Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

May 19, 2020

Considering the Source: Varieties of COVID-19 Information

Introduction

In common parlance, the terms *propaganda*, *misinformation*, and *disinformation* are often used interchangeably, often with connotations of deliberate untruths of nefarious origin. In a national security context, however, these terms refer to categories of information that are created and disseminated with different intent and serve different strategic purposes. This primer examines these categories to create a framework for understanding the national security implications of information related to the Coronavirus Disease 2019 (COVID-19) pandemic.

Categories of Information

Propaganda Definition

There is no commonly accepted definition for what constitutes propaganda. To some, it connotes the spread of false information from a governmental source, intended to have persuasive effects. For others, propaganda is merely any promotional material related to organizations both public and commercial. For purposes of this discussion, propaganda is defined as the intentional propagation of an idea or narrative in order to influence and persuade a target audience. Although it may contain factual information, propaganda is intended to persuade rather than merely to inform. By this definition, an organization or government communicating its intent, policies, and values through speeches, press releases, and other public affairs can be considered propaganda. Some forms of propaganda present selective information that is intended to manage perceptions of the truth. Other forms may be unverifiable rhetorical devices, such as slogans, illustrations, editorials, and opinion pieces that lack factual content. These communications can create perceptions that affect behavior and steer decisionmakers toward a certain course of action.

Misinformation Definition

Misinformation is unintentionally false information. Examples include unfounded conspiracy theories, rumors, and web hoaxes spread through social media by users believing them to be true. Misinformation may be the result of laypersons' misinterpretations of scientific material. In some cases, misinformation results from theoretical preliminary scientific research being interpreted as accepted fact. In other cases, the scientific material may be well-researched and documented, but later proven to rely on faulty premises. Major news outlets and governmental sources sometimes unintentionally spread misinformation by reporting on rapidly changing events. While the reporting itself may be caveated as unconfirmed, the information contained therein may then be widely disseminated by well-intended users and platforms. Though unintentional, misinformation can have the effect of exacerbating societal divisions and creating chaos, as the truth becomes more difficult to discern.

Disinformation Definition

Unlike misinformation, disinformation is intentionally false, intending to deceive the recipient. In the international security context, governments and foreign actors seek to use disinformation to their advantage. Examples of disinformation include covertly planting deliberately false news stories in the media, or altering private and/or classified communications before their widespread public release. Coordinated disinformation campaigns often seek to exploit existing fissures within certain demographics, causing further political polarization and the erosion of trust in public institutions. These campaigns may cause decision paralysis, where decisionmakers are overwhelmed with contradictory or otherwise unreliable information. Some disinformation may be easily detected and discredited, such as fraudulent accounts or suspicious news media websites that may be full of typographical errors. Some viral videos and images give the appearance of documentation, but in reality have been computer-generated or altered in a way that is virtually undetectable to the naked eye. These "deep fakes" are an example of disinformation that is increasingly ubiquitous and particularly difficult to combat. Psychological phenomenon such as confirmation bias, defined as the tendency of individuals to interpret new information as confirmation of their existing beliefs, may render attempts to discredit sources of disinformation ineffectual. Disinformation may continue to spread throughout cyberspace even after it has been exposed as false.

Sources: Cyberspace as Medium for Transmission

Cyberspace presents a force multiplier for groups in other countries seeking to amplify a message or narrative. Through the use of social media platforms, all three forms of information discussed here may proliferate throughout the internet, with the combined effect of fomenting discord and confusion. Much of today's information is transmitted in cyberspace, leading many to associate information operations with cybersecurity. Yet on its own, cybersecurity, if defined as securing cyberspace from attack, may be insufficient to prevent the spread of potentially harmful information.

Cyberattacks on Information Sources

While cyberspace is the medium for information transmission, cyberspace operations can be used to achieve strategic goals. For example, an offensive cyberattack on sources of information may be used to create psychological effects such as doubt and mistrust. A cyberattack may be a demonstration of ability, intended to project power through cyberspace regardless of the level of sophistication evident

in the attack methods. An unsophisticated cyberattack on a high-value target may give the appearance of vulnerabilities in the target and capabilities greater than what the attacker may possess, thereby creating a false sense of panic. Some cyberattacks instill fear of worse attacks to come, or carry threats of attacks in the physical world. Using this fear and uncertainty, the cyberattacker may attempt coercion or other forms of exploitation. A cyberattacker may also deny or degrade access to information, overwhelming a website with internet traffic and rendering it unusable. Some attackers tamper with legitimate websites through defacement and placement of other forms of propaganda. Websites and other platforms of online communication may be compromised when an attacker covertly implants malicious code to infect the computers of anyone using those services. Similarly, the communications themselves may be compromised, such as by emails containing attachments and links with malicious code that downloads to the receiver's computer when opened.

The COVID-19 Information Case

COVID-19 and Propaganda

In large part, propaganda efforts center on controlling the narrative around the origin of the virus and management of the outbreak. Chinese and Russian media manipulation, for example, has exploited uncertainties in the origin of COVID-19, encouraging conspiracy theories on the coronavirus as a deliberately engineered creation brought to China by the United States rather than a naturally occurring phenomenon. Other state-sponsored propaganda places a positive spin on the government's positive crisis response, participation in global relief efforts, and ability to contain infection rates compared with other nations. This is often aided by suppression of information that complicates a preferred narrative.

According to CRS Report R46354, *COVID-19 and China: A Chronology of Events (December 2019-January 2020)*, it appears that Chinese officials and state-controlled media initially downplayed the severity and scope of the outbreak, releasing incomplete information on the spread and prevention of the disease and blocking access to some Chinese and foreign news reports. At least eight individuals who attempted to share early information were reprimanded by public security officials for "spreading rumors" and creating "negative social influence." After elevating containment to a national priority, Chinese officials and media shifted to public claims of successful crisis management, with official numbers released to media outlets showing the epidemic coming under control. As other countries have struggled to contain the disease, the Chinese government appears to promote the narrative of China as world leader and the Chinese system of government as superior. Human rights groups such as Reporters Without Borders allege that China monitors and suppresses independent news sources that depart from this narrative.

The accuracy of China's COVID-19 statistics, as well as those from Russia, Iran, and North Korea, has been questioned by U.S. officials.

COVID-19 and Misinformation

Reports of early medical studies on the communicability and prevention of COVID-19 may have had the unintentional effect of misinforming the public, as such reporting was interpreted as having been scientifically proven. Examples include the efficacy of face masks in preventing transmission, whether transmission occurs by airborne or droplet presence of the virus, whether younger persons are relatively less susceptible, and whether certain blood types are more susceptible to contracting the disease. The proliferation of conflicting reports and studies that were later disproven could cause individuals to disregard all medical advice or to take measures that may in fact be counterproductive. Another potentially dangerous aspect of misinterpreting information is the "paradox of warning," where alerts of an imminent crisis lead to policies and behavior changes that prevent or slow the crisis. This in turn leads some observers to conclude that the initial risks were overstated. This interpretation can encourage risky behavior capable of contributing to a resurgence in infection rates.

COVID-19 and Disinformation

Disinformation around COVID-19 may closely resemble propaganda, making it difficult to distinguish between the two. As part of their disinformation efforts, foreign powers may be fabricating stories of COVID-19's creation by the United States as a weapon of war and deliberately planting false accusations in online media. Governments may likewise be fabricating their own crisis handling and rates of infection, or they may be exaggerating, manipulating, or presenting incomplete sets of facts in an attempt to control the narrative. As a propaganda technique, selective omission of factual information can have the same effects as that of commission or active fabrication.

On March 23, 2020, the U.S. State Department released a fact sheet documenting Iran's disinformation attempts, which include false claims of having evidence of COVID-19 as a "biological attack." Russia and China have reportedly attempted to support and amplify Iranian claims that COVID-19 was created by the U.S. government as a biological weapon. In a convergence of messaging, all three governments have criticized the U.S. government's inability to contain the pandemic.

Cyberattacks on COVID-19 Information Sources

In a time of crisis, government and citizen decisionmaking requires timely information. Cyberattackers can capitalize on this need using cyber tools to suppress information on a large scale, gain intelligence, and compromise users and devices. One attack method is to implant malware in factual sources such as government websites and trusted viral information materials. Another method is to target the platforms of producers and disseminators of information through attacks that inhibit access to these resources. For example, recent reported denial-of-service attacks on the Department of Health and Human Service's public-facing website could have been intended to suppress information flow on COVID-19. Such attacks may have other effects, such as undermining source credibility and eroding trust in otherwise accurate sources of information.

Catherine A. Theohary, Specialist in National Security Policy, Cyber and Information Operations

IF11552

Disclaimer