and Russia?

Introduction

Epidemics and Rumors

On December 12, 1964, Nature published an article titled, “Epidemics and Rumors.” The article details how rumors spread and posits an epidemiological approach to understanding the actual process – even articulating how a person’s reluctance to tell stale news can be incorporated into a mathematical model to better estimate spread rate. Of course, the modern Internet and social media did not exist in 1964 but rumors and people-to-people networks did. With the Internet, rumors are spread through various mediums as mis- and disinformation, distinguished by the disseminator’s intent and whether their spreading of false and/or misleading information is inadvertent (mis-) or deliberate (dis-). Yet, despite the countless innovations that have changed how the average person accesses and consumes information, the 1964 analogy still holds: the way information is spread across people is like the way a contagion may proliferate.

To investigate the phenomenon of social media, this table paper discusses how the medium and related technologies can produce very different outcomes, enabling civil discourse while simultaneously exacerbating social divisions and tensions. This paper also discusses how adversaries can attack the US homeland and population directly through the information environment by inserting false, misleading, and potentially dangerous information into social narratives, manifesting as distrust, conspiratorial thinking, trolling and even physical violence. Finally, this paper proposes that understanding the complex networks that exist online through the lens of complex contagions offers policy prescriptions for inoculating a population against the threat of mis- and disinformation and its implications for democracy and democratic institutions.
The Modern Rumor Mill

As the quintessential disruptive technology of the 21st Century, social media has changed how we communicate and interpret the world around us. From basic hand gestures to dancing on TikTok, humans have come a long way in communicating with each other. Social narratives – often enabled by technologies like radio, television, print media, and the Internet – help us form a collective understanding of the world, but social media has altered the way we interact with information, technology, our families, neighbors, colleagues, and strangers around the globe. Long distance communications are now inexpensive and easy, a home office is the new corner office, and social media influencers are the new celebrities. Built around networks and connections, social media has turned local issues into national or international news as physically separate communities of people suddenly feel close and intimate.

Social media is lauded as a tool for freedom of speech, democracy, and information sharing. The internet and social media have also changed how we think about access to information which, in some countries, is considered a basic information right, and can include “rights to create and communicate information (e.g., freedom of expression, freedom of association), to control others’ access to information (e.g., privacy and intellectual property), and rights to access information (e.g., freedom of thought, the right to read).” But access to information is only half the story—information quality also matters, and access to quality information is important (just like access to food is less meaningful for one’s health if it not sufficiently nutritious). Information quality has many dimensions, two of which are constantly at risk in the age of tweets, retweets, shares, and likes: accuracy and completeness. Just as the amount of information an average person has access to has grown, social media has simultaneously become increasingly polluted by inaccurate and incomplete soundbites of information.

But regardless of whether poor quality information is classified as mis- or disinformation, it is pervasive and the overall accuracy and completeness of the information we encounter on a regular basis is generally low. To further complicate the information environment, individuals knowingly and unknowingly spread falsehoods and dangerous rumors faster than the truth, which potentially distorts or influences the worldview of anyone who consumes it. False information can manipulate peoples’ opinions and more importantly, their behaviors. Examples include foreign agents organizing crowds (for both political parties or both sides of an issue) for US political and social justice protests sowing information that promotes clashes over the efficacy of vaccines, and numerous other strategies, to increase public distrust in the government. Given its virtually unlimited potential to enable information dissemination, social media and its various online platforms are frequently used (and abused) to spread poor quality information, falsehoods, and other harmful content, underscoring the need for aggressive approaches to combatting the spread of mis- and disinformation.

Political Learning and the “News Finds Me” Phenomenon

As society moves away from traditional forms of print media and towards online media sources, researchers are paying attention to how people ingest and process information and whether news and information encountered via online platforms have the same knowledge impact as reading a book or the printed news. Unfortunately, offline media platforms are better at facilitating
political learning than online media outlets because they encourage a linear consumption from the beginning to the end, while news on computers and mobile devices is consumed in a nonlinear manner. Linear consumption enables deep learning because information is consumed in an ordered, rational progression whereas nonlinear consumption is erratic and disconnected. The presence of hyperlinks in online news pieces, for example, promotes nonlinear consumption, leading the reader to jump from headline to headline before reading the full story and without understanding the full context.

Second, offline formats contain more editorial cues than does news on computers and mobile devices. Editorial cues are important because they assist the reader in learning by focusing them on the content being presented, the facts, and explanations that aid in understanding. Third, with offline formats, people are exposed to complete stories, whereas on computers and mobile devices, people are exposed to headlines and shorter information pieces that are sometimes opinion pieces instead of well-researched and accountable journalism. Fourth, there are usually more distractions when consuming news on computers and mobile devices, coming from both what other information is available on the platforms and the context in which people use the different media platforms – consider how different it feels to read an article in a physical newspaper versus an article on a phone and how the location where each activity may take place could differ. Fifth, research shows that people consume news in shorter and more fragmented periods on computers and mobile devices. Such news snacking and grazing is not likely to promote learning. It might promote a sense of being informed but feeling informed and being informed are not the same.

Additionally, research suggests that relying on social media and networks for news and information – particularly political information – is associated with a phenomenon of “news will find me” (NFM). Instead of actively seeking out information, research shows that people are increasingly relying on social networks for their news, which promotes detachment from the regular habits of traditional news consumption and linear learning. The NFM perception is also negatively associated with political knowledge and political interest – two important facets of a healthy democracy. Perhaps more concerning is how the NFM perception may have a negative, indirect effect on voting: declining political knowledge coupled with a public that is losing interest in politics may also lead to less political participation. Ultimately, an overreliance on personal networks and social media for political news and information is creating a less informed public that is more susceptible to mis- and disinformation – a vulnerability our adversaries are quick to exploit.

**Foreign Operations in the Information Environment**

Our modern media and information consumption habits are creating social vulnerabilities that foreign adversaries find advantageous. Using various social media platforms and services (e.g., Facebook, Twitter, YouTube, Instagram) foreign operations in the information environment (OIE) are infiltrating communities across the US and will continue to do so. Tactically, OIE encompasses “actions taken to generate, preserve, and apply information power against a relevant actor in order to increase or protect competitive advantage or combat power potential within all domains of the operating environment.” Importantly, by pushing influence narratives – including misleading or unsubstantiated allegations against political figures, media
organizations, US officials, public health authorities, and private citizens – Russia and China have direct access to the American public. And, with their astute assessment of America’s cultural pressure points and the witting and unwitting participation of “useful idiots” (e.g., unwitting, high-profile persons) to amplify disinformation, Russian and Chinese OIE target inflammatory issues spanning the political, economic, and social spectrum.\(^{13}\) Additionally, OIE should not be construed as distinctly partisan or as a partisan problem.\(^{14}\) Instead, Russia, China, and other adversarial nations stoke fires on both sides of the aisle, adding inflammatory content to already passionate narratives to deepen social divisions, widen the ideological gap between opposing groups, and increase distrust across the population.

Recently, in March 2021, the Office of the Director of National Intelligence released a declassified assessment entitled Foreign Threats to the 2020 Federal US Elections which identified Russia as interfering in the election cycle.\(^{15}\) Russia’s purpose, according to the assessment, was to undermine America’s democratic institutions to weaken US power and legitimacy – at home and abroad. This goal is not new: Russia’s modern disinformation history began in the early 1920s with Feliks Dzherzinski, founder and head of the infamously brutal Cheka secret police, as political warfare intended to crush anti-revolutionary activities in Bolshevik Russia and abroad.\(^{16}\) Today, various arms of the Russian intelligence apparatus contribute to these efforts, including the employment of proxy actors, making their malign activities difficult to track and stop. Even though election interference only comprises a small portion of Russian activities in the information environment (Russia has other lines of effort, like the hacking of the Democratic National Committee in 2016, the NotPetya ransomware campaign, and the more recent SolarWinds hack), the assessment reiterates how Russian OIE targets social cleavages in a strategic and calculated manner to affect public perception.\(^{17}\)

In everyday life, information manipulation and foreign OIE often have a deleterious effect but on the battlefield the consequences can be dire. Of particular concern is the targeting of the US military and veteran populations by adversarial influence campaigns. As a subset of the US population, service members and veterans are “not only susceptible to information manipulation targeting the average citizen but are actually the target of additional foreign manipulation efforts.”\(^{18}\) Instead of attacking military targets or infrastructure, adversaries located outside the US can easily access regular information streams and influence networked individuals from within the US—to include military units and service members.\(^{19}\) In hostile regions or combat locations, the information environment is available for manipulation. Traditional psychological operations target the hearts and minds of local populations and intelligence officers consider social media postings and population sentiment in their analysis of the operational context. In short, foreign OIE is truly a whole-of-society problem.

### Blending In

The state of Maryland, and Baltimore City in particular, provides an interesting case study to further illustrate how adversaries can influence the American population. In June 2015, @BaltimoreOnline\(^{20}\) started tweeting. The account shared local-interest news, like the story\(^{21}\) of a five-year-old boy who shot himself in the foot and the death of construction worker killed\(^{22}\) on I-95 in Maryland. In fact, the account continued tweeting Baltimore-specific interest stories until
August 2017, when Twitter traced the account to the St. Petersburg-based Internet Research Agency (IRA) in Russia.23

Roughly a year after @BaltimoreOnline started tweeting, @Blacktivist joined Twitter and Facebook, and started posting in support of various causes in the Black community, eventually gaining more followers than the official Black Lives Matter account.24 Initially, @Blacktivist posted a lot about Freddie Gray, a man whose death in April 2015 at the hands of the Baltimore police sparked protests and riots across the city.25 Posts about Gray were passionate, exclaiming things like, “We are fed up with police violence, racism, intolerance and injustice!”26 And, despite having no clear ties to other longstanding social justice oriented accounts or organizations, people showed up in the streets when @Blacktivist began organizing police brutality protests across the US.27 Parallel to @Blacktivist’s posts about racial justice, @BacktheBadge ran a pro-police and law enforcement ad on Facebook that linked to its “community of people who support our brave police officers” – the ad appeared in the feeds of over 1.3 million users.28 Eventually, Facebook linked both @Blacktivist and @BacktheBadge back to Russia and the IRA.29

Further examples of inflammatory Russian social media accounts are numerous:30 @SecureBorders targeted illegal immigration, posting a photoshopped image of a woman holding a sign that read, “Give me more free sh*t!” and pro-gun Russian bots flooded feeds after the Parkland shooting – some accounts even mimicked the language of National Rifle Association.31 But Russian activity in Maryland is particularly notable: although Maryland is not a presidential election swing state, Russian activities targeted local fissures and tensions in the lead up to the 2016 election, hoping that the local stories would become part of the national consciousness by amplifying inflammatory content online. Looking back, Russia’s activities in the information environment exhibit a deep knowledge of American society and the issues and topics that divide and stress the greater public. Because Russian operatives understand the complicated history of race and law enforcement in America, the killing of a young black man by police, like Freddie Gray and many others, is an easily exploited story.

What Can We Do?

Based on the similarities between the spread of contagions and false information, policymakers should adopt a public health approach to the mis- and disinformation epidemic. The lessons learned from the ongoing battle with COVID-19 provide insight into how a coordinated public health response could work in the information environment. For example, upon entering any government facility or private business, it is immediately clear that there is an ongoing public health crisis: walls are decorated with signs and posters, recommending a suite of sanitizing measures to protect against infection and the spread of COVID-19. Countless internal memos about keeping workspaces, troops, and families safe have circulated, and most guidance places the onus on the individual to self-report an illness or vaccination status, to wear a mask when feeling ill or unvaccinated, to maintain social distance, and to hold one another accountable. To combat mis- and disinformation, similar measures should be taken to alert, educate, and reinforce mitigation measures, drawing the public’s attention to the threat.
Leadership, in the private and public sectors, is also on task for countering the COVID-19 pandemic: events, meetings, and training exercises require COVID-19 risk mitigation plans, and most leaders are also reporting on COVID-19 and vaccination statistics for their respective units or organizations. Vaccination mandates are requiring minimum standards for workplaces while public service announcements continue to urge caution and vigilance. Social media platforms are automatically attaching links to COVID-19 facts and information to any post that mentions the pandemic, public figures regularly give updates to the public, and celebrities use their fame to encourage their fans to get vaccinated. Additionally, the Center for Disease Control’s website is flush with COVID-19 related information and links to additional sources of credible data and information. Again, policymakers should take a similar approach to mis- and disinformation: leaders and public figures should publicly denounce false and misleading claims or persons who spread falsehoods, they should work with private social media platforms to encourage additional efforts to flag and remove false and misleading stories or posts, and the government and trusted public entities should create a repository for resources on events, topics, and issues that foreign adversaries are using to target the American public via influencing campaigns.

However, government intervention is an incomplete response to foreign OIE and domestic mis- and disinformation risks. Returning to the example of COVID-19, the pandemic has highlighted the role of individual responsibility during a public health crisis – ultimately, individuals and their behavior can contribute to, or inhibit, an effective public health response. A single infected person that fails to abide by safety protocols can create a ripple effect that extends beyond their immediate social circle or extended network. The same is true of mis- and disinformation: individual responsibility will play a key role in any effort to build American resilience to foreign OIE and targeted foreign influence campaigns. In many ways, it is our own, individual choices that will determine the outcome of the battle against mis- and disinformation, regardless of the policy choices or their implementation. While a public health and inoculation approach is a good start towards creating resiliency, individuals must also be encouraged to take responsibility for the content they consume.

**Further Reading**

[How to Defeat Disinformation](https://www.foreignaffairs.com/articles/2020-07-14/how-defeat-disinformation) | [Foreign Affairs](https://www.foreignaffairs.com)

[Washington Wakes Up to the Dark Reality of Online Disinformation](https://www.foreignaffairs.com/articles/2020-07-14/washington-wakes-up-dark-reality-online-disinformation) | [Foreign Affairs](https://www.foreignaffairs.com)


Endnotes


20 Twitter Archive, @BaltimoreOnline, http://web.archive.org/web/20160415152157/twitter.com/BaltimoreOnline.


