Richard Stengel. Former Under Secretary of State for Public Diplomacy and Public Affairs
Distinguished Fellow, Digital Forensics Research Lab at the Atlantic Council.
"The Road to 2020: Defending Against Election Interference. November 19, 2019.
The Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation of the House Committee on Homeland Security

"Governments are instituted among men," the Declaration declares, "deriving their just powers from the consent of the governed." In a democracy, how do we obtain that consent? Through information, the Framers said, true information. The rise of disinformation is a threat to our democracy because it undermines our consent. If that consent is acquired through deception and disinformation, the powers derived from it are not just.

Disinformation is deliberately false information designed to deceive or mislead. Misinformation is simply false information that is not deliberate or designed to mislead. Disinformation is the much greater threat and it is on the rise around the world and at home. In the realm of politics, it is the promulgation of false narratives to undermine democracy.

Disinformation is asymmetric warfare: You might not be able to afford an F35, but you can always hire a few trolls with laptops. Yet it is often a weapon used by the strong against the weak: authoritarian leaders have learned that they can repress free speech at home and spew disinformation on state media. That's a dangerous combination for the future of democracy. Disinformation is difficult to fight because it is hidden in plain sight. It uses all the principles of behavioral economics—and the tools of the big social media companies—to find a targeted audience. Disinformation is as old as information, but social media has made it exponentially easier to create, deliver and instantly find large and receptive audiences.

My book Information Wars is the story of how we attempted to fight Russian and ISIS disinformation from the State Department during the last three years of the Obama administration. I went into government after seven years as the editor of TIME and I thought I understood media. ISIS was something new in terrorism: a non-state actor as adept at social media as barbaric killings. But ISIS's digital jihadis did not pretend to be anyone else other than who they were—unlike the Russians, that is. The Russians adopted other identities and masqueraded as Americans to insert their poison into our digital bloodstream. From the State Department, we first saw Russia create a wave of social media disinformation in the Russian periphery around Putin's illegal invasion of Ukraine in 2014—and then the Russians took what they learned there and aimed it squarely at our election space in 2016.

What also makes disinformation effective is that there is often a kernel of truth in it. What united ISIS and Russian disinformation was what I called the weaponization of grievance. ISIS weaponized the grievances of Sunni Muslims who felt left out by modernity and repressed by their rulers. Putin weaponized the grievances of Russians who mourned the loss of the

Soviet Union and never adapted to the modern world. If ISIS had a slogan, it was Make Islam Great Again. If Putin had a slogan, it would be Make Russia Great Again. They had their mantras long before we heard about making America great again. This global weaponization of grievance is the unified theory behind the rise of nationalism and right wing strongmen across the globe.

But the ultimate threat is here at home. It's easier and more comfortable for us to see this problem as a threat from the outside, from foreign influence operations. And, indeed, they remain a grave national security threat. But the scale and range of domestic disinformation—created and spread by Americans to other Americans—dwarfs any foreign threat or troll factory. Our foreign adversaries seek to engage Americans and do so, but our homegrown disinformation overwhelms what our adversaries produce. Our internal challenge is far greater and more dangerous than any external one.

In attempting to counter Russian and ISIS disinformation I came to see that government was not the answer. I saw that "countering" disinformation was often counter-productive. When we tried to create content ourselves, we very often played into our adversaries' hands. After all, we were the enemy. It's very hard for a tweet from the U.S. State Department to persuade someone of our point of view if we are seen as the cause of the problem. They see our efforts to rebut them as confirmation that they are right and that their strategy is working.

Democracies just aren't very good at combatting disinformation. Why is that? One reason is that our opponents not only use our freedoms against us, but our technology. They exploit freedom of speech to create dangerous and false speech, which is protected by the First Amendment. They utilize the same tools of micro-targeting that advertisers use to market sneakers and phones but they use them to sell us false narratives and conspiracy theories. Disinformation is hard to fight because it's not just a supply problem, it's a demand problem. People embrace it when it seems to confirm their beliefs. It's a missile that hits its target because the target welcomes it. The truth is, disinformation doesn't create divisions so much as widen them.

At the end of last year, the initial Senate Select Committee on Intelligence report on Russian interference in the 2016 election said the Internet Research Agency in St. Petersburg had created more than 10 million tweets—of which six million were original—across 4,000 accounts; more than 100,000 Instagram posts; and more than 50,000 Facebook post. The second Senate Intelligence Committee report that came out last month reported that the Russians had done more since the election than they did before it. Now, as then, it's a whole of government effort which includes Russian intelligence services, conventional Russian media, and even the foreign ministry. The Russians are shrewd about using our own biases against us. In 2016, they sought out groups who were afraid of immigrants and Muslims and stoked their fears. They targeted African American voters and told them voting was a waste of time. After Twitter and Facebook removed many online assets attributed to Russia in 2017, the Russians

returned with a more tailored focus to activist communities who were susceptible to disinformation. With a focus on 2020, the Russians will again seek out cultural and social divisions and try to magnify them. As with 2016, they will often amplify both sides of divisive issues. Anything to create chaos and disunity and doubt about the integrity of our political process.

Even though I don't think government has much of a role in countering disinformation through creating content or taking it down, I do think there is a clear government role in raising awareness and creating resilience to disinformation. Combatting disinformation is a cross-cutting issue that has implications for a wide range of different agencies and committees. First, I think government has a role in regulating the platforms that host disinformation. Currently, there is an alignment of economic interests between the disinformationists and the platforms: the social media companies make money when disinformation goes viral. Right now, the law doesn't treat the platform companies as publishers and they have complete immunity from liability for the content on their platforms. Not only are these companies publishers, they are the biggest publishers in the history of the world. No, they don't have human editors, but as a former editor I'm here to tell you that algorithms and content recommendation engines are editors—the fastest and most efficient editors in history.

To be sure, these companies cannot have the same liability that I used to have as editor of TIME. But they need to have some liability for content that is on their platform that is demonstrably false, that is created by robots, that attacks others on the basis of race, religion, ethnicity, gender or sexual orientation, that is created by foreign actors to deceive American voters. They need to be legally accountable for making a good faith effort to remove such content from their platforms.

As the 2020 election approaches, there are a host of new problems: deep fakes; data manipulation, where bad actors don't steal data but manipulate it; the professionalization of interference, as private companies hire out their services to create disinformation; the rise of domestic disinformation and the recruiting of Americans as witting or unwitting agents of disinformation.

Combatting these new efforts requires the detection and removal of foreign influence in our election, greater ad transparency, more accountability for the platform companies, and greater data protection. I would endorse the Senate Intelligence Committee's recommendations for fighting disinformation, and in particular the timely sharing of information between the private and public sector of real-time threats. I believe the tech companies would welcome that too. I'd also recommend the Five D's of combatting disinformation: detection, demotion, deletion, disclosure and digital literacy. The empowering of the Global Engagement Center, which was created at the end of 2016, to truly help fight all kinds of disinformation could be a vital effort of the government. It is important to pass the Honest Ads Act, which would provide for more transparency in political advertising. All of this in

addition to giving the content companies more liability for publishing proscribed content would help but not remedy the flood of disinformation. I've often said we don't have a fake news problem, we have a media literacy problem. Media and digital literacy need to be taught and the schools, and I can't think of a better source of that funding than the platform companies. We also need a privacy bill of rights that protects our information as part of a new digital social contract. The ownership of one's personal information is an unalienable right.

The disinformationists know that it's far easier to create confusion rather than clarity, to confuse rather than persuade. They want people to see empirical facts as an elitist conspiracy. Citizens have trouble discerning fact from fiction and we need to teach media and digital literacy in the schools from an early age. In a new poll from this past week, 47% of Americans say they find it difficult to know whether the information they encounter is true. The public needs to see that countering disinformation is a civic duty for which we all are responsible. Ultimately, the problem of disinformation is not so much that people will come to believe what is false. The greatest problem is that they it will cause them to question what is true.