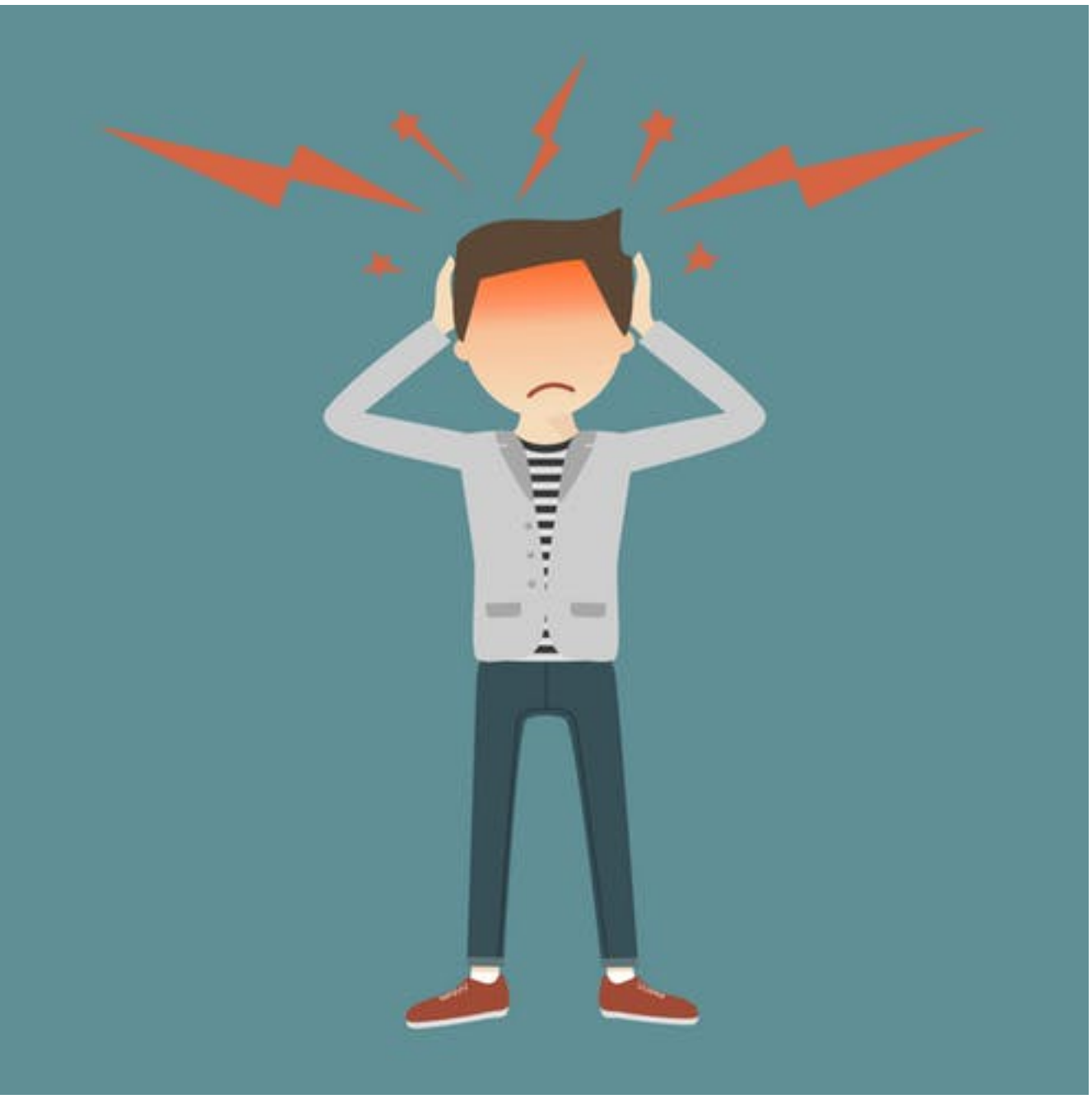
THE CONVERSATION

Academic rigor, journalistic flair



Cyberattacks target Americans' thinking. Fancy Tapis/Shutterstock.com

Weaponized information seeks a new target in cyberspace: Users' minds

July 30, 2018 6.30am EDT

The Russian attacks on the 2016 U.S. presidential election and the country's continuing election-related hacking have happened across all three dimensions of cyberspace – physical, informational and cognitive. The first two are well-known: For years, hackers have exploited hardware and software flaws to gain unauthorized access to computers and networks – and stolen information they've found. The third dimension, however, is a newer target – and a more concerning one.

Author

Richard Forno

Senior Lecturer, Cybersecurity & Internet Researcher, University of Maryland,

Baltimore County

This three-dimensional view of cyberspace comes from my late mentor, Professor Dan Kuehl of the National Defense University, who expressed concern about traditional hacking activities and what they meant for national security. But he also foresaw the potential – now clear to the public at large – that those tools could be used to target people's perceptions and thought processes, too. That's what the Russians allegedly did, according to federal indictments issued in February and July, laying out evidence that Russian civilians and military personnel used online tools to influence Americans' political views – and, potentially, their votes. They may be setting up to do it again for the 2018 midterm elections.

Some observers suggest that using internet tools for espionage and as fuel for disinformation campaigns is a new form of "hybrid warfare." Their idea is that the lines are blurring between the traditional kinetic warfare of bombs, missiles and guns, and the unconventional, stealthy warfare long practiced against foreigners' "hearts and minds" by intelligence and special forces capabilities.

However, I believe this isn't a new form of war at all: Rather, it is the same old strategies taking advantage of the latest available technologies. Just as online marketing companies use sponsored content and search engine manipulation to distribute biased information to the public, governments are using internet-based tools to pursue their agendas. In other words, they're hacking a different kind of system through social engineering on a grand scale.

Americans are used to seeing Russian propaganda that looks like this. AP Photo/Kirsty Wigglesworth

Old goals, new techniques

More than 2,400 years ago, the Chinese military strategist and philosopher Sun Tzu made it an axiom of war that it's best to "subdue the enemy without fighting." Using information – or disinformation, or propaganda – as a weapon can be one way to destabilize a population and disable the target country. In 1984 a former KGB agent who defected to the West discussed this as a long-term process and more or less predicted what's happening in the U.S. now.

The Russians created false social media accounts to simulate political activists – such as @TEN_GOP, which purported to be associated with the Tennessee Republican Party. Just that one account attracted more than 100,000 followers. The goal was to distribute propaganda, such as captioned photos, posters or short animated graphics, purposely designed to enrage and engage these accounts' followers. Those people would then pass the information along through their own personal social networks.

Starting from seeds planted by Russian fakers, including some who claimed to be U.S. citizens, those ideas grew and flourished through amplification by real people. Unfortunately, whether originating from Russia or elsewhere, fake information and conspiracy theories can form the basis for discussion at major partisan media outlets.

As ideas with niche online beginnings moved into the traditional mass media landscape, they serve to keep controversies alive by sustaining divisive arguments on both sides. For instance, one Russian troll factory had its online personas host rallies both for and against each of the major candidates in the 2016 presidential election. Though the rallies never took place, the online buzz about them helped inflame divisions in society.

The trolls also set up Twitter accounts purportedly representing local news organizations – including defunct ones – to take advantage of Americans' greater trust of local news sources than national ones. These accounts operated for several years – one for the Chicago Daily News, closed since 1978, was created in May 2014 and collected 20,000 followers – passing along legitimate local news stories, likely seeking to win followers' trust ahead of future disinformation campaigns. Shut down before they could fulfill that end, these accounts cleverly aimed to exploit the fact that many Americans' political views cloud their ability to separate fact from opinion in the news.

These sorts of activities are functions of traditional espionage: Foment discord and then sit back while the target population becomes distracted arguing among themselves.

Fighting digital disinformation is hard

Analyzing, let alone countering, this type of provocative behavior can be difficult. Russia isn't alone, either: The U.S. tries to influence foreign audiences and global opinions, including through Voice of America online and radio services and intelligence services' activities. And it's not just governments that get involved. Companies, advocacy groups and others also can conduct disinformation campaigns.

Unfortunately, laws and regulations are ineffective remedies. Further, social media companies have been fairly slow to respond to this phenomenon. Twitter reportedly suspended more than 70 million fake accounts earlier this summer. That included nearly 50 social media accounts like the fake Chicago Daily News one.

Facebook, too, says it is working to reduce the spread of "fake news" on its platform. Yet both companies make their money from users' activity on their sites – so they are conflicted, trying to stifle misleading content while also boosting users' involvement.

Real defense happens in the brain

The best protection against threats to the cognitive dimension of cyberspace depends on users' own actions and knowledge. Objectively educated, rational citizens should serve as the foundation of a strong democratic society. But that defense fails if people don't have the skills – or worse, don't use them – to think critically about what they're seeing and examine claims of fact before accepting them as true.

American voters expect ongoing Russian interference in U.S. elections. In fact, it appears to have already begun. To help combat that influence, the U.S. Justice Department plans to alert the public when its

investigations discover foreign espionage, hacking and disinformation relating to the upcoming 2018 midterm elections. And the National Security Agency has created a task force to counter Russian hacking of election systems and major political parties' computer networks.

These efforts are a good start, but the real solution will begin when people start realizing they're being subjected to this sort of cognitive attack and that it's not all just a hoax.

US politics | Vladimir Putin | Propaganda | Donald Trump | Information warfare | 2016 election campaign | Russian hacking | Russian propaganda