LAWFARE

DISINFORMATION

The Next Gray Zone Conflict: State-Based Disinformation Attacks on the Private Sector

By **Matthew F. Ferraro**, **Preston B. Golson** Tuesday, March 24, 2020, 10:30 AM

DayZero: Cybersecurity Law and Policy

For years, the Russian-backed TV channel RT America has been airing a series of deceptive reports on the dangers of upgraded cell technology known as 5G. These reports have linked 5G signals to all manner of diseases—including brain cancer, autism and Alzheimer's disease. All these claims are scientifically baseless. The likely goal of this spurious reporting is to sow doubt about a technology that the U.S. believes is key to its future high-tech dominance—and for which Vladimir Putin's Russia has no equivalent. If Russia can't compete in the lab, it can try to spread confusion on the airwaves.

The story of RT's attack on 5G is a glimpse of the near-future. Adversaries such as Russia, Iran and China look for ways to harass American interests without triggering all-out conflict. As trade wars proliferate, technological rivalries intensify, and multinational corporations take public positions on hot-button social issues, this form of "gray zone conflict"—coercive actions that lie somewhere between diplomacy and warfare—will likely increase in scale and scope as competitors seek a strategic and economic advantage over the United States.

American businesses will increasingly find themselves in the crosshairs of nation-state-sponsored disinformation operations.

There are several reasons why.

First, more and more countries have disinformation capabilities in their arsenal. According to a recent Oxford University report, more than 70 countries have state-sponsored disinformation units. There's no reason to think their targets will remain solely political. After all, economic interests have become further entangled with national interests. Economic espionage, state-sponsored hacks of private firms, and regulatory war over leading-edge technologies are all fixtures of current geopolitics. Disinformation attacks on the private sector are the next frontier in that conflict.

Second, these operations are difficult for governments to deter. These campaigns are deniable, and proving attribution is difficult. Think of Russia's Internet Research Agency, sometimes referred to as the "St. Petersburg troll factory," which seeds social media with false narratives while trying to cover its tracks, or web pages that push disinformation and do not have clear Russian attribution but are supported by Moscow.

Third, in the contemporary information ecosystem, businesses are exposed to reputational damage as never before—a persuasive post can wing from one corner of the globe to the other in mere moments.

Fourth, disinformation attacks on U.S. companies can help protect the favored domestic industries or companies (the so-called national champions) of adversary nations. For example, Russian propagandists have pushed false stories targeting the U.S. fracking industry in an effort to curtail a sector that hurts Russia's oil wealth. Russia-linked outlets have done the same to amplify voices raising concerns about Western food production, GMOs and vaccines.

New technologies, such as highly realistic forged video and audio media known as deepfakes will make these campaigns more dangerous by tricking people into doubting their own eyes and ears. For example, imagine a Chinese automotive company publicizing a convincing deepfake video showing a gruesome crash of an American autonomous vehicle, in a bid to undermine confidence in a U.S. competitor. A Russian company has already staged an electric car accident as a public relations stunt. Several media outlets shared the faked video as if it was real footage, spreading disinformation about the cars' safety.

Fifth, disinformation against private actors is particularly attractive to adversaries because it can help them meet their strategic objectives. In particular, information operations can foster dissent and undermine public faith in the democratic process and trusted institutions—a strategic aim of Russia, according to an intelligence community assessment. Because certain brands and companies can be symbols of national identity, damaging them can be a proxy attack on the nation itself. And reputational damage can not only impact public faith in a business but also lead to tangible losses—of customers, stock values, jobs and market share. Weaponized information can cause real damage.

The writing is already on the wall.

For example, early on Thanksgiving Day 2015, someone named "Alice Norton" posted a message on a cooking website, saying her family had been stricken after eating a turkey linked to a small business in Pennsylvania called Koch's Family Farm. Thousands of tweets and posts on social networks shared comparable claims. An article on a website marketed to African Americans asserted that 200 people were in "critical condition" in New York City—all from eating turkeys from Koch's Family Farm. A page appeared on Wikipedia about the incident; someone filed a complaint about it with the U.S. Department of Agriculture.

In response, the farm began an internal food-safety review. It then realized that the whole campaign was a hoax. The Wall Street Journal reported that Russia's Internet Research Agency had propagated some of the phony stories to sow discord among Americans, pushing the narrative that a large corporation was victimizing a minority group. The farm's president thinks they may have been victims of mistaken identity—the farm shares no relation to the politically active Koch brothers. Propaganda expert John Kelly believes the farm was merely collateral damage as Russian actors practiced sowing discord within American online communities. The Russians were then studying how to spread disinformation and rehearsing for the kind of campaign they launched during the 2016 election to widen social fissures. As companies increasingly take stances on controversial social issues, malicious state actors will have greater opportunities to target private-sector entities with similar operations.

Sixth and finally, disinformation is inexpensive and can even make money for nation-states. According to one estimate, fake news websites with clickable headlines and sufficient traffic net at least $100,000 a month in ad revenue. In aggregate, ad revenue from disinformation can be massive. The Global Disinformation Index, a British nonprofit group, estimated that websites peddling disinformation have taken in $235 million worth of advertising revenue. Fraudsters are already using manipulated media and falsified audio to trick company employees to wire money to thieves posing as company CEOs. Monetizing bogus stories is a logical next step.

Consider: North Korea's economy shrank by more than 4 percent in 2018—the most in more than two decades. Pyongyang has sophisticated information warfare capabilities and has shown no compunction about brazenly using malicious technology to harm U.S. companies and to fill North Korean state coffers. Little would stop them from getting into the disinformation business, too.

While all businesses face risks to their reputations and valuations from disinformation, some companies face greater exposure. A business may be particularly vulnerable to such campaigns if its technology is the subject of a nation-state rivalry, like 5G technology or artificial intelligence. A company may also face an increased risk if the company's leadership has taken a stand criticizing an autocratic nation-state or its policies—the offended autocrat may reward the CEO's courage with bot farms pushing disinformation about the CEO personally or her company. Finally, if a foreign state has already targeted a business with cyber hacks or cybercrime, it is a good bet a disinformation attack may be next.

This new gray zone conflict will require a full-spectrum response. Both the private sector and the federal government need to get involved. Businesses should practice top-notch cybersecurity and prepare for disinformation attacks similar to how companies plan for cybersecurity breaches. They should red team and consider the messages that may be used to exploit their reputational vulnerabilities. And they should develop and test responses that will help build resilience among their stakeholders. The federal government (including the Cybersecurity and Infrastructure Security Agency, the Federal Trade Commission, and the Securities and Exchange Commission, among others) should work with the private sector to buttress their cyber defenses, encourage information sharing, monitor threats, and safeguard consumers and markets. Protecting the American economy from foreign state-based disinformation campaigns must be a national security priority.

Topics: Disinformation, Cybersecurity

Tags: Information Operations

Matthew F. Ferraro, an attorney and former U.S. intelligence officer, is a term member of the Council on Foreign Relations and a visiting fellow at the National Security Institute at George Mason Law School.

@MatthewFFerraro

Preston B. Golson is a Director at the Brunswick Group and was formerly a Spokesperson and intelligence analyst at the Central Intelligence Agency.