MITIGATING THE SPREAD OF DISINFORMATION

"Man's capacity for justice makes democracy possible; but man's inclination to injustice makes democracy necessary."

Reinhold Niebuhr
(The Children of Light and the Children of Darkness, August 1944)

"No one in my administration was surprised that Russia was attempting to meddle in our election. … What does still nag at me, though … [w]as my failure to fully appreciate at the time just how susceptible we had become to lies and conspiracy theories."

Barack Obama
(Stanford University, April 21, 2022)

Much has been said in recent days about the disinformation campaigns unleashed by Russia in the lead-up to, and continuing during, the invasion of Ukraine. We should be under no illusion that Russian disinformation around the war in Ukraine is a limited tactical effort. In fact, it is part of a far broader pattern that goes well beyond the election interference we are now all too aware of and whose antecedents stretch back decades as Soviet, then Russian, doctrine embraced so-called "active measures" or "influence operations" as a means of achieving geopolitical goals well beyond their economic and conventional military capabilities.

Russia is not the only malign actor deploying weaponized disinformation. Autocrats in addition to Vladmir Putin have been emboldened by the failure of the West to do more than call out violations of human rights, oppressions of minority populations and the trampling of the rule of law. China, Iran and North Korea each also have their own influence and disinformation operations. And, of course, there is an entire ecosystem of extremist groups (including what in the UK are referred to as "hateful extremists" but also violent extremists) dedicated to spreading disinformation, conspiracy theories and hate.

In a November 2020 interview with then President Obama by Atlantic editor-in-chief, Jeffrey Goldberg, Obama identified disinformation as the "single biggest threat to our democracy." In a subsequent interview with Goldberg at an April 6, 2022 conference (Disinformation and the Erosion of Democracy) hosted by The Atlantic and the University of Chicago, Obama spoke at length about disinformation. Disinformation and the challenges to democracy in the digital age have become a key theme for Obama and the Obama Foundation. These were the central topics of his keynote address at Stanford University this past week.

When asked how one breaks through authoritarian regimes or populations controlled by authoritarian leaders to give the public an understanding of reality, President Obama noted that America has its own information disfunction. In our society, he noted, where information is not *per se* filtered, roughly 40% of Americans believe the 2020 election was rigged and President Biden was fraudulently elected (see my prior briefing note, available here), and between 30-35% of Americans have chosen not to be vaccinated.

The Russian invasion has caused many to ask why the West only now understands what Putin intended all along. Similarly, the invasion as well as the disinformation tactics (admittedly only part of the assaults that may well constitute war crimes and crimes against humanity, and possibly genocide) highlight the extent to which the West failed to appreciate the vulnerability of democratic societies to autocrats. While the signs, beginning really around 2014 were unmistakeable, it is only recently that the issue of disinformation and the relationship between disinformation and the vulnerability of democracies has entered the mainstream.

While malign actors – state and nonstate – have targeted the full spectrum of civil society, a significant contributor to the attention paid to disinformation undoubtedly has been the pandemic. As many have noted, the "infodemics" surrounding the pandemic have highlighted the role of extremist groups, populist national political groups and authoritarian groups, as well as the exploitation of "us versus them" narratives (*see, e.g.*, ISD Global and CCE Study (March 2021)). Ultimately, disinformation fed distrust of COVID-19 vaccinations, which had fatal consequences.

Not surprisingly, the European External Action Service, as part of the EU Action Plan against disinformation, identified Russian disinformation as a grave threat to the European Union. This is noteworthy because this morning, the European Parliament, the French (as president of the Council of the European Union) and the European Commission reached agreement on the text of the Digital Services Act ("DSA"). *See* below.

Disinformation

By way of background, it is important to note that disinformation and misinformation are two different concepts.

- Misinformation is information that is false, misleading or inaccurate and disseminated without an intention to deceive. The disseminator of misinformation believes the information to be true.
- Disinformation is false information that is deliberately created or disseminated with the intention of causing harm. The creator or disseminator of disinformation knows the information is false and can be motivated by any number of factors: political, geopolitical, financial, social or psychological. Misinformation can be transformed into disinformation when the disseminator knows that the misinformation is false and further disseminates the information to cause harm.

Both misinformation and disinformation can be distinguished from propaganda, being the deliberate spread of information to influence an attitude, encourage a response or provoke a desired feeling within the context of ideology or political rhetoric. While often associated with Soviet or Nazi efforts (the concept dating back to Ancient Greece and the Roman Empire, and the term itself dating back to the 1620s), propaganda, may, but need not, be based on a falsity; it may present facts selectively (half-truths) and it may manipulate descriptions to enhance the emotional appeal. Propaganda typically has a specified goal.

Historically, disinformation campaigns undertaken by malign state actors, principally the Soviet Union, were referred to as "active measures" or "influence operations" (see Active Measures and Disinformation (1985) and Active and Sharp Measures (2021)), or simply "covert" propaganda. A classic example of covert propaganda before the digital age was the KGB's disinformation campaign that blamed HIV/AIDS on experiments supposedly undertaken by the US military with biological weapons. As noted in an article by Mark

Kramer (2020) in the MIT Press, the KGB amplified existing conspiracy theories circulating in the United States, added a new element of specificity and spread the disinformation internationally. (See also Wilson Center and CNN Business interview.)

Scholars believe that following the collapse of the Soviet Union, Russian active measures long favored by the KGB (including through Service A of its First Main Directorate, established in the 1950s, and facilitated though Warsaw Pact allies) were curtailed. However, under Putin, information warfare was resurrected as a hybrid effort with military aims as well as political aims being undertaken by the security services (the FSB and the SVR, successors to the KGB) and the GRU (foreign military intelligence). (See Active and Sharp Measures.) What historically required dissemination via traditional media of radio and television, often needing agents on the ground susceptible to arrest, could now be weaponized via social media (from the comfort of an office in Moscow or Saint Petersburg).

The modern version of these efforts were characterized by Christopher Paul and Miriam Matthews of the RAND Corporation (2016) as following the "firehose of falsehood" model of propaganda - that is, multi-channel, rapid, continuous and repetitive, lacking any commitment to consistency and shameless in its willingness to disseminate partial truths or outright fictions. The are set out in the declassified version of the US intelligence community's assessment of Russian activities and intentions in the 201+6 election.

It is important to note that while external malign state and nonstate actors play key roles as sources of disinformation, in recent years domestic actors also have played increasingly prominent roles in the disinformation supply chain, supporting external narratives. Disinformation becomes far more effective when it is amplified; it can be amplified by human users or digitally, including via mainstream social media channels as well as through online forums (such as Reddit, Discord and 4chan) and encrypted messaging apps. Automated social media accounts (bots) and algorithmic amplification have enabled malign actors to weaponize disinformation, in the sense of enabling these actors to intentionally mislead and manipulate at scale, in an anonymous, inexpensive and extremely efficient manner, with the goal of eroding trust and confidence in democratic processes and institutions.

The predicate for today's assaults on democracy is the pervasive presence of the digital world in every aspect of our lives. Disinformation is the ideal tool of authoritarian regimes that are able to harness digital communications channels and other technologies to repress their domestic populations and undermine the democracies they confront beyond their borders.

Democracies have failed to stay ahead of the threats. (*See, e.g.*, The Digital Technology Agenda at the Summit for Democracy (March 2021).) The threat landscape is expected to get worse given the advances in artificial intelligence that will enable malign actors to deploy with ease deep fake videos and other fake multimedia content. The challenge is that the open source nature of the technology (including Generative Adversarial Networks) will make these tools readily accessible. (*See, e.g.*, Preparing for the Age of Deepfakes and Disinformation (November 2020).)

Asymmetric Warfare

The Russian invasion cast onto the world stage what heretofore had been the subject of significant concern only among small groups – students of authoritarianism (speaking as journalists, authors and academics), NGOs that had been tracking extremism in the post 9/11 world as jihadi extremist groups launched what ultimately became sophisticated online recruitment campaigns, the intelligence community and certain elements of civil society that had either been monitoring, or had been on the receiving end of, the weaponization of disinformation and hate.

In 2017, the US Helsinki Commission held a hearing on Russian disinformation across the 57-nation members of the Organization on Security and Cooperation in Europe. Testimony largely coalesced around the following themes:

- disinformation is at the heart of a war being waged by Russia against the West, and the United States in particular;
- disinformation does not create societal traits, but rather exploits and distorts existing grievances and divisions to sow discord, fear and paralysis that ultimately undermines democratic institutions; and
- disinformation should be seen as part of a broader coordinated effort to disrupt liberal democracies by whatever means are readily available.

Incidentally, around the same time as this hearing, some commentators were noting that it was short-sighted to view Russian disinformation solely in terms of sowing chaos in the West. In the broader view, disinformation should be seen as a means to advance other strategic goals, including restoring Russia to great power status (by diminishing the global influence of the United States and disrupting the Atlantic alliance); preserving Russia's sphere of influence; protecting the Putin regime (by eroding confidence in democratic processes to discourage Russians from aspiring to democracy); and enhancing the effectiveness of the Russian military. This latter goal highlights the blurring in Russian strategic thinking of the lines between war and peace. In effect, Russia views itself as being engaged in continuous information warfare with the West. (*See, e.g.* Why does Russia Use Disinformation? and Countering Russian Information Operations in the Age of Social Media.) We are now seeing this all play out in Ukraine.

Elections provided fertile ground for disinformation campaigns – some believe Ukraine's election in 2004 and Georgia's election in 2014, as well as campaigns in the Baltic States, and elections in western Europe and the Brexit referendum all were targets of Russian active measures, before they were deployed in the 2016 US elections. However, as Clint Watts, an expert on counter-terrorism, social media influence and Russian disinformation, noted in 2017 testimony before the Senate Select Committee on Intelligence at a hearing on Russian Active Measures and Influence Campaigns, winning elections is not the goal of active measures, rather the goal is to topple democracies through five complementary sub-objectives:

- undermining confidence in democratic governance;
- fomenting and exacerbating divisive political fissures;
- eroding trust between citizens and elected officials and their institutions;
- popularizing Russian policy agendas within target populations; and
- creating general distrust or confusion over information sources by blurring the lines between fact and fiction.

Anne Applebaum sets out two examples that should have tipped us all off to the involvement of Russia in the 2016 election. Trump campaign slogans (Hillary would start WWIII; Obama had created ISIS) eerily echoed Russian media stories at the time. The leak of the DNC emails was part of the classic Russian playbook – dissemination of nothing of substance, whose significance was blown completely out of proportion simply because it had been secret.

Weaponization of Hate

While the leaders of the Soviet Union/Russia, like their brethren in other autocracies, have long deployed disinformation as a tactic, what is new is the way we communicate. The amplification of hate by social media platforms and the fact that communication has become a single market are recent phenomena. In short, as Applebaum noted, the dark side of globalization is that it has enabled networks of fake or semi-fake accounts, bot nets and trolls to create the impression across the West that disinformation is fact/news. The same technology that allows countless businesses to target particular audiences can easily be deployed to sow distrust in a highly inexpensive and highly effective manner.

Another key Russian tactic of stirring up fear found its mark in America's culture wars. Russian disinformation – in the guise of providing explanations for mysterious facts – will tie moral threats posed by liberal policies (*e.g.*, on immigration) to existing government policies, heightening the sense of distrust in government and setting the stage for efforts to quash institutions. An earlier incarnation of this was the "birther" conspiracy, an explanation of how a Black man with a strange name could have risen to the presidency. And recall the effectiveness of the tactic – if the President were illegitimate (and up to 30% of Americans at one time or another believed he was), so too were Congress, the courts and the other institutions of government.

Where Do We Go from Here?

Addressing disinformation requires an understanding of the threat, which in turns involves assessing a mix of technology and psychology. Experts note, for example, that traditional efforts to counter propaganda may be of limited use, if not counterproductive. (*See, e.g.*, Paul/Matthews.) Disinformation moves at lightning speed; if too much time has elapsed, people will have greater difficulty separating fact from fiction. Seeking to refute disinformation (for example, via fact-checking operations) may serve to reinforce the disinformation and, by definition, is reactive. Other psychological factors drive vulnerabilities to disinformation, in that disinformation plays to emotions and biases, simplifies difficult topics, allows recipients to feel as if they are exposing truths and offers validation of identity (playing to the need to belong). (*See* Weapons of Mass Distraction.)

Focusing only on trying to refute/fact-check allows purveyors of disinformation to drive the narrative and fails to account for the unprecedented global trust gap. (*See* Nina Jankowicz (March 2017).)

Building resilience

Writing for the majority in *United States v. Alvarez*, Justice Kennedy wrote that "[t]he remedy for speech that is false is speech that is true. This is the ordinary course in a free society. The response to the unreasoned is the rational; to the uninformed, the enlightened; to the straight-out lie, the simple truth." There is a growing consensus as to the importance of increasing digital awareness and digital citizenship. It is an obvious place to start, and the literature provides an additional rationale: a study that focused on how information travels - *broadly* or *deeply* - found that fact and fake news appear to travel equally broadly and equally deeply, but fake news spreads more *easily*, because it is more infectious. Thus, efforts aimed at lessening the infectiousness of fake news – encouraging users to think before sharing or imposing delays are worth considering, as are programs aimed at providing consumers of information with the tools to better navigate the disinformation space.

Awareness programs need not only target younger consumers of digital information. Just as there are initiatives to create a more digitally resilient workforces (*see, e.g.*, Digital US), so too are there campaigns to build community resilience to disinformation through adult education programs (*see, e.g.*, IREX's Learn to Discern program and Nina Jankowicz (September 2017)). Here businesses have an important role to play.

Addressing the role of social medial platforms

There is near universal agreement that efforts to address threats posed by disinformation must include the social media platforms. While the tactics that divide society – racism, sexism, ethno-nationalism and other features of the culture wars – are by no means the product of the digital revolution and social media platforms, the heart of the platform product design serves to amplify divisive content. Again, to paraphrase Obama, the issue is not so much what people post, but rather what the platforms promote. In the words of journalist and Nobel laureate Maria Ressa (delivered at the April 6th conference), social media allows "lies laced with hate" to "spread faster and further than facts."

The problem, Ressa noted, is that, while the focus has been on content moderation, concerns over content moderation have allowed the upstream elements, namely the algorithms that amplify hate speech and the vast collection/repackaging for profit of personal data that allows the speech to be disseminated in a micro-targeted fashion, to remain largely beyond scrutiny.

While platforms continue to tout self-regulation, there is also a growing consensus on the need for some form of regulation. The key, as many others have noted as well, is to understand how the algorithms work. Focusing regulatory solutions on content moderation is misplaced – the focus should be on opening up the algorithms to scrutiny by regulators or researchers. There are countless examples of sectors that are subject to regulation for reasons of public safety – and for which regulators have access to what arguably is as proprietary as the algorithms. These sectors not only have not suffered, but have thrived. The proposed Platform Accountability and Transparency Act, introduced by Senators Coons, Portman and Klobuchar, would mandate that the platforms provide data to independent researchers, or lose the immunity provided by Section 230 of the Communications Decency Act.

As was the case with the adoption of the General Data Protection Regulation (GDPR), the Europeans again have taken the lead on legislation that will have extra-territorial effect on the global digital world. The DSA (political agreement on which, as noted above, was announced this morning) and the Digital Markets Act ("DMA") (political agreement on which was reached on March 25) form part of a single set of new rules intended to create a safer digital space and establish a level playing field for digital services. Among other things, the DSA provides for more oversight over online platforms and seeks to mitigate systemic risks such as manipulation and disinformation. One critical feature is the transparency regime for algorithms and access by researchers to key platform data, applicable to "very large online platforms." The final text of the DSA will not be available for a few weeks (the December 2020 proposal is available here, and proposed amendments by the European Parliament are available here). The DSA will have extra-territorial effect to the extent that a platform targets EU consumers.

Recreating communities of trust

Another element is to focus on recreating the communities of trust, which goes beyond understanding the algorithms to the broader ecosystem that underpins fact and truth – academia, journalism, government, all of which, as Anne Applebaum has noted, have been disrupted. If people have issues with elites, journalists and/or government, then truth and lies become indistinguishable.

In 1958 (according to the Pew Research Center), 73% of Americans trusted government to do the right thing most of the time or almost always. Today that figure is 24% (36% among Democrats and Democratic-leaning independents, and 9% among Republicans and Republican-leaning independents; admittedly trust tends to be higher among members of the party that controls the presidency). Trust in media has plummeted, with 68% of Americans saying that made-up news and information has sapped their confidence in government and 54% saying that the state of media has sapped their confidence in each other (Pew Video (January 2022)). And with diminished trust, American have turned to digital services. According to a January 2021 Pew Research study, 86% of Americans get news from digital devices often or sometimes (52% preferring digital platforms).

The current state of journalism has two consequence – one is that local journalism is larlgely an anachronism. While the center of policy debates over issues that have significant impact on Americans – ranging from voting rights, to reproductive rights, education and redistricting – is at the state level, the number of reporters covering state capitols has decreased (*see, e.g.*, Pew Research Center study (April 2022)) and local print newspapers largely have disappeared (according to statistics published by the Washington Post, around 2,200 local print newspapers closed between 2005-2020; the total number of newspaper journalists decreased by more than 50% between 2008-2020; out of the 3,000+ counties in the United States, half had just one local print newspaper and over 200 counties had no local newspaper).

The other consequence is that the traditional function of the editor has disappeared. The internet has democratized communications, but in the process, it has allowed individuals to amplify messages via social media without the intervention of any form of editorial oversight, and in fact without any oversight. It is critical that efforts to rebuild local news organizations can be funded and otherwise supported.

It is also important to recognize the pliability of opinions. Sarah Longwell, Executive Director of Republicans for the Rule of Law and publisher of The Bulwark, in a recent article in The Atlantic (April 2022), highlights how conspiracy theories can find purchase, in this case the "big lie" embraced by perhaps one-third of Americans (including close to 70% of Republicans). She notes that, "For many of Trump's voters, the belief that the election was stolen is not a fully formed thought. It's more of an attitude, or a tribal pose. They know something nefarious occurred but can't easily explain how or why. What's more, they're mystified and sometimes angry that other people don't feel the same." "[S]omething does not have to make sense for voters to believe it is true."

The post-WWII acceptance by politicians of all stripes of process twined with a healthy debate on policies, based on shared space and a sufficient consensus, no longer exists. Obama cites a study of Fox news watchers/hard core conservatives who were paid to watch CNN for a period of time; even after a short period of time, people's views on significant issues had changed by 5-8-10 points (*see* The Guardian article (April 2022)).

Concluding Thoughts

As we emerge from an unprecedented public health crisis and continue to face challenges ranging from emboldened autocrats to the existential effects of climate change, unprecedented polarization and, in some cases, risks of political sectarianism, we cannot lose sight of the role that disinformation plays in creating, maintaining and exacerbating the divisions that undermine democracy. It was in a bygone era that the world wide web was extolled for its unique positive potential in opening up the world – from communications to education to cultural exchange, the means to build a global community. Along the way, malign actors who viewed the benefits with disdain discovered they could use the internet to undermine its very benefits. In fact, malign actors were among the early users of the internet (*see* Online Extremism). The spread of disinformation by malign actors, amplified in ways unimaginable only ten years ago, is now a mainstream topic. It behoves us first to understand the extent of the threat and then to support efforts, large and small, to mitigate the threat.

* * * *

Mark S. Bergman
7Pillars Global Insights, LLC
Washington, D.C.
April 23, 2022