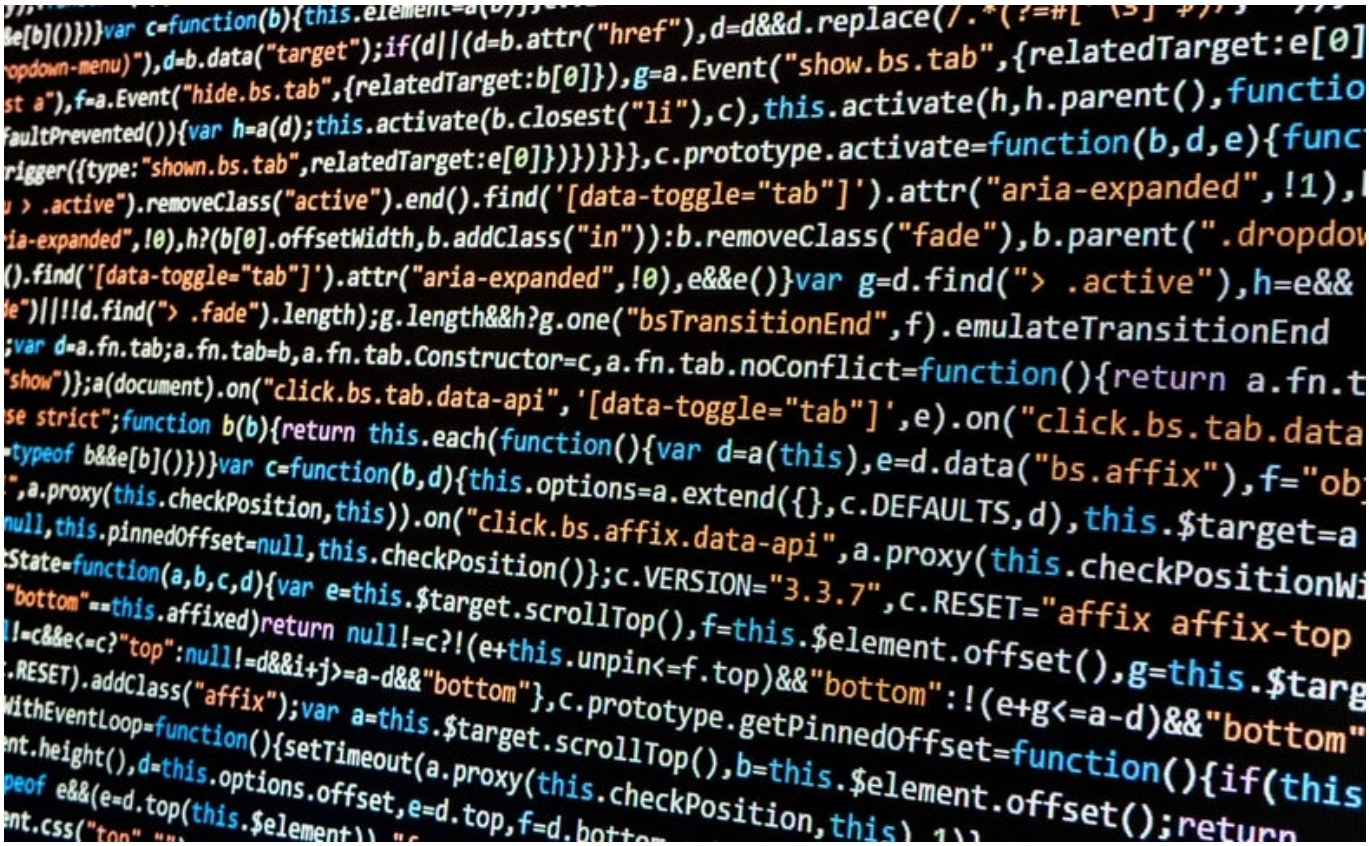
Published on *USC Center on Public Diplomacy* (http://uscpublicdiplomacy.org)

Thumbnail Image:



Can Public Diplomacy Survive the Internet? [1]

Gone are the days of digital euphoria, where thought leaders pontificated on the ways in which the internet and global connectivity would unite the world and foster a new era of world peace and prosperity. With speculation of Russia trying to digitally disrupt Western elections, to news of suicides being broadcast in real-time via Facebook Live, we are increasingly confronted with the reality of a world where information abundance is threatening to wreak havoc on our lives and the institutions we've come to depend on. If presentations from the Atlantic Council's #DisinfoWeek are any indication, things are likely to get worse before they get better.

Yet to blame our current predicament on information abundance alone doesn't tell the complete story. Today's social and internet platforms are places of constant change, but much like the allegory of a frog, slowly heated in water and not realizing the possible death-by-boil, the slow changes to our online platforms in the form of trolls and bots risk scalding the information space around us.

Alarm bells are starting to ring but it's important to understand the danger and how to mitigate it. The three main tools for manipulation are trolls, bots, and hackers. Trolls are individuals who post content or simply comment on the content of others and try to undermine it. They often do not just take the form of one persona online, but frequently swarm by the dozen. Bots can be used in two main ways: first to simply amplify content, and second to mimic actual human beings online. On Twitter for

example, one individual may control hundreds of bots that can automatically retweet the content of their favorite politician or bolster the perceived virality of a tweet or hashtag. Bots can also be used to respond to specific triggers using artificial intelligence—responding to breaking news, for example—or give the perception that the bot is actually in conversation with you. Chatbots are frequently used by companies as online customer service representatives. They are programmed to automatically respond to customer queries with a tailored, intelligent response sourced from the internet or company databases.

Hackers can disrupt our information space by stealing information or undermining the trust in systems. We have seen many examples of emails being stolen from companies or individuals to influence public perception of these organizations. Hackers can also undermine the credibility of processes such as exposing vulnerabilities in donation systems to reduce donations to a political candidate or undermining the perceived credibility of electronic voting machines to give publics concerns about the reliability of the poll results. Growing use of trolls, bots, and hackers each represent unique threats to the platforms we have come to depend on, not just for social messaging, but also to interface with many of the institutions we depend on every day.

Collectively, these threats constitute a clear shift towards the weaponization of information. Presently, that threat comes most prominently from Russian affiliated trolls and hackers, though other governments and non-state actors are not far behind. These entities and their affiliates seek to distort the information space for political or monetary gain. This is a major departure from the days of old propaganda where one's aim was to create a sense of affinity for one's cause. Today, Russia's aim is squarely to disrupt. It is far easier to convince individuals to question everything, undermining the credibility of good and bad actors alike. These disruptions, even if minor, force legitimate actors to spend time, money, and credibility responding to these tactics as opposed to governing or serving a client.

Rather than obsessing over trending news topics alone, we need to develop greater capacity to understand competing public narratives in foreign contexts and track how they adapt over time.

Despite what the cyber thriller *Mr. Robot* would have us believe, the aim of these efforts isn't simply to take down a single government or corporation. Rather, taken collectively, they risk a loss of faith in institutions, empiricism, and truth. The manipulation of the information space has become so sophisticated it is easy to lose one's perspective on reality. This can be as simple as fake news being promulgated as reliable or as sophisticated as voice and video technology that can manipulate a person's voice and likeness to say anything the programmer desires. These tools can be used to manipulate the newsfeed, the markets, and potentially even lead to military conflicts. Far too many think that this is a problem for others, those unable to see disinformation campaigns for what they are. In fact, between August and November 2016, fake stories earned more shares, reactions, and comments on Facebook than real news stories. If you are on Facebook, chances are you read, or even shared, some fake news story in the past 12 months.

Despite the growing risks involved in our current era of information abundance, we need not throw the baby out with the bath water. At the height of the Cold War it may have been tempting to want to ban all nuclear technology, but as we have discovered through the years, nuclear technology can

provide life changing and saving outcomes for millions around the world. The same is true for online platforms and digital communication tools. They have allowed us to connect with lost friends and family, unite around causes, and celebrate just how crazy our cats are. These technologies have positive, peaceful, or just mundane legitimate uses. What we have to decide is how to protect the good from the bad. How do we create a safe space for expression while limiting the harm bad actors may wish to inflict?

To be sure, both governments and corporations are eager to find a way to preserve the current information ecosystem so that users can trust the safety and integrity of their digital experiences. Microsoft, for example, has proposed a Digital Geneva Convention, suggesting sets of rules for governments, corporations, and civil society to abide by to restore the Web and digital's future. Facebook, too, is eager to crack down on government-led misinformation campaigns. Companies whose business model depends on widespread use and trust in digital communications platforms likely see the onslaught of bots, trolls, and hackers as a potentially existential threat, and will act accordingly.

What does this mean for public diplomacy?

The U.S. Advisory Commission on Public Diplomacy recently published a report, *Can Public Diplomacy Survive the Internet: Bots, Echo Chambers, and Disinformation*, aiming to address precisely these questions. In short, to survive these changes, public diplomacy professionals needs to focus on four main lines of effort: better understand how social platforms are used and manipulated in specific contexts to be prepared for computational propaganda campaigns; ensure reliability of analytics; maintain human and institutional relationships; and work to establish norms of conduct for the information space.

1. Better understanding the actual uses of these tools means moving beyond our reliance on "folk theories" of social media, and instead focusing on their actual use and impact in specific communities. Folks theories—how we think something works, regardless of how it actually functions—place far too much emphasis on concepts like the "echo chamber," which research shows is actually less of a concern online than offline.

2. Related, we need to be more careful in our consideration and use of popular web analytics. Virality—the crown jewel in the social media realm—is overemphasized often at the expense of more important metrics like context and longevity. Many of the metrics used to measure the effectiveness of social media campaigns are vulnerable to manipulation, and more importantly, don't measure engagement in any meaningful way. These metrics were built for an industry reliant on advertising for revenue generation, and as a result, may not be well-suited when applied to the context of public diplomacy. To ensure the reliability of analytics, we need to work with the private sector to find ways to modernize our digital tools or develop new metrics to judge engagement, sentiment, and impact.

3. Using both traditional and technological tools, we need to maintain the relationships we have already formed and dialogue directly to our friends, associates, and adversaries. Not only will this be crucial if trust continues to erode in the digital space, but it is also central to creating, and forging consensus around, strategic narratives that synchronize U.S. foreign policy priorities with global prosperity. Rather than obsessing over trending news topics alone, we need to develop greater capacity to understand competing public narratives in foreign contexts and track how they adapt over time. Understanding distinctions between system (or governance), value, and identity narratives allows public diplomacy practitioners to construct policy narratives that speak to, or at least acknowledge, the underlying pillars of belief in a given community.

4. Last, working closely with the private sector, the State Department should take lead in establishing

standards of conduct for the information space and encourage the rest of government, as well as our allies, to sign on as well. More than ever, intellectual leadership is needed to navigate this increasingly contested and information-rich space.

As outlined in greater detail in the report, much more work needs to be done in the private sector, in government, and in academia to not just react to the challenge of trolls, bots, and hackers, but rather to get ahead of them and restore trust in our digital ecosystem. These are only the first steps.

Many public diplomats were trained (on the job or otherwise) in a world of information scarcity, often operating in countries where information, especially credible news, was the scarce resource. Today, credible information remains scarce, but it is, by all accounts, in high demand in a flooded information space. As a result, focusing attention is now the critical factor. Bots, trolls, and hackers have mastered the art of competing in a crowded marketplace for attention, but what they can't offer in any sustainable way is meaningful, credible information. This represents both the challenge, and path, for public diplomacy to not just survive, but thrive, on the internet.

Photo by Lorenzo Cafaro I *CC0*
