CEPA

Owning the Conversation

Assessing Responses to Russian and
Chinese Information Operations
Around COVID-19

Vera Zakem, Edward Lucas,
and James Lamond

ABOUT CEPA

Contents

About the Authors

Vera Zakem is a recognized leader in advancing technology in service of democracy, countering disinformation, digital authoritarianism, and building resilient societies. She is currently a Senior Technology and Policy Advisor with the Institute for Security and Technology, a Non-Resident Senior Associate with the Center for Strategic and International Studies, and a Founder of Zakem Global Strategies. She has spent two decades working on these issues with the US Government, civil society, and the technology sector.

Edward Lucas is a Nonresident Senior Fellow at the Center for European Policy Analysis. He was formerly a senior editor at The Economist. Lucas has covered Central and Eastern European affairs since 1986, writing, broadcasting, and speaking on the politics, economics, and security of the region.

James Lamond is the Director of the Democratic Resilience Program at the Center for European Policy Analysis. Previously, he was the Managing Director of the Moscow Project and a Resident Fellow at the Center for American Progress, where he covered trans-Atlantic relations, the European Union, US-Russia relations, and countering malign foreign interference.

Acknowledgments

Executive Summary

- Russia and China have created and amplified disinformation and propaganda about COVID-19 worldwide to sow distrust and confusion and to reduce social cohesion among targeted audiences.

- The United States government, the European Union, and multinational organizations have developed a series of interventions in response. These include exposing disinformation, providing credible and authoritative public health information, imposing sanctions, investing in democratic resilience measures, setting up COVID-19 disinformation task forces, addressing disinformation through regulatory measures, countering emerging threat narratives from Russia and China, and addressing the vulnerabilities in the information and media environment.

- Digital platforms, including Twitter, Meta, YouTube, and TikTok, have stepped up to counter COVID-19 disinformation and misinformation via policy procedures, takedowns of inauthentic content, addition of new product features, and partner with civil society and multinational organizations to provide credible and reliable information to global audiences. In addition, digital platforms are addressing COVID-19-related disinformation and misinformation stemming from a variety of state and non-state actors, including China and Russia.

- Several of these initiatives have proven to be effective, including cross-sectoral collaboration to facilitate identification of the threat; enforcement actions between civil society, governments, and digital platforms; and investment in resilience mechanisms, including media literacy and online games to address disinformation.

- Despite some meaningful progress, gaps in countering COVID-19 disinformation and propaganda stemming from Russia and China and unintentional misinformation spread by everyday citizens still exist. Closing these gaps will require gaining a deeper understanding of how adversaries think; aligning and refining transatlantic regulatory approaches; building coordination and whole-of-society information-sharing mechanisms; expanding the use of sanctions to counter disinformation; localizing and contextualizing programs and technological solutions; strengthening societal resilience through media, digital literacy, and by addressing digital authoritarianism; and building and rebuilding trust in democratic institutions.

Introduction

The crisis around COVID-19 and the resulting "infodemic" has been exploited by authoritarian regimes to spread propaganda and disinformation among populations around the world. The Russian Federation and the Chinese Communist Party (CCP) have used the pandemic to engage in information warfare, spread divisive content, advance conspiracy theories, and promote public health propaganda that undermines US and European efforts to fight the pandemic.

In 2021, the Center for European Policy Analysis (CEPA) published two reports, *Information Bedlam: Russian and Chinese Information Operations During COVID-19*[1] and *Jabbed in the Back: Mapping Russian and Chinese Information Operations During COVID-19*,[2] comparing how the Kremlin and CCP have deployed information operations around the COVID-19 pandemic, virus origins, and efficacy of the vaccines to influence targeted populations globally, using the infodemic as a diplomatic and geopolitical weapon. The CCP mainly spread COVID-19 narratives to shape perceptions about the origins of the coronavirus and often push narratives to shun responsibility. Meanwhile, the Kremlin recycled existing narratives, pushing and amplifying them via validators and unsuspecting people in order to sow internal divisions and further exploit polarized views in the West about the efficacy of vaccines, treatments, origins of new variants, and impact to the population. While the world has learned about new COVID-19 variants, such as Omicron, China and Russia have evolved their tactics to spread covid-19 disinformation and propaganda and further sow doubt and confuse the population about the pandemic.

As Russia and China's tactics evolve, this policy brief examines whether Western institutions, including governments, digital platforms, and nongovernmental organizations, have been able to counter information warfare around this unprecedented crisis. This paper examines a broad range of initiatives and responses to counter COVID-19 disinformation coming from Russia and China, and to strengthen societal resilience more broadly. Because addressing this challenge requires a whole-of-society approach, this report highlights government, technology, and civil society interventions, both in Europe and in the US, identifying what works and where there are existing gaps.

Of note, the interventions and related assessments presented here are based on currently available data. It is important to highlight that governments regularly pass new regulations and measures, and digital platforms continue to evolve their policy, product, and enforcement actions in response to COVID-19 disinformation.

A note on terminology: Information operations often take on different forms and can include propaganda, disinformation, and misinformation. For the purposes of this paper, CEPA defines disinformation as the intentional use of falsehoods, narratives, and images by malicious actors to mislead targeted populations. Propaganda, often state-sponsored, seeks to mislead and psychologically manipulate the population by limiting and suppressing access to factual and external information the population can consume. Misinformation is often spread by everyday citizens or benign actors across all mediums unintentionally, but equally, that can have serious real-world consequences and lead to violence. This paper examines covid-19 disinformation and propaganda stemming from Russia and China, as well as the unintentional spread of misinformation that may contain Russian and Chinese disinformation and propaganda.

Government Interventions

While initially caught off guard by the information crisis that accompanied the pandemic, over the last two years the United States federal government, select European nations, the European Union (EU), and multinational institutions have made a series of interventions to counter COVID-19 information operations from Russia and China.

United States Federal Government

With significant spikes in COVID-19 cases, especially from variants such as Delta and Omicron, the US government has been taking proactive measures to counter COVID-19 disinformation. In 2021, US Surgeon General Vivek H. Murthy put out an advisory on building a healthy information environment to counter COVID-19 disinformation.[3] The focus of this advisory is to equip the US public with the best resources and tools to identify both misinformation and disinformation so that the US public can make the most informed choices; address health disinformation in local communities; expand research on health disinformation; work with digital platforms to implement product designs, policy changes, and their enforcement; invest in long-term resilience efforts to counter COVID-19 disinformation; and use the power of partnerships to convene federal, state, local, tribal, private, and nonprofit leaders to identify the best prevention and mitigation strategies.

Similarly, the Cybersecurity and Infrastructure Security Agency (CISA) in the US Department of Homeland Security (DHS) put forth a COVID-19 disinformation tool kit to educate the US public about COVID-19 disinformation, provide the best resources, and help the public understand credible versus misleading content. The tool kit calls out Russian and Chinese state-sponsored elements as some of the key actors pushing and amplifying COVID-19 disinformation. As DHS/CISA point out, the Kremlin and CCP's goal is to create "chaos, confusion, and division ... and degrade confidence in US institutions, which in turn undermines [the US government's] ability to respond effectively to the pandemic." [4]

The US Department of State's Global Engagement Center (GEC) continues to be the US government's interagency belly button for understanding, assessing, and building partnerships to counter foreign state sponsors (and non-state sponsors) of disinformation and propaganda. This includes understanding and assessing disinformation activities from Russia and China globally. The GEC partners with civil society, research, and academic institutions to understand Russian and Chinese disinformation and malign influence. Of note, in August 2020, the GEC released a special report on the pillars of the Russian disinformation and propaganda ecosystem, which highlights Russia's tactics and narratives to spread COVID-19 disinformation to targeted countries and populations.[5] Considering extensive Russian disinformation and propaganda in Ukraine, the State Department created a website aimed at disarming disinformation, which provides credible content, informs the public about disinformation, and exposes disinformation from Russia (and other) actors.[6]

In February 2021, the US Agency for International Development's (USAID's) Center of Excellence on Democracy, Human Rights, and Governance released a Disinformation Primer, which highlights counter disinformation programs to deter and prevent disinformation from China, Russia, and other malicious actors.[7] This primer specifically focuses on building societal resilience in developing nations, strengthening media development, promoting internet freedom, and supporting democracy and anti-corruption-related programs.

The US government has also taken strong actions through more traditional measures of statecraft. For example, in April 2021, the Biden administration issued sanctions against Russia for a series of malign activities, including cyberattacks, election interference, corruption, and disinformation. These sanctions were not specifically directed at COVID-19 information operations necessarily but were broadly meant to impose costs for Russian malign activities, including disinformation.[8]

Congress also proposed a series of measures to limit the spread of disinformation, promote digital literacy, and keep digital platforms accountable. These measures include a plan to appropriate $150 million toward countering propaganda and

A person riding down an escalator. Credit: «covid-19» by Silvio Naef, April 24, 2020, is licensed under CC BY-ND 2.0, https://www.flickr.com/photos/108147727@N03/49816469732

disinformation from China, Russia, and foreign non-state actors through the Strategic Competition Act.[9] However, getting bipartisan congressional approval to pass disinformation-related legislation has not been easy. For example, efforts such as the Honest Ads Act, the Digital Citizenship and Media Literacy Act, and Protecting Americans from Dangerous Algorithms Act have been introduced in Congress, but have not passed.[10,11] In addition, in order to address the spread and promotion of health-related disinformation on digital platforms, US Sen. Amy Klobuchar (D-MN) recently introduced the Health Misinformation Act, co-sponsored by US Sen. Ben Ray Luján (D-NM), to create an exception to Section 230 of the Communications Decency Act, which gives digital platforms legal immunity from liability for content posted by users.[12] This was introduced in July 2021; it is still pending approval.

European Governments and the European Union

Compared to the US, the EU and several European governments have been ahead of the curve in countering Russian and Chinese disinformation and malign influence, as well as keeping digital platforms accountable. This is largely because Europe, particularly Central and Eastern European states, have been dealing for some time now with malign influence, disinformation, and misinformation campaigns; election

interference; and digital authoritarianism certainly from Russia and, to a lesser degree, from China.

European Union

Most notably, in 2015, the EU created the East StratCom Task Force, which identifies, monitors, and analyzes the impact of Russian disinformation on targeted populations.[13] Following earlier efforts, in 2020, the EU adopted the European Democracy Action Plan (EDAP) with a focus on promoting free and fair elections, strengthening media freedom, and countering disinformation.[14] As part of the EDAP, the EU strengthened the Code of Practice designed to keep online platforms and advertisers accountable in countering disinformation.[15] To receive credible information on the pandemic and vaccines and prevent malicious information from actors like China and Russia reaching the European public, the signatories to the Code of Practice created a COVID-19 monitoring and reporting program to curb COVID-19 disinformation on digital platforms.[16] Finally, the European Parliament has given initial approval to the Digital Services Act, which will enable the EU to conduct greater scrutiny and regulation of technology companies and digital platforms, including monitoring their policies and enforcement actions, to create a healthy information ecosystem.[17]

The United Kingdom

The United Kingdom's (UK's) Department for Digital, Culture, Media, and Sport established a counter disinformation unit to monitor disinformation coming from state actors as well as non-state actors.[18] In addition, the UK's minister of state for digital and culture, Caroline Dinenage, launched a digital literacy strategy for ordinary citizens to combat COVID-19 and other disinformation to ensure people know how to distinguish credible from inauthentic content, think critically, and act responsibly online.[19]

Sweden

Sweden created a Psychological Defense Agency with the goal of identifying, analyzing, and responding to disinformation and other misleading content.[20] As the agency explains, disinformation can be aimed at "weakening the country's resilience and the population's will to defend itself or unduly influencing people's perceptions, behaviors, and decision making."[21] A big part of this agency's work is to strengthen the Swedish population's ability to withstand disinformation campaigns and defend society as a whole. Tasked with both preventive and operational measures, the agency aims to conduct its activities and operations during crises and steady state.

France

The French government has taken a series of measures with mixed results. In spring 2020, the government created the website Désinfox to combat COVID-19 disinformation and serve as a reliable collection of news on the pandemic. However, it immediately faced criticism for its selectivity of news outlets and its lack of articles critiquing the government's response and the site was soon removed.[22] The government also launched a website, Santé.fr, dedicated to informing citizens about health topics via articles and other resources. Due to the pandemic, it now includes information on vaccination and testing sites as well as a range of other COVID-19-related topics.[23] The government recently created an agency, Viginum, to counter foreign information operations, particularly in the lead-up to the 2022 presidential election.[24]

Germany

In response to the increased threat of disinformation, Germany reformed its media regulatory framework in 2020, and enforced the 2020 Interstate Media Treaty.[25] State media authorities in Germany contact online providers about online allegations that were presented without sources, images that were taken out of context, and conspiracy theories, among other harmful online content.[26] German conspiracy counseling centers have also helped curb the spread of disinformation by treating clients who believe conspiracy theories regarding the pandemic, masks, and vaccinations.[27] These free centers help citizens who have construed views based on false information.

"Elves"

The Baltic states have long been targets of Russian disinformation. In 2014, citizens in Lithuania established voluntary watchdog groups, known as the "Elves"—a direct response to the Kremlin "trolls"—to flag disinformation online, report suspicious accounts, and fact-check news reports. During the pandemic, the Elves created a new task force to specifically tackle COVID-19-related disinformation and created a Facebook page to share accurate news coverage and address conspiracies and disinformation.[28] The Elves take COVID-19 disinformation extremely seriously; two-thirds of the Elves' administrators work in health care.[29] Over the years, the Elves have gained more followers and have grown from 40 to more than 5,000 members active in the Czech Republic, Finland, Slovakia, Ukraine, and even Germany.[30]

Hospital staff at the Hospital Clínic in Barcelona conduct their work. Credit: «Atenció pacients de COVID-19 a l'Hotel Plaza_18» by Francisco Àvia_Hospital Clínic de Barcelona, March 31, 2020, is licensed under CC BY-ND 2.0, https://www.flickr.com/photos/140728541@N03/49722534448

United Nations

With the rise of COVID-19 disinformation, the United Nations (UN) has taken a number of actions to ensure that citizens of the world have the most accurate, up-to-date information and abilities to identify and distinguish credible from inauthentic content. For example, UN Under-Secretary-General for Global Communications Melissa Fleming outlined the UN's "Verified Initiative," which is charged with countering malicious content, including related to COVID-19.[31] The idea behind the initiative is to provide creative and credible content in more than 60 languages. In addition, the UN engages with digital platforms to address the productive role that these platforms can play in countering disinformation more effectively. Along with traditional mediums such as the UN Information Centers, the UN uses social media to push out credible information to citizens. However, given the role that Russia and China play in the UN, the international body's influence to counter Russian and Chinese disinformation and propaganda remains somewhat limited.

World Health Organization

With so much malicious content stemming from Russia, China, and other actors over the efficacy of COVID-19 vaccines, the World Health Organization (WHO) has been the leading multinational organization and has partnered with governments, civil society organizations, and digital platforms to counter COVID-19 disinformation. In response to the COVID-19-related infodemic, the WHO launched several initiatives

over the last two years. These include partnering with the UK government to create a "Stop the Spread" public awareness campaign to encourage people to verify the credibility of the information they access and think critically about the information that is being consumed.[32] In addition, the WHO launched a "Reporting Misinformation" awareness campaign to show the public how to effectively report disinformation and misinformation to digital platforms.[33] Additionally, in partnership with Cambridge University and the UK Cabinet Office, the WHO developed a "Go Viral" game that exposes disinformation and teaches players how to identify false information.[34] As part of the game, players are connected with the WHO's "MythBusters."[35]

NATO

NATO has done extensive work to counter disinformation in collaboration and partnership with member states, media, the EU, the UN, and civil society. For example, NATO created a COVID-19 Task Force[36] to combat COVID-19-related disinformation. Through its Public Diplomacy Division, NATO monitors COVID-19-related and other disinformation stemming from Russia and other actors and fact-checks in collaboration with the EU. NATO set up a webpage, "NATO-Russia: Setting the Record Straight,"[37] to expose Russian disinformation and dispel myths. NATO also conducts regular cybersecurity trainings, such as the annual Cyber Coalition exercise and the Crisis Management Exercise, which educate the entire alliance about cyber defenses. To further share best practices about cyber defense, NATO has designated training centers such as the NATO Cooperative Cyber Defense Center of Excellence, the NATO Communications and Information Academy, and the NATO School in Oberammergau, Germany, which offers training and courses on cyber defense.[38]

G7 Rapid Response Mechanism

The G7 Rapid Response Mechanism (RRM) is another multilateral institution that has improved coordination and sharing of best practices to counter disinformation. The RRM was created in June 2018 to strengthen coordination across the G7 in "assessing, preventing, and responding" to threats to democracy, including disinformation and foreign interference[39] At present, this is a government coordination mechanism, with Canada serving as the coordinating agent with the other six G7 countries. The goal for the RRM is to share information about impending threats and coordinate on potential responses should attacks occur. The coordination unit produces analysis on threats and trends to anticipate threats and prepare for coordinated action. This increased coordination is a useful development from what existed prior to 2018 as democracies around the world work to counter common challenges.
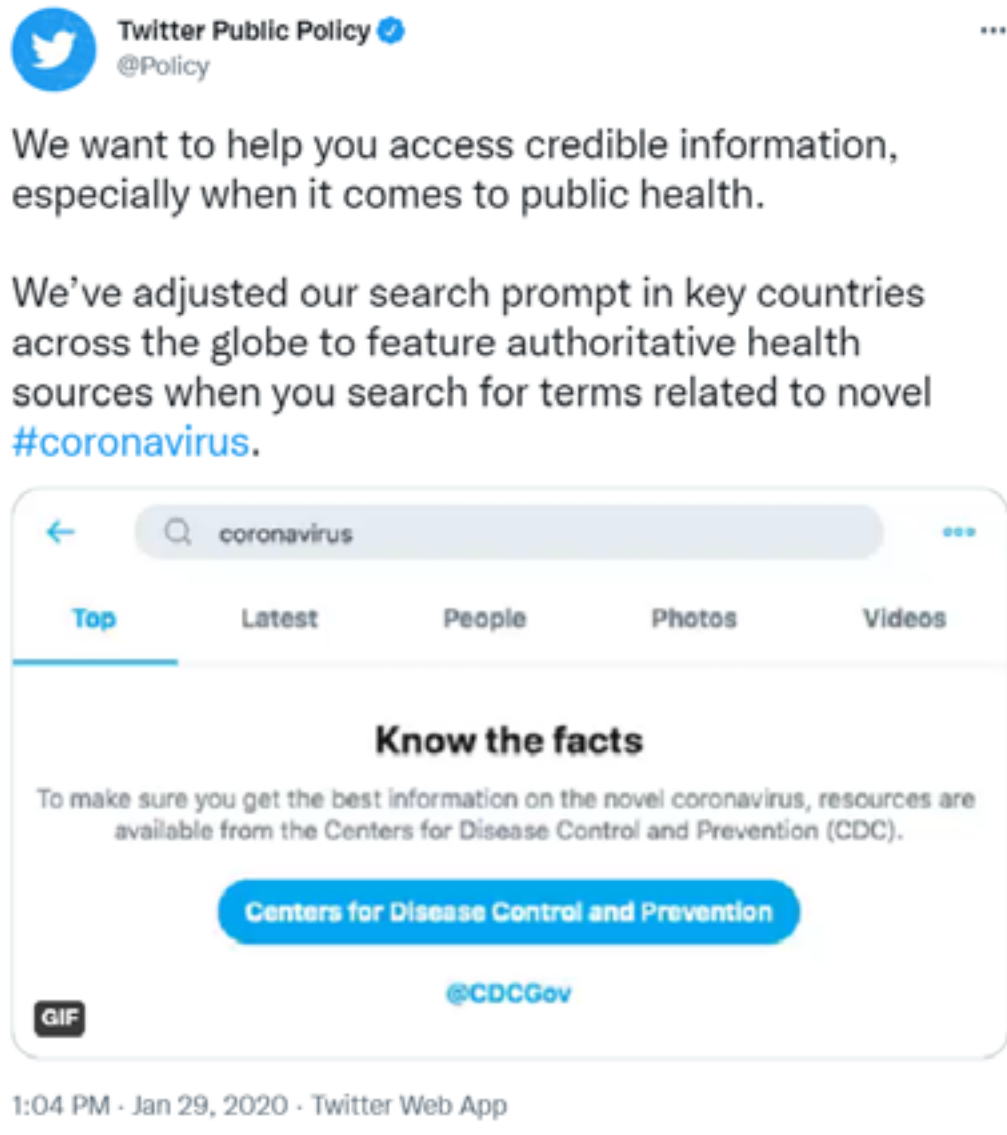
Digital Platform Responses

The Kremlin, the CCP, and their allies have exploited the virality of social media and citizens' inability to think critically about the information they are consuming to create and amplify false content globally. During the pandemic, sharing falsehoods costs lives. In response to this massive challenge, digital platforms have stepped up their efforts to counter COVID-19 disinformation and misinformation. These efforts have focused on developing COVID-19-specific policies, take downs of malicious and inauthentic content, designing new product features and policy campaigns to push credible content about the pandemic, and partnering with governments, civil society, and nongovernmental organizations (NGOs) locally and globally to address these evolving threats. While there are many digital platforms, blogs, messaging services, and providers, this report focuses on a select few: Twitter, Meta, YouTube, TikTok, and Microsoft. As mentioned previously, policies, enforcement actions, and product features change on a regular basis in response to the continuous flow of COVID-19 disinformation from threat actors. In addition, as we highlighted above, a majority of these interventions have been designed to be actor agnostic.

Twitter

Twitter has developed a comprehensive set of strategies to counter COVID-19 disinformation.[40] These strategies focus on providing reliable information from credible sources regarding COVID-19; protecting the public conversation, which includes a mix of new policies; enforcement actions and product features; building private-public-civic partnerships with governments, journalists, and NGOs; empowering researchers to study COVID-19 disinformation; building transparency metrics on COVID-19 disinformation, among other initiatives. For example, Twitter developed a "Know the Facts" prompt with links to reliable sources, such as WHO and vaccines.gov, to inform the public about where to go for credible information.[41] The graphic below shows this prompt.

Separately, in December 2021, Twitter outlined a comprehensive COVID-19 misleading information policy that provides information on what content and behavior constitutes a violation of this policy.[42] This includes misleading people about the efficacy of preventive measures, treatments, vaccines, official regulations, and other protocols. Twitter also outlined its enforcement actions; when accounts are in violation of its policies, the accounts may be removed, have their visibility reduced, or be permanently suspended. For example, in June 2020, Twitter removed more than 170,000 accounts tied to Chinese influence operations that spread COVID-19 narratives.[43]

Source: Twitter, https://twitter.com/policy/status/1222581255574827008.

Meta

Meta, formerly Facebook, has also put forth a number of strategies to reduce the prevalence of COVID-19 disinformation campaigns on its suite of apps, provide credible information to consumers, and partner with NGOs, verified government officials, and journalists.[44] Among its strategies, Meta launched a COVID-19 information center (as depicted in the graphics below), prohibiting exploitive tactics in advertisements, supporting health and economic relief efforts, "down-ranking" false or disputed information on the platform's news feed, and activating notifications for users who have engaged with misleading content related to COVID-19.[45] In addition, the encrypted messaging platform WhatsApp, owned by Meta, has also been plagued by COVID-19 disinformation. In response, WhatsApp created a WHO Health Alert, a chatbot to provide accurate information about the coronavirus that causes COVID-19.[46]
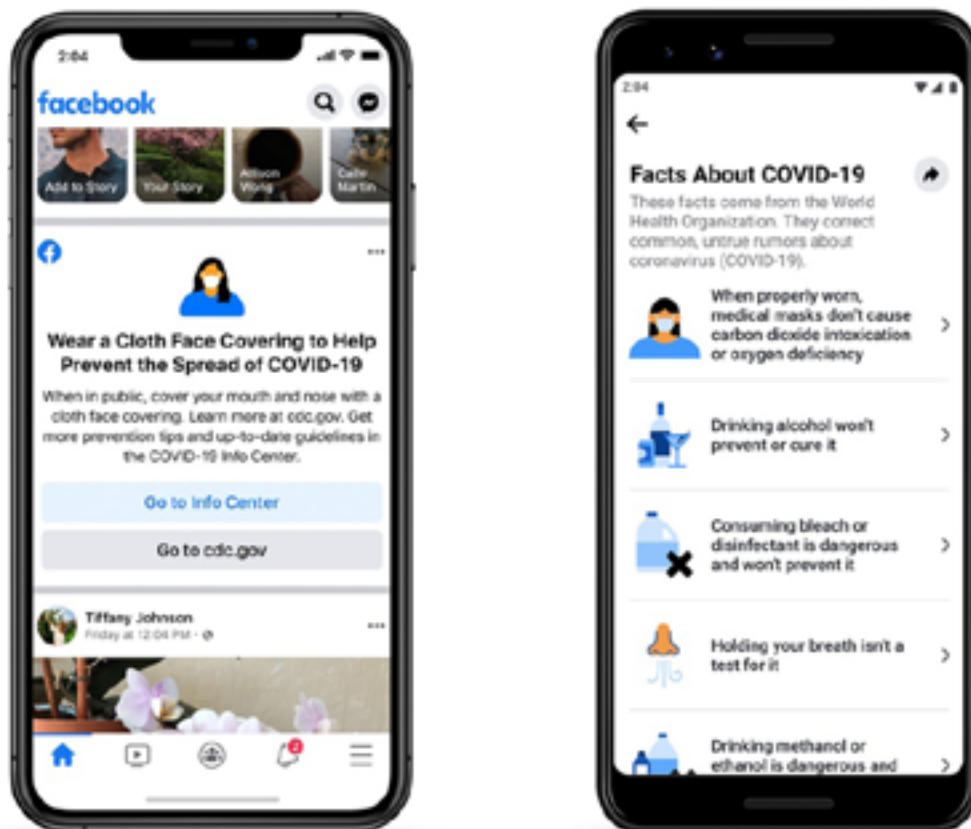
Source: Kang-Xing Jin, "Keeping People Safe and Informed About the Coronavirus," Meta, December 18, 2020 https://about.fb.com/news/2020/12/coronavirus/.

With Russia, China, and their affiliates spreading COVID-19 disinformation throughout the Meta family of apps, Meta has continuously removed inauthentic behavior and content originating from these two countries. For example, in December 2020, Meta partnered with Graphika, a software as a service and a managed services company, to remove coordinated inauthentic content and accounts that originated in Russia, including 61 Facebook accounts, 29 pages, seven groups, and one Instagram account.[47] These networks posted misleading content about COVID-19 and the Russian vaccine, among other topics, in French, English, Portuguese, and Arabic. Similarly, in December 2021, Meta removed more than 600 accounts, pages, and groups connected to Chinese influence operations spreading COVID-19 disinformation, including an account falsely claiming to be a Swiss biologist.[48] This account also posted misleading content on Twitter, claiming that the US was pressuring the WHO to blame China for the rise of COVID-19 cases.

YouTube

YouTube also established a range of policies and product features and has taken enforcement actions to curb the spread of COVID-19 disinformation and Russian and Chinese malign content.[49] YouTube's community guidelines prohibit medical disinformation. In addition to setting policies, YouTube has begun to label content that it believes may be spreading COVID-19 disinformation and misinformation.[50] Like other platforms, YouTube has been working with health officials, NGOs, and government agencies to give its viewers access to authoritative and credible content about COVID-19. This includes the latest news on vaccines and tests, as depicted below.

YouTube has also taken specific actions against Russian and Chinese disinformation. For example, it suspended the German-language Russia Today channel for one week after it violated its COVID-19 information guidelines.[51] In response, the Russian Federal Service for Supervision of Communications, Information Technology, and Mass Media, *Roskomnadzor*, accused YouTube of censorship and threatened to block the service.

Source: Twitter, March 19, 2020. https://twitter.com/YouTubeInsider/status/1240734272325070855.

15

TikTok

With approximately 15 million daily active users and the appeal of younger audiences, TikTok has become a major source of information on politics, health, sports, and entertainment. Unfortunately, it has also become a source of widespread COVID-19 disinformation.[52] TikTok's connection to ByteDance, a Chinese multinational internet technology company, has created concerns that TikTok could be spreading digital authoritarianism, Chinese propaganda, and censorship. To that end, TikTok developed strong community guidelines to combat COVID-19 disinformation and related harmful online content, partnered with multinational organizations and government institutions, and creatively provided credible information about the pandemic.[53] To enforce disinformation policies, TikTok has partnered with international fact-checkers to ensure the accuracy of its content and identify disinformation threats early. TikTok promotes COVID-19 best practices through campaigns such as the #SafeHands Challenge to promote healthy handwashing, which has gained 5.4 billion views, and the #DistanceDance challenge to encourage physical distancing.[54]

Microsoft

While not a digital platform, Microsoft has become a leading player in developing technology solutions, partnering with civil society and governments to counter disinformation. For example, in response to COVID-19, Microsoft created "information hubs" on its news tabs, and has put public service announcements about COVID-19 atop its search queries.[55] Microsoft also adopted an advertisement policy that prohibits advertisements that seek to exploit the COVID-19 pandemic for commercial gain, spread disinformation, and undermine the health and safety of citizens. As part of this effort, Microsoft advertising prevented approximately 10.7 million advertiser submissions based on these criteria, 5.73 million of which would have gone to the European markets. With its Defending Democracy Program,[56] Microsoft has partnered with media organizations on content authenticity and media literacy, and has been developing technical solutions to take down fake images and videos.[57]

Civil Society and the Emerging Technology Ecosystem

To counter Chinese and Russian COVID-19 disinformation, civil society and emerging technologies organizations such as Zignal Labs, Logically, Graphika, Alethea Group, and many others have pioneered collaborations with digital platforms, civil society, media, and governments to understand, identify, and expose the evolving Russian and Chinese disinformation narratives, and provide mitigating strategies via content moderation, threat deception, and exposure. Critical to this effort has been the

use of artificial intelligence, machine learning, and natural language processing to identify disinformation narratives and develop mitigation strategies.

Similarly, many research and academic institutions and NGOs have stepped up to provide much needed novel research and analysis to counter Russian and Chinese disinformation campaigns, share information, and provide critical information to governments, media, and digital platforms globally when they have needed it most. In addition to CEPA, organizations such as the Atlantic Council's Digital Forensic Research Lab (DFRLab); Stanford University's Internet Observatory; Carnegie Endowment for International Peace's Partnership for Countering Influence Operations; Harvard University's Shorenstein Center on Media, Politics and Public Policy; the Institute for Security and Technology; German Marshall Fund's Alliance for Securing Democracy, and many others have contributed to developing solutions. In addition, organizations such as the National Democratic Institute (NDI), the International Republican Institute (IRI), the International Research and Exchanges Board (IREX), and other implementing partners have been working with the US government and other partner government missions around the world to counter Russian and Chinese COVID-19 and political disinformation in developing nations. These efforts have included media and digital literacy programs, such as IREX's Learn to Discern; journalistic and cyber hygiene trainings; public diplomacy and strategic communication initiatives; anti-corruption initiatives; and institution-building initiatives.[58]

What Is Working

As disinformation and misinformation have evolved and adapted over time, there are numerous ways that European governments, the US government, digital platforms, and civil society have made progress, and several initiatives are already working. While there is more to be done, particularly when dealing with the global infodemic and nefarious actors like China and Russia, it is important to acknowledge areas where there have been improvements.

Exposure of disinformation campaigns has worked *somewhat* to raise awareness

Regardless of the actors who spread it, COVID-19 disinformation and propaganda have real-world impacts — the infodemic costs lives. Awareness about this concern coupled with the ability of policy makers, health officials, and community leaders to communicate to the public about the dangers of disinformation and misinformation via direct communication, social media, and infotainment is critical to address this challenge, and in this case, save lives. Efforts to expose disinformation campaigns have helped shed light on the challenge. One such effort was the GEC's August 2020 report, *Pillars of Russia's Disinformation and Propaganda Ecosystem*, that outlines official government communications, state-funded global messaging, cultivation of proxy sources, weaponization of social media, and cyber-enabled disinformation. It also profiled seven Kremlin-aligned disinformation proxy sites and organizations, highlighting their amplification of anti-US and pro-Russian positions during the COVID-19 outbreak.[59] Similarly, EUvsDisinfo has issued a series of special reports on the narrative campaigns from China and Russia.[60] Separately, according to the Pearson Institute and the Associated Press-NORC Center for Public Affairs Research, in October 2021, 95% of US citizens believed that disinformation is a problem, including on COVID-19.[61] Despite this statistic, some continue to believe that the government, public health officials, and vaccine manufacturers are the ones spreading disinformation about the pandemic. Governments, civil society, and digital platforms continue to evaluate the impact of exposure campaigns. Questions such as how much exposure reaches the target audience, does it change audience and threat actor behavior remain important points for analysis, policy considerations, and interventions.

> **"COVID-19 disinformation and propaganda have real-world impacts — the infodemic costs lives."**

Building long-term resilience

Wellbeing Coordinator Poh Geok Hui recaps the smartphone skills that Madame Chong Yue Qin acquired during her inpatient stay at a SingHealth Community Hospital in Singapore. Credit: © WHO / Blink Media — Juliana Tan https://photos.hq.who.int/search/results?s[adv]=1&s[credit]=WHO+%2F+Blink+Media+%E2%80%94+Juliana+Tan

Countering disinformation from China, Russia, and other actors is a long-term challenge that does not have quick fixes — rather, long-term resilience mechanisms are needed. To that end, the international community has started to recognize the need to strengthen democratic institutions, support independent media, counter digital authoritarianism, and strengthen digital citizens and media literacy skills of journalists. At the Summit for Democracy in December 2021, US President Joseph R. Biden, Jr., announced a set of sweeping proposals on democratic renewal with a desired objective of strengthening societal resilience to respond to these challenges.[62] For example, the US announced a $30 million International Fund for Public Interest Media, a multi-donor fund to support free and independent media around the world, particularly in the developing world, and a Media Viability Accelerator to support the financial viability of independent media.[63]

The US and many European countries are investing significantly in digital and media literacy and civic education for all ages to strengthen societal resilience and counter Russian and Chinese COVID-19 and other related disinformation. Thanks to innovative initiatives from partner and implementing organizations, the US and Europe have been implementing initiatives in developing countries. For example, IREX's Learn to Discern training program and curriculum has been offered to diverse audiences with the goal of inoculating communities from public health disinformation, decreasing polarization, and empowering people to think critically about the information they consume.[64] To reach audiences in creative ways, academics and technologists have developed counter disinformation games that force the players to tackle disinformation head on by creating fake personas, attracting followers, and creating fake content. By playing

On the US 7th Fleet flagship, USS Blue Ridge (LCC 19), in the South China Sea, Lieutenant Commander Rebecca Pavlicek and Hospital Corpsman Gian Molina test samples in a BioFire Film Array. Credit: «200314-N-VA840-0005 - U.S. Navy photo» by Mass Communication Specialist 1st Class Leonard Adams, March 14, 2020, is licensed under CC BY-ND 2.0, https://www.flickr.com/photos/43397645@N06/49682014766

games such as DROG and the University of Cambridge's Bad News Game,[65] players can get into the mindset of the threat actor and their tactics.

Improved coordination between digital platforms and civil society

Over the past years, there has been greater collaboration between digital platforms and civil society to combat disinformation around elections and COVID-19 and stemming from violent extremists. For example, the Trust and Safety community formed a Digital Trust and Safety Partnership to foster collaboration and a shared lexicon between digital platforms.[66] The long-term success of this initiative remains to be seen. Similarly, as part of an effort to curb COVID-19 disinformation, digital platforms have been meeting with the WHO and government officials to ensure that people receive credible information about the pandemic, and digital platforms take appropriate action on COVID-19 disinformation.[67]

In addition, organizations such as NDI, IRI, and the DFRLab have been critical in serving as a partner and a liaison between digital platforms and civil society in emerging markets, including the Global South. This has been important in ensuring that civil society organizations and citizens know how to report disinformation to digital platforms, get access to credible information, know how to engage in the technology space, and receive digital literacy training to be responsible stewards of information. The Design 4 Democracy Coalition, a coalition of civil society and human rights organizations, also plays an important role in forging partnerships between civil society and digital platforms.[68] These organizations provide access, relationships, and critical exposure to marginalized communities and populations in the Global South — places where digital platforms may not have the full operational capability. However, civil society has struggled with access to data, making it difficult for outside researchers to meaningfully study certain platforms.

Recognition of the need for a whole-of-society approach

While governments, digital platforms, civil society, emerging technology organizations, and researchers have differing viewpoints on ways to protect the public and marginalized communities from COVID-19 disinformation, all of them recognize that a whole-of society approach is needed to counter Russia and China's intentional spread of propaganda and disinformation and build long-term resilience mechanisms. However, as described below, gaps still exist on how to implement such an approach.

As with elections or politically motivated disinformation, countering COVID-19 information operations from Russia, China, and other actors requires a whole-of-society approach that strengthens partnerships and prioritizes information sharing and collaboration between governments, multinational organizations, digital platforms, civil society, and the research community. However, while progress has been made to bring these stakeholders together and move the needle on this issue, gaps remain, and additional progress is needed. As Alina Polyakova and Daniel Fried point out in their report, *Democratic Offense Against Disinformation*, the "whack-a-mole" approach must stop; it is crucial for governments and organizations to get on the offense.[69]

How do we get on the offense? Gaps that exist in designing holistic and operational campaigns to counter COVID-19 disinformation must be addressed and greater focus must be centered on what these adversaries fear most — resilient democratic societies with healthy information ecosystems that can withstand information manipulation and disinformation in all its forms.

What Is Still Missing

Understand how the adversary thinks

First, in playing a "whack-a-mole" game, a gap exists in the inability to think from the perspective of the adversary. *What are their desired objectives? What are the end states? What tools do the Russians and Chinese use to spread disinformation, and how do they seek to influence change in behavior?* Therefore, to design strategic and operational-level campaigns to counter COVID-19 and other disinformation from Russia and China, it is crucial to think about the threat actor, how they share content, and their desired outcome: to cause confusion, reduce social cohesion, spread fear, and, ultimately, change the behavior of the targeted population. Thus, the transatlantic community needs to articulate the desired outcome and change in behavior of their interventions. The desired objective should be populations that are capable of critical thinking, distinguishing facts from fiction, who are supported by democratic norms and values, and strong resilient institutions.

Develop, refine, and align on transatlantic regulatory approaches

Second, there is no common transatlantic regulatory approach to address disinformation coming from Russia and China. For example, the EU adopted the European Democracy Action Plan and the Code of Practice to counter disinformation, yet individual European countries respond to disinformation campaigns from Russia and China differently as information proliferates online in unique ways. While the EU initially passed the Digital Services Act's provisions to curb big tech's ill-intended advertising practices, these provisions need to be negotiated with each individual EU member state to enforce the provisions stipulated in the act. How each state will establish transparency, accountability, and auditability measures with the digital platforms is yet to be determined. In addition, the US Congress has proposed a series of meaningful legislative proposals that could stymie disinformation and other malicious content, and keep actors like Russia and China, and digital platforms

> "Gaps that exist in designing holistic and operational campaigns to counter COVID-19 disinformation must be addressed and greater focus must be centered on what these adversaries fear most — resilient democratic societies with healthy information ecosystems that can withstand information manipulation and disinformation in all its forms."

accountable. However, due to partisan gridlock and differing understanding about the harmfulness of disinformation, Congress has had trouble passing legislation that has been introduced on this subject and there have been delays implementing authorized initiatives.

As the US Department of State stands up its Bureau for Cyberspace and Digital Strategy, an opportunity exists for the US to partner with European counterparts on diplomatic engagement. The US government has yet to put forth a codified disinformation strategy that is coordinated by the White House. Such a strategy should pull together all instruments of US national power and all respected agencies that address the threat domestically and internationally, build democratic institutions, strengthen societal response, and assess how disinformation impacts marginalized populations globally, including women and girls.

Stand up a coordination and information-sharing whole-of-society mechanism for information integrity and resilience

Third, given the different regulatory environments and overall acknowledgement of the societal challenges that stem from Russian and Chinese COVID-19 and related disinformation, the

"These provisions need to be negotiated with each individual EU member state to enforce the provisions stipulated in the act."

international community does not have a unified forum to address disinformation and other harmful content. The G7 RRM has done some work in establishing coordination among the G7 governments, but at the present time, a mechanism does not exist to pull aligned governments, including those from the Global South, digital platforms, civil society, and research communities, together to collaborate and share information, foster exchanges, anticipate and address threats *before* they escalate, and develop mechanisms to strengthen societal resilience to disinformation. The bipartisan Task Force on the US Strategy to Support Democracy and Counter Authoritarianism proposed a Global Task Force on Information Integrity and Resilience.[70] In this proposal, like-minded democracies would take rotational responsibilities to lead this task force and establish a forum for a whole-of-society collaboration, coordination, and information sharing, including participation from the Global South's like-minded democracies. Without such a mechanism, the "whack-a-mole" game, rather than a cohesive strategy and campaigns to counter Russian and Chinese COVID-19 and other disinformation efforts, will continue.

Photo: Wellbeing Coordinator Kwek Peck Keow helps patient Kwok Alex Djenbu learn how to use their mobile phone at Sengkang Community Hospital in Singapore. Credit: © WHO / Blink Media — Juliana Tan, 2021 https://photos.hq.who.int/preview/89649

Leverage traditional tools of statecraft

Fourth, the US and Europe can better coordinate on leveraging traditional tools of statecraft, such as sanctions, to combat information operations. As previously noted, the US has issued sanctions as a mean of imposing costs on targets for maliciously and deliberately spreading disinformation. However, the deterrent effect of these sanctions has been limited because it has primarily been the US implementing them, and as was demonstrated with the 2014 package of sanctions against Russia for its invasion of Ukraine, sanctions are most effective when the US and the EU work together. The European Parliament's Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation, recently voted to approve a report that, among other things, calls for the EU to beef up its capabilities and build a sanctions regime against disinformation.[70] An effort such as this in coordination with the US could be a more effective measure for creating a cost for malign information operations.

Localize and contextualize interventions

Fifth, to counter the various forms of disinformation, a one-size-fits-all approach will not work. Rather, a continued set of localized, population-centric, contextual, culturally appropriate solutions is needed. While digital platforms have expanded their global footprint and partnerships with civil society, human rights organizations, and governments, a significant investment in localized and contextual solutions is needed. For example, digital platforms should increase investment in research on the impact of disinformation on marginalized populations, including in the Global South, and invest in continuous engagement and operations in emerging markets and local languages.

A real need exists to reach people outside of the capitals and across diverse communities, including women and girls. This matters because these communities are the ones that specifically need access to credible information, digital and media literacy training, knowledge about how to report disinformation to digital platforms, and with whom to engage. Thus, creating these types of local solutions can have a significant impact. In addition, addressing bias in algorithms, particularly as it relates to cultural, linguistic, religious, and ethnic bias among marginalized communities, remains a concern. As digital platforms work on these solutions, localized and culturally appropriate research that can complement the work of addressing algorithmic bias can help steer toward localized solutions to counter disinformation in these communities. Finally, to help localize and contextualize interventions, digital platforms should make greater investments in sharing data to facilitate research to understand the impact that platform interventions have on diverse populations.

> **"A real need exists to reach people outside of the capitals and across diverse communities, including women and girls."**

Building and rebuilding trust in democratic institutions

Sixth, countering disinformation from Russia and China requires developing long-term solutions to strengthen democratic institutions and societal resilience. While there has been significant headway in this arena, several gaps exist on both sides of the Atlantic. First, while instant results in countering disinformation are wanted, they will not be achieved without understanding the root causes within societies, including divisions, and cultural, religious, and historical underpinnings that can further divide a society and drive polarization. Second, due to a lack of trust in democratic institutions, people do not view these institutions as reliable and

credible sources of facts about COVID-19 or other contentious topics. For example, in June 2020, only 13% of US citizens had a great deal of trust in the COVID-19 information that was provided by the federal government.[71] As a solution to these gaps, leaders should prioritize listening to people from all backgrounds, people-to-people engagement, and creatively using social media to communicate effectively and empathetically and regain trust with people from diverse backgrounds.

Strengthen societal resilience through advancing media and digital literacy, countering digital authoritarianism, and measuring the impact of policy interventions

Seventh, and finally, while there is a broad agreement that promoting internet freedom, strengthening media institutions, and increasing media and digital literacy are crucial to building a healthy information ecosystem to counter disinformation, additional resources are needed to fully implement these initiatives at scale and with the right local context and nuance globally. Russia and China have been perfecting their disinformation strategies because they understand their local and global audiences, can tailor their tactics, and pull the right levers based on what works in local context. Equally, Russia and China have started to export digital authoritarianism to further censor information in developing countries, export propaganda, and clamp down on free press and free expression.

To that end, the US and European countries need to double down on existing commitments and invest in local and regional solutions. This can be done in multiple ways:

- First, greater financial investments should be made in institutions such as the US Agency for Global Media, which includes Radio Free Europe/Radio Liberty and Radio Free Asia, that exist to share credible information with local audiences that may have limited access to credible information, especially in rural markets, underdeveloped areas, or authoritarian regimes.

- Second, training of local and regional journalists by trusted partners should continue to be a priority. This is in addition to adding greater funding for new and independent media that is free from manipulation and corruption. Equally important is training citizens across demographics about digital literacy and civic skills so that they can be good stewards of information and not fall victim to Russian and Chinese COVID-19 disinformation and misinformation. These skills should be shared across towns, villages, tribes, religious and community centers, and schools.

- Third, investing in critical infrastructure, emerging technologies, and increased access to free and open internet to counter digital authoritarianism in emerging markets must be part of the solution to fight disinformation. After all, digital

authoritarianism and disinformation are two sides of the same coin; addressing both in emerging markets will be crucial to countering malign influence from Russia and China. In addition, investing in local tech entrepreneurship and youth programs will be critical to addressing these challenges. Young people are the future and can forge innovative private-public-civic partnerships to address these challenges.

- Fourth, and finally, the only way to assess the effectiveness of these investments is to measure the holistic impact of the efforts. This must be done at both the individual program level and the strategic level that is tied to the broader goal of countering Russian and Chinese disinformation.

Endnotes

1. Edward Lucas, Jake Morris, Corina Rebega, "Information Bedlam: Russian and Chinese Information Operations During COVID-19," Center for European Policy Analysis, March 15, 2021, https://cepa.org/information-bedlam-russian-and-chinese-information-operations-during-covid-19/

2. Ben Dubow, Edward Lucas, Jake Morris, "Jabbed in the Back: Mapping Russian and Chinese Information Operations During COVID-19," Center for European Policy Analysis, December 2, 2021, https://cepa.org/jabbed-in-the-back-mapping-russian-and-chinese-information-operations-during-covid-19/

3. Vivek H Murthy, "Confronting Health Misinformation: The U.S. Surgeon General's Advisory on Building a Healthy Information Environment," U.S. Public Health Service, 2021. https://www.hhs.gov/sites/default/files/surgeon-general-misinformation-advisory.pdf.

4. Joint Cybersecurity Authority, "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure," Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and the National Security Agency, January 11, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-011a

5. "GEC Special Report: August 2020 Pillars of Russia's Disinformation and Propaganda Ecosystem" U.S. Department of State, Global Engagement Center, August 2020, https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report/.

6. "Disarming Disinformation: Our Shared Responsibility," U.S. Department of State. February 3, 2022, https://www.state.gov/disarming-disinformation/

7. Joshua Machleder et. al, "Center of Excellence on Democracy, Human Rights, and Governance Disinformation Primer" United States Agency International Development, February 2021, https://pdf.usaid.gov/pdf_docs/PA00XFKF.pdf

8. "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government," The White House, April 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

9. Murphy Portman "Applaud Inclusion of Provision to Fight Global Propaganda and Disinformation in Senate Passage of U.S. Innovation and Competition Act," Rob Portman United States Senator for Ohio, June 8, 2021, https://www.portman.senate.gov/newsroom/press-releases/portman-murphy-applaud-inclusion-provision-fight-global-propaganda-and

10. Digital Citizenship and Media Literacy Act Bill (2019)

11. "Reps. Malinowski and Eschoo Reintroduce Bill to Hold Tech Platforms Accountable for Algorithmic Promotion of Extremism" Congressman Tom Malinowski, March 24, 2021, https://malinowski.house.gov/media/press-releases/reps-malinowski-and-eschoo-reintroduce-bill-hold-tech-platforms-accountable.

12. Shirin Ghaffary and Rebecca Heilweil. "A New Bill Would Hold Facebook Responsible for COVID-19 Vaccine Misinformation," Vox, July 22, 2021, https://www.vox.com/recode/2021/7/22/22588829/amy-klobuchar-health-misinformation-act-section-230-covid-19-facebook-twitter-youtube-social-media.

13. "Questions and Answers about the East Stratcom Task Force," European External Action Service, April 28, 2021, https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en.

14. " European Democracy Action Plan," European Commission , December 9, 2021, https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en.

15. "Code of Practice on Disinformation," Shaping Europe's digital future. European Commission, 2021, https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

16. "COVID-19 Disinformation Monitoring: Shaping Europe's digital future," European Commission, 2020, https://digital-strategy.ec.europa.eu/en/policies/covid-19-disinformation-monitoring.

17. "The Digital Services Act Package," Shaping Europe's digital future. European Commission, 2020, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

18. Kate Proctor, "UK Anti-Fake News Unit Dealing with up to 10 False Coronavirus Articles a Day," The Guardian, Guardian News and Media, March 29, 2020, https://www.theguardian.com/world/2020/mar/30/uk-anti-fake-news-unit-coronavirus.

19. Caroline Dinenage. "Minister Launches New Strategy to Fight Online Disinformation," Department for Digital, Culture, Media & Sport, July 14, 2021, https://www.gov.uk/government/news/minister-launches-new-strategy-to-fight-online-disinformation.

20. Emma Woollacott, "Sweden Launches Psychological Defense Agency to Counter Disinformation," Forbes, Forbes Magazine, January 6, 2022, https://www.forbes.com/sites/emmawoollacott/2022/01/05/sweden-launches-psychological-defense-agency-to-counter-disinformation/?sh=28a4738e4874

21. "Sweden Launches Psychological Defense Agency to Counter Influence Ops," Homeland Security Today, January 11, 2022, https://www.hstoday.us/subject-matter-areas/intelligence/sweden-launches-psychological-defense-agency-to-counter-influence-ops/

22. "French government pulls COVID-19 fake news website offline," RFI, May 6, 2020, https://www.rfi.fr/en/france/20200506-french-government-pulls-covid-19-fake-news-website-desinfox-offline-press-freedom

23. "Santé.fr," Santé.fr. https://www.sante.fr/

24. Théophile Lenoir, "The Noise Around Disinformation," Institut Montaigne, October 13, 2021, https://www.institutmontaigne.org/en/blog/noise-around-disinformation; Arthur P.B Laudrain, "France Doubles Down on Countering Foreign Interference Ahead of Key Elections," Lawfare, November 22, 2021, https://www.lawfareblog.com/france-doubles-down-countering-foreign-interference-ahead-key-elections-0

25. Kristina Wilfore. "The gendered disinformation playbook in Germany is a warning for Europe," Brookings, TechStream, October 29, 2021. https://www.brookings.edu/techstream/the-gendered-disinformation-playbook-in-germany-is-a-warning-for-europe/

26. Alexander Hardinghaus and Philipp Süss and Ramona Kimmich, "Germany's next steps in digitization: Finally, the new Interstate Treaty on Media has been ratified by all German federal states," ReedSmith, Technology Law Dispatch, November 3, 2020, https://www.technologylawdispatch.com/2020/11/regulatory/germanys-next-steps-in-digitization-finally-the-new-interstate-treaty-on-media-has-been-ratified-by-all-german-federal-states/; «Media regulator takes action against online media,» Sueddeutsche Zeitung, February 16, 2021, https://www.sueddeutsche.de/medien/kenfm-landesmedienanstalt-1.5208177.

27. Alessio Perrone, "Germany's Promising Plan to Bring Conspiracy Theorists Back From the Brink," Slate, October 18, 2021, https://slate.com/news-and-politics/2021/10/germany-conspiracy-theory-counseling-centers-covid-misinformation-zebra-veritas.html

28. Simon Ostrovsky, "Inside Estonia's approach in combating Russian disinformation" PBS, January 15, 2022, https://www.pbs.org/newshour/show/inside-estonias-approach-in-combating-russian-disinformation

29. Gil Skorwid. "A Job for Elves," AreWeEurope, June 9, 2021, https://www.areweeurope.com/stories/a-job-for-elves-gil-skorwid

30. "A Counter-Disinformation System that Works," Content Commons, February 20, 2020, https://commons.america.gov/article?id=44&site=content.america.gov

31. "Officials Outline United Nations Fight against Disinformation on Multiple Fronts as Fourth Committee Takes Up Questions Related to Information," Meetings Coverage and Press Releases-United Nations, October 15, 2021, https://www.un.org/press/en/2021/gaspd734.doc.htm

32. "Countering Misinformation about COVID-19: A Joint Campaign with the Government of the United Kingdom," World Health Organization, May 11, 2020, https://www.who.int/news-room/feature-stories/detail/countering-misinformation-about-covid-19.

33. "How to Report Misinformation Online," World Health Organization, 2022, https://www.who.int/campaigns/connecting-the-world-to-combat-coronavirus/how-to-report-misinformation-online.

34. "Fighting Misinformation in the Time of Covid-19, One Click at a Time," World Health Organization. World Health Organization, April 27, 2021, https://www.who.int/news-room/feature-stories/detail/fighting-misinformation-in-the-time-of-covid-19-one-click-at-a-time.

35. "Coronavirus Disease (COVID-19) Advice for the Public: Mythbusters," World Health Organization, January 19, 2022, https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters.

36. Giovanna De Maio, "Nato's Response to COVID-19: Lessons for Resilience and Readiness," Brookings, October 2020, https://www.brookings.edu/wp-content/uploads/2020/10/FP_20201028_nato_covid_demaio-1.pdf

37. "NATO-Russia: Setting the Record Straight," North Atlantic Treaty Organization, January 27, 2022, https://www.nato.int/cps/en/natohq/115204.htm

38. "Cyber defence," North Atlantic Treaty Organization, July 02, 2021, https://www.nato.int/cps/en/natohq/topics_78170.htm

39. "G7 Rapid Response Mechanism," Government of Canada, January 30, 2019, https://www.canada.ca/en/democratic-institutions/news/2019/01/g7-rapid-response-mechanism.html/

40. Twitter Inc. "Coronavirus: Staying Safe and Informed on Twitter," Twitter, April 3, 2020, https://blog.twitter.com/en_us/topics/company/2020/covid-19.

41. Del Harvey, "Helping you find reliable public health information on Twitter," Twitter, May 10, 2019, https://blog.twitter.com/en_us/topics/company/2019/helping-you-find-reliable-public-health-information-on-twitter

42. "COVID-19 misleading information policy," Twitter, December 2021, https://help.twitter.com/en/rules-and-policies/medical-misinformation-policy

43. Katie Paul, "Twitter takes down Beijing-backed influence operation pushing coronavirus messages," Reuters, June 11, 2020, https://www.reuters.com/article/us-china-twitter-disinformation/twitter-takes-down-beijing-backed-influence-operation-pushing-coronavirus-messages-idUSKBN23I3A3

44. Reuters Staff, "Facebook to notify users who have engaged with harmful COVID-19 posts," Reuters, April 16, 2020, https://www.reuters.com/article/us-health-coronavirus-facebook/facebook-to-notify-users-who-have-engaged-with-harmful-covid-19-posts-idUSKCN21Y1YB

45. Ibid

46. Hayden Field and Issue Lapowsky, "Inside WhatsApp, Instagram and Tik Tok, a race to build COVID-19 tools," Protocol, March 28, 2020, https://www.protocol.com/coronavirus-instagram-tiktok-whatsapp-response

47. Nathaniel Gleicher, "Removing Coordinated Inauthentic Behavior from France and Russia," Meta, December 15, 2020, https://about.fb.com/news/2020/12/removing-coordinated-inauthentic-behavior-france-russia/

48. Shannon Bond, "Facebook takes down China-based network spreading false COVID-19 claims," National Public Radio, December 1, 2021, https://www.npr.org/2021/12/01/1060645940/facebook-takes-down-china-based-fake-covid-claims

49. The Youtube Team, "Managing harmful vaccine content on YouTube," YouTube, September 29, 2021, https://blog.youtube/news-and-events/managing-harmful-vaccine-content-youtube/

50. Jennifer Elias, "YouTube to add labels to some health videos amid misinformation backlash," CNBC, July 19, 2021, https://www.cnbc.com/2021/07/19/youtube-labeling-some-health-videos-amid-misinformation-backlash.html

51. "YouTube purges anti-vaccine misinformation and provokes ire of Russia," Sky News, September 29, 2021, https://news.sky.com/story/youtube-purges-anti-vaccine-misinformation-and-provokes-ire-of-russia-12421402

52. Brady Zadrozny, "On Tik Tok, audio gives new virality to misinformation.," ABC News, July 13, 2021, https://www.nbcnews.com/tech/tech-news/tiktok-audio-gives-new-virality-misinformation-rcna1393

53. "COVID-19," Tik Tok, 2022, https://www.tiktok.com/safety/en-us/covid-19/

54. "#distancedance," Tik Tok, March 2020, https://www.tiktok.com/tag/distancedance

55. "Reports on July and August Actions – Fighting COVID-19 Disinformation Monitoring Programme," European Commission, October 1, 2021, https://digital-strategy.ec.europa.eu/en/library/reports-july-and-august-actions-fighting-covid-19-disinformation-monitoring-programme

56. "Defending Democracy Program," Microsoft, 2022, https://news.microsoft.com/on-the-issues/topic/defending-democracy-program/

57. Tom Burt, "New Steps to Combat Disinformation," Microsoft, September 1, 2020, https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator/

58. Katya Vogt, Tara Susman-Peña, Michael Mirny "Learn to Discern (L2D) - Media Literacy Training," The International Research & Exchanges Board, March 2019, https://www.irex.org/project/learn-discern-l2d-media-literacy-training.

59. Global Engagement Center, "GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem, " United States Department of State, August 2020, https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdfhttps://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

60. "EEAS Special Report Update: Short Assessment of Narrative and Disinformation around the COVID-19 Pandemic," EUvDisinfo, April 28, 2021, https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-december-2020-april-2021/

61. "The American Public Views the Spread of misinformation as a Major Problem," The Associated Press, NORC Center for Public Affairs Research and the Pearson Institute. October 8, 2021, https://apnorc.org/projects/the-american-public-views-the-spread-of-misinformation-as-a-major-problem/https://apnorc.org/projects/the-american-public-views-the-spread-of-misinformation-as-a-major-problem/

62. "Fact Sheet: Announcing the Presidential Initiative for Democratic Renewal," The White House2December 9, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/09/ fact-sheet-announcing-the-presidential-initiative-for-democratic-renewal/

63. Ibid.

64. "Learn to Discern (L2D)-Media Literacy Training," International Research and Exchanges Board, Accessed February 7, 2022, https://www.irex.org/project/learn-discern-l2d-media-literacy-training

65. "Bad News," GetBadNews, Accessed February 7, 2022, getbadnews.com/#intro

66. "The Safe Framework: Tailoring a Proportionate Approach to Assessing Digital Trust and Safety," Digital Trust and Safety Partnership, December 2021, https://dtspartnership.org/#:~:text=What%20is%20the%20Digital%20Trust,safer%20and%20more%20trustworthy%20internet.

67. Christina Farr and Salvador Rodriguez, "Facebook, Amazon, Google and more met with WHO to figure out how to stop coronavirus misinformation," CNBC, February 14, 2020, https://www.cnbc.com/2020/02/14/facebook-google-amazon-met-with-who-to-talk-coronavirus-misinformation.htmlhttps://www.cnbc.com/2020/02/14/facebook-google-amazon-met-with-who-to-talk-coronavirus-misinformation.html

68. "Design 4 Democracy Coalition," Design for Democracy Coalition, Accessed February 7, 2022, https://d4dcoalition.org/

69. Alina Polyakova and Daniel Fried, "Democratic Offense Against Disinformation," Center for European Policy Analysis and The Digital Forensic Research Lab at the Atlantic Council, December 2, 2020, https://cepa.org/wp-content/uploads/2020/12/CEPA-Democratic-Offense-Disinformation-11.30.2020.pdfhttps://cepa.org/wp-content/uploads/2020/12/CEPA-Democratic-Offense-Disinformation-11.30.2020.pdf

70. Task force on US Strategy To Support Democracy and Counter Authoritarianism, "Reversing the Tide: Strategies and Recommendations," Freedom House, Center for Strategic International Studies, and the McCain Institute, April 2021, https://freedomhouse.org/democracy-task-force/special-report/2021/reversing-the-tide/strategies-and-recommendations#countering-disinformationhttps://freedomhouse.org/democracy-task-force/special-report/2021/reversing-the-tide/strategies-and-recommendations#countering-disinformation

71. Sandra Kalniete, European Parliament. Draft Report on foreign interference in all democratic processes in the European Union, including disinformation. Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation, October 18, 2021, https://www.europarl.europa.eu/doceo/document/INGE-PR-695147_EN.pdf

72. John Boyle, Thomas Brassell, and James Dayton, "As cases increase, American trust in COVID-19 information from federal, state, and local governments continues to decline," ICF International, July 20, 2020, https://www.icf.com/insights/health/covid-19-survey-american-trust-government-june