Statement of Glenn S. Gerstell[*]

Before the Subcommittee on Cyber, Innovative Technologies, and Information Systems of the U.S. House of Representatives Committee on Armed Services

Hearing on Technology and Information Warfare: The Competition for Influence and the Department of Defense

April 30, 2021

A thoughtful book about the digital age observed that as people spend more and more time in cyberspace, the growing power of the internet "will make everything different: power shifting away from the center toward individuals and small organizations, more fluidity and continuous change, increasingly irrelevant national boundaries." The internet will give individuals "the ability to be heard across the world…along with the ability to spread lies worldwide…and will foster decentralization…undermining central authorities whether they are good or bad."

While we would recognize that as a description of our cyber world today, these prescient statements appeared 24 years ago, in Esther Dyson's *Release 2.0* – written in 1997, before the invention of Facebook, YouTube or the iPhone.

I mention this quotation because we need some perspective or sense of distance to appreciate the ramifications of the digital revolution, or the "Fourth Industrial Revolution." We tend to view both the exceptional benefits of technology and the negative consequences in isolation, looking at each new function and drawback as a separate, unrelated event, marveling at how we can now control our garage doors from halfway around the world, or worrying about cyber ransomware attacks on hospitals. But in this onrush of both innovation and mischief, we do not fully appreciate the fundamental, novel and transformational changes that we are in the midst of – and these changes have national security implications.

Technology has Yielded New Vulnerabilities Threatening our National Security

There are three related implications of these technological changes that our nation – and in particular this Subcommittee – must consider. First, our overall domestic wellbeing is, for the first time since America became a global power, directly threatened by what happens beyond our shores. Second, our wellbeing, in other words, our national security, is now partly the responsibility of the private sector, not just government. And the third point, which I will concentrate on today, is that the cyber-enabled spread of disinformation on the private sector's social media platforms is altering our political landscape, threatening democracies and global coordination.

[*] Glenn S. Gerstell served from 2015 to 2020 as the General Counsel of the National Security Agency and is currently a non-resident Senior Adviser at the Center for Strategic and International Studies. Additional background at https://glenngerstell.com.

Let's take the first and most obvious of these changes – the risks to our national security posed by other countries. Historically, when we think about this kind of vulnerability, we have thought of it as a threat posed by other nations' weapons; we rightly spend a great deal of time and money deterring or defending against those dangers. For over two centuries America has responded to foreign threats by dealing with them where they were located, in other words, overseas -- not allowing them (with the sole exception of the 9/11 attacks) to manifest themselves on our domestic soil. But as we've seen recently – due to technology – a virus that can be propelled around the world, and cyber mischief that is equally oblivious to sovereign boundaries, can have a devastating effect on our personal and commercial lives. While we must of course remain vigilant about the risk of another nation's weapons injuring us on our soil, we are far more likely to be harmed by other technology-propelled dangers emanating beyond our borders.

Or to put it in a more serious way, due to technology, our overall national wellbeing – our national security – is for the first time challenged by, and vulnerable to, other countries in ways that we will have difficulty managing, since these other threats are not deterred or blocked by our superior military strength.

These new vulnerabilities do not reside in weapons systems, but instead pervade our private sector. With responsibilities for cyber-safeguarding its vast troves of data about our personal and commercial lives and for stemming the tide of disinformation on the social media we all rely on for our news, the private sector clearly bears critical national security burdens. We rely on the private sector to a degree unthinkable just a decade or two ago: even at its heyday, a problem at General Motors wouldn't have affected our national wellbeing, but today, a mishap at Google or Facebook or a disruption at Amazon or Microsoft (together responsible for almost half of the nation's cloud computing capacity) might well cause deep disruptions to our society. In short, as the recent *Final Report* of the National Security Commission on Artificial Intelligence (NSCAI) succinctly stated: "Digital dependence in all walks of life is transforming personal and commercial vulnerabilities into potential national security weaknesses."

We focus less on these vulnerabilities, for many reasons. First, we don't typically think of the private sector as responsible for national security. It used to be clear that only government was responsible for national security, or the "common defense" as the American Constitution calls it, and our private sector was largely free to pursue its business goals, and the lines between the two were pretty clearly delineated. But the digital revolution has shifted those lines, and in many ways, for the first time in our nation's history, our national security increasingly rests not with the federal government but instead with a private sector that conducts our digital lives. Second, even when there are problems with private sector technology, we typically view them as incidents confined to one company, not signs of systemic risk to our country. Finally, and more significantly, the enormity of the ongoing shift of responsibilities to the private sector is difficult to embrace.

Online Disinformation is the Most Pernicious of those Vulnerabilities

Some of those technological mishaps could simply be technical failures to provide service, but in the area of information technology, problems affecting the substance of communications can be equally consequential. And that takes us to the third transformational consequence: the advent of disinformation on domestic social media platforms. Perhaps the most pernicious aspect of the digital revolution, disinformation threatens our very democracy. By disinformation, I am referring to the deliberate (or at least reckless) creation or dissemination of knowingly false (or at least baseless) information, with an intention to mislead the reader or viewer; the goal might be a specific effect or simply a more diffuse confusion or chaos. While the line might be hard to draw, it's clearly more than a spoof or simply erroneous information.

Esther Dyson's prescient vision has indeed come to pass. The fact that the internet gives everyone a potentially equal megaphone – whether you are the *Washington Post* or a white supremacist blogger – means that the lines between establishment news sources and unreliable ones are blurred. So with no curated and vetted sources of information, without elites more or less shaping the flow of the news, anything goes – and it does. Human nature being what it is, we are drawn to the more lurid, improbable or conspiratorial, at least to explain what might not be apparent or understandable. So rather than being an unalloyed good for democracies, it turns out that chat and other online platforms are a fertile ground for populism, divisiveness and political disintegration. Admittedly, it's not wholly negative and there are many examples where the ability of individuals to obtain and disseminate information has worked against authoritarian regimes; but my point is simply that – absent safeguards – the technology seems to easily lend itself to bad outcomes.

Over the past few months, as we've seen in detailed reports from many organizations, including the Alliance for Securing Democracy, Avaaz, Graphika and The New York Times, those platforms have been awash in falsehoods on political topics ranging from election fraud, to the Capitol insurrection, to climate change and to Antifa protestors. When you stop to think about it, it's quite extraordinary that we are now more worried about the private sector, which owns Facebook, Twitter, YouTube, Instagram and the other popular platforms, shaping and influencing what we think. America was founded in part on concerns that the government might control what we think and believe, and while that remains an enduring concern, the reality is that our domestic wellbeing is threatened far more by private sector social media polluted by falsehoods.

It can't be healthy for a democracy when almost half the population wasn't sure if our president was duly elected, and more shockingly, that only four in ten Americans thought the recent election was fair and accurate. At least in the case of elections and political speech, disinformation has a corrosive effect on democracy, leading to mistrust of institutions, cynicism about our leaders and skepticism about our ability to solve social problems, and ultimately raising the specter of authoritarianism as a reaction to that corrosion. Indeed, one of the key trends identified in the just-released *Global Trends 2040* report from the Office of the Director of National Intelligence was that online technologies would continue to foment and channel public discontent – yielding a deeply disturbing picture "with a mix of implications for social cohesion."

But disinformation is affecting not merely our political institutions. When three out of four Americans get some or all of their news from social media platforms, it is clear that the risk of deliberately incorrect online information is national in scope, and could get worse. A recent Gallup poll revealed that, due to erroneous fears spread on social media about the safety of COVID vaccines, roughly a third of the country has doubts about getting a shot, and many others refuse to follow the advice of doctors and scientists and wear face masks, choosing instead to believe false online claims that masks are useless. So even a seemingly non-partisan sphere such as public health can be politicized and damaged by cyber-disinformation.

Beyond threats to the fundamentals of our democracy and our public health, disinformation could affect our military in concerning ways. At the most general level, the cynicism about our institutions and mistrust of political leaders endangers the national consensus that we must devote sufficient resources to our armed services. It stands to reason that a lack of trust in our military might well threaten public support for Congressional appropriations for weapons systems or veterans affairs and more directly, recruiting for our all-volunteer military forces. And speaking of personnel, it isn't much of a stretch to attribute, at least to some degree, extremism in the military to the effects of malicious lies spread online. Although it is beyond my scope today, information warfare in armed conflict is obviously a threat to service personnel morale, command and control of forces, and relations with local populations in the area of operations. Indeed, recent press reports indicate that senior military leaders are seeking closer cooperation with the US Intelligence Community to help counter malign influence campaigns of Russia and China.

These concerns about disinformation are not just idle speculation. Just a few months ago, the Reagan Institute survey revealed that, after several politically turbulent years, citizens' trust and confidence in our military dropped to just 56%, down from 70% as recently as 2018. Even more shocking was the finding that levels of trust in institutions from law enforcement to public schools to the news media and the presidency and Congress were all below 50% of the population. How much of that is attributable to online disinformation? There's no way of knowing, but common sense tells us that the manifestly corrosive effect of such disinformation must be a key element in this societal disintegration.

Broader threats to our military arise from a world situation in which our foreign adversaries use disinformation as a tool of their statecraft. Lies fomented by our overseas foes about foreign affairs and our vital interests abroad could similarly make cooperation with our allies and friends more difficult. For example, China's concerted online campaign to deflect investigations into the cause of the COVID19 outbreak, to paint themselves as successful in curtailing the virus when Western democracies have been foundering, and to deny their militarization of the South China Sea, all complicate if not undermine our foreign relations, and heighten the chance for conflict. The combination of disinformation and the difficulty of promoting a concerted establishment message have all hampered efforts at, or at least made it more difficult to achieve, global cooperation on a variety of matters. All of these geopolitical consequences, with their myriad and complex effects, are the product of a technology in which electrons are ignorant of sovereign boundaries.

Foreign-Generated Disinformation is Likely to Get Worse

Recent events have caused us to focus mostly on domestic disinformation in somewhat contained (albeit critical) channels, and on the relatively limited efforts of our foreign adversaries to undermine our democracy and promote their governing systems over our own. For both technical and political reasons, however, the effects of cyber-propelled disinformation are likely to get much worse; we would have difficulty in fending off weaponized disinformation coming from a sophisticated foe. As the five-volume bipartisan report of the Senate Select Committee on Intelligence on the 2016 elections clearly illustrated, Russia availed itself of the open and unquestioning nature of social media platforms to create fictitious online personas to spread falsehoods about the presidential election, and recycled their fabrications through controlled spurious news sites to corroborate and amplify their disinformation. So we have seen what a sophisticated adversary can do in a focused area such as election influence, but there's no reason to think their playbook couldn't be greatly expanded.

On the technical side, the advent of 5G wireless communications and essentially ubiquitous smart phone use mean that virtually everyone will have instantaneous access to information, both accurate and inaccurate, and the deployment of artificial intelligence in an integrated way in communications systems has the potential for shaping and micro-curating news feeds. Referring to a "gathering storm of foreign influence and interference," the NSCAI *Final Report* notes that "adversaries are using AI systems to enhance disinformation campaigns….They are harvesting data on Americans to build profiles of their beliefs, behavior, and biological makeup for tailored attempts to manipulate or coerce individuals." Moreover, increasingly sophisticated AI systems will enable the rapid creation of probably undetectable deep-fake videos and audio recordings, with rich potential for malice and immediate effect. The result might be a world in which we are suspicious of any communications that we cannot authenticate ourselves. While that skepticism might limit the believability of deep-fake videos, such suspicion would surely extend equally to "official" news sources, yielding a chaotic and unreliable reality in which truth and genuine information are elusive.

The seemingly inexorable trajectory of foreign cyber hacks and attacks is instructive for predicting the future of online disinformation from our adversaries. Over the years, Russia, China, Iran and North Korea have all incrementally stepped up their cyber maliciousness, as new vulnerabilities come into existence, ever-more sophisticated tools are created to exploit them, and hacks and attacks succeed again and again without any serious repercussions to the wrongdoers. Operating just below the threshold of war, our cyber rivals can, for a variety of reasons, mostly act with impunity. The same factors that shield those foes in hacks and attacks – the uncertainty of provable attribution, the absence of directly caused actual injury or physical damage and other factors – also will insulate them as they inevitably step up their disinformation campaigns. Indeed, as disinformation is more diffuse in its effect and can be cloaked as mere opinion, it can be wielded with even less concern for retribution. It's hard to see why those adversaries will in the future limit themselves to election influence – little is standing in the way of general commercial disinformation (say, questioning the safety of Boeing aircraft) or undermining our governmental system (for example, asserting that jury trials are rigged, or that municipal water supplies aren't properly maintained).

More specifically, what if Russia or Iran seizes on a real natural disaster – say, a hurricane or flood – and weaponized the crisis with false information online, amplifying and corroborating it on their controlled news sites, and fed false information about the hurricane's path or expected river crestings or even wrong instructions about escape routes? In the future, a coordinated disinformation attack on multiple platforms, especially one seizing on an urgent public safety problem or an already contentious issue such as vaccine safety, could provide the kind of apparent corroboration that would lead to chaos, and it could take weeks – if ever – for the truth to be broadly accepted. What if days before the next election, a deep-fake video manufactured by Russia's intelligence services – virtually undetectable as a fraud – goes viral on YouTube purporting to show a Congressional candidate having a sexual liason with a minor?

Starting to Fix the Problem

We know disinformation is already a big problem, and we fear it could be even worse, so why haven't we done something about it? As with any complex problem, there are many answers. First, like other bad side effects of our cyber lives, there's no miracle drug to cure this disease. Second, we've historically taken a minimal and reactive approach to regulation of the private sector, and even if we started to draw up laws to deal with it, disinformation has itself become a paralyzing political issue. Besides, we're uncomfortable with regulating any speech, and it's not really obvious what we can do about the problem anyway, so we just throw up our hands. As long as disinformation is just gradually corroding our institutions or hindering our national political will or insidiously prolonging a pandemic, there's no one day that we must fix the problem.

We could wait until a crisis or disaster. But we don't need to. The very fact that there are many sources contributing to disinformation means that we have multiple ways to stem it. There are steps we can take to start to fix the problem. No one solution is at hand, but we have tools at our disposal to use and they will, bit by bit, make a difference. I'll mention just three that will help attenuate the threats to our national security.

Probably the most obvious tool is the law, but we first have to get over what seems like a big obstacle. We want neither government nor the private sector to be the final arbiter of the truth or the decider of what we hear and see. Yet allowing the private sector to profit from manipulating what we view online without regard to its truthfulness or the consequences of viral dissemination is simply not sensible public policy. But it's not all or nothing, there is room for some thoughtful regulation. After all, the First Amendment applies only to government and not to private businesses.

So there's room for Congress to act in tightening rules on political campaign ads, perhaps by making certain knowing or intentional falsehoods illegal, such as deliberately spreading incorrect information about polling places – much in the way that the law prevents someone from filing a false police report. Admittedly, there is a delicate line between a prank or spoof, and something clearly malicious and potentially illegal. But the mere fact that the line may be difficult to draw, need not preclude legislation that provides a framework for that process. As has been the subject of recent Congressional attention, some amendment of Section 230 of the Communications Decency Act could be helpful. However well-intentioned at the time of its adoption, the law has come to insulate the business models of social media platforms that are the source of information for billions of people around the globe. These ad-driven models rely on secret, complex algorithms that micro-target users, facilitating the forwarding of material without regard to its accuracy, thus allowing falsehoods to go viral, and often amplifying problematic material.

Another obvious tool is the technology itself. The very technology that helps spawn the problem can be used to correct it too, with AI helping social media platforms spot lies in the first place, identify doctored videos and photographs, and track the dissemination of falsehoods by both domestic and foreign users. And after social media was awash in disinformation during the pandemic and this last election, the platforms finally abandoned their hands-off approach and were more muscular in blocking objectionable content and taking down sham or malevolent accounts. True, there will always be difficulty in deciding what's sufficiently objectionable or incorrect to warrant labeling or even removal – but again, just because it's tough to draw the line doesn't mean we shouldn't even start. One helpful step would be for greater transparency about how such decisions are made, and how a platform's algorithms make recommendations and curate what we see and hear.

Finally, there's a whole range of other steps that can be taken beyond regulation of social media platforms. For example, we could promote international coordination to stop the export of disinformation or to bring cross-border cyber criminals to justice. We could do a much better job of organizing our federal government in a coherent way to fight disinformation, perhaps by setting up a national disinformation center within our intelligence community, just the way we've successfully done with the national counterterrorism center. The Intelligence Community could work more in a more integrated way with the military to counter adversaries' ongoing malign influence campaigns. Saving the potentially most profound step for last, we would garner rich benefits by teaching digital literacy and putting civic education back in our schools – so that disinformation, whether foreign or domestic, will be less likely to take hold in an educated and cyber-sophisticated populace.

Addressing the Threat of Disinformation Is Difficult but Necessary

Cyber-enabled disinformation, whether domestically or foreign generated, is a national security problem, corroding our democracy and governmental institutions, and threatening our public health and, potentially, public safety. It presents special challenges to our military, both because our armed forces are one of those governmental institutions whose credibility is at stake, and because the military obviously plays a unique role in assuring our national security. Those challenges are likely to get worse, with the ongoing march of technology and increasing willingness of our foreign adversaries to use the tool of disinformation to advance their interests. Responding to these challenges will not be easy, since it will require making difficult and controversial decisions about the responsibility of the private sector for our national wellbeing and about restrictions on speech.

Differing ideas are inherent and indeed necessary in any democracy, and there is always fertile ground for discord. But when that discord is polluted by disinformation – whether maliciously homegrown or skillfully fomented by foreign adversaries – it is difficult for government alone to respond. Congress should lead the way, but in the end it is up to our society to come together to manage the increasing cyber vulnerabilities of our everyday personal and business lives. Our national wellbeing depends on nothing less.

Thank you for the opportunity to present my views to the Subcommittee.