FOREIGN AFFAIRS

How to Counter Fake News

Technology Can Help Distinguish Fact From Fiction

By Martin J. O'Malley and Peter L. Levin

January 5, 2017

During the 2016 U.S. presidential election, Macedonian teens looking to get paid for ad-clicks, Russian cyber sophisticates apparently looking to tilt the outcome, and some homegrown mood manipulators broadcast outrageous and false stories packaged to look like real news. Their counterfeit posts were nearly indistinguishable from authentic coin and remain so, even in the face of skeptical but impatient fact-checking.

Although much of the establishment has been left wringing its hands about what to do—how to ferret out fake news and those who produce it—there are already tools and systems to help digital investigations and gumshoe reporters connect the dots and discover scams. Metadata—the data about data—can provide a digital signature to identify actors on the Internet. And the Web itself allows us to examine timelines, serialize events, and identify primary sources. Some signatures are harder to find than others, but they are all there; you just need to know where to look and what to analyze.

Indeed, the intelligence community already thwarts terrorist attacks through methods like these, known in the vernacular as “tools, processes, and procedures,” and the Department of Homeland Security maintains a knowledge center of vulnerabilities. Such work will be aided by the newly created Global Engagement Center, (section 1287 of the National Defense Authorization Act signed by U.S. President Barack Obama just before Christmas), which expands the government’s repertoire and mandate to “identify current and emerging trends in foreign propaganda and disinformation in order to coordinate and shape the development of tactics, techniques, and procedures to expose and refute foreign misinformation and disinformation and proactively promote fact-based narratives and policies to audiences outside the United States.”

The language comes from a cybersecurity bill that U.S. Senator Rob Portman (R-Ohio) introduced last spring. According to co-sponsor Chris Murphy (D-Conn.), the United States now has dedicated “resources to confront our adversaries’ widespread efforts to spread false narratives that undermine democratic institutions and compromise America’s foreign policy goals” in the digital age. With modest funding and proper oversight, the Global Engagement Center will help the government reach back in time and across virtual space to ensure that streams of data are not contaminated by state-sponsored misinformation or falsehoods.

The center's special envoy and coordinator, Michael Lumpkin, told us that it is an agile, innovative, data-driven organization, and this is precisely the approach needed to take on the emerging threats in the information space. Unfortunately, the State Department is not known for agility or innovation. Too often we are using nineteenth century bureaucracy, with twentieth century technology to fight twenty first century adversaries. We simply have to get better in the information battlespace. We’ve made progress since ISIS first came onto the world stage, but as the challenges and adversaries morph, agility will continue to be key.

There are other steps Washington and the media can take now, born of Portman's legislation, network architecture, and operational practices, which would protect the public.

In November, Merrimack College media professor Melissa Zimdars posted some tips for analyzing news sources. Her report was followed last month by Silicon Valley publisher Tim O'Reilly's outline of a basic verification framework that chronicles the steps he took to fact-check an Internet "meme" that claimed to correlate crime rates to voting trends. The story was easily proved false, but doing so required personal persistence and the ability to make creative connections between authentic root sources. Few people could, or would, invest the amount of time that Zimdars or O'Reilly recommend, but computers are not intimidated by a mountain of pattern-matching tasks. Indeed, O'Reilly's framework is ripe for automation. From a technological perspective, these are surprisingly easy problems to address, and we can do so safely, securely, and reliably.

Today almost 40 percent of Americans get their news online. A "we report, you decide" approach to truth undermines a critical feedback loop that makes democratic governance possible. If the most reputable news organizations do not invest time and treasure in confirming sources and facts, then representative democracy becomes a mayhem of funhouse mirrors.

But the Internet is constructed to resist obstructions. Picture water flowing around rocks in a river. Place a big boulder in the middle, and the current will divert around it, although the water level may rise in the vicinity of the blockage. In this analogy, the drops of water are data packets, and Internet packets are designed to remember the precise path they take to keep the aggregate flow manageable and predictable.

Consequently, network gateways—the tributaries to and channels from the aggregate flow—can always determine where a message originates. Although it is impossible to predict what will happen downstream, it is easy to know how many and which nodes a packet passed through on its way from its source to a waypoint. Indeed, in much the same way that we "authenticate" people we can hear but not see—by their phone number, by the sound of their voice, by their vocabulary, by their interests—so too can we authenticate real news. We can do this by generating (through machine learning or by brute-force pattern-matching) a signature that reconstructs the flow of a packet. We can examine the waypoints of the packets between source and destination to determine its origin (a proxy for authenticity), and we can patiently maintain a record of trustworthy signatures over time. In that way technology can quickly distinguish between uncontaminated springs of news and manufactured springs that have been poisoned with misinformation or disinformation.

Of course, attribution and anonymity are zero-sum. And not even an intelligent machine will sort perfectly. But for now, the problem is that identifying fake news is a manual process prone to human error and the duress of news-cycle urgency. As long as media and readers are unable to quickly and reliably expose fake news, it will undermine the public's ability to govern itself. And the inability to unmask state-sponsored Internet propaganda could well pose a very real threat to national security. That is why even an imperfect automated sorting process is better than nothing.

The inability to unmask state-sponsored Internet propaganda could well pose a very real threat to national security.

The scourge of misinformation is as old as language itself, but Internet-fast global manipulation is relatively new. The good news is that there are methods and systems that can help ordinary users discern what's reliable from what's invented. Major distribution platforms—from network and cable news to web-based platforms that service billions of users—should move quickly toward sensible solutions that do not censor, but that do provide citizen consumers with a qualitative indication of reliability. Software applications will learn how to do this, much like they already, if imperfectly, catch spam in email.

"Trust but verify" is a serviceable policy framework when there's plausible reason to trust, and ready means to verify. The erosion of these traditional norms on the Internet scuttles authentic debate on the rocks of superstition, impulse, emotion, and bias. With new public-sector investment and private-sector innovation, we are optimistic that the United States can fight back against fake news and foreign influence in U.S. elections.