Addressing Cyber-Enabled Information Operations

Gary Brown

Perhaps the greatest current cyberspace threat is cyber-enabled information operations, which strike at the narratives that underlie social cohesion. The long-term solution is education in critical thinking, but some legal changes could help blunt the effects in the short term.

In the three decades since cyberspace entered the public consciousness, much of the strategic discussion about it has been focused on using cyber capabilities to affect physical systems. For example, cyber attacks on power plants, dams, uranium enrichment facilities and pipelines have all garnered huge attention. This kind of attack seemed futuristic and exciting – a completely new area of operations. Only in 2016, when Russian attempts to influence the US presidential election became public, did serious attention turn toward the use of cyberspace to manipulate information and influence decision-making.

Defending against cyber aggression aimed at networks, systems and infrastructure is vital, but it is more likely that core democratic interests will be compromised by cyber-enabled information operations than by cyber attacks. Leveraging cyber capabilities in support of kinetic warfare is now the norm, and cyber attacks present unique challenges, but they are not fundamentally different from traditional kinetic warfare. Desired cyber-driven effects occur primarily in the physical space, degrading integrated air defence systems or switching off a power grid, for example, and military contests are still dominated by kinetic military power. Large-scale, cyber-only warfare is decades away. Cyber-enabled information operations is a critical competition space now.

Some aspects of modern information operations are nothing new – for example, propaganda distributed through leafleting or state-sponsored radio stations. But while there are parallels between the traditional information environment, there are also real differences between old methods and current techniques. The most significant are how cyberspace enables the rapid de-isolation of radical individuals, the use of big data to target information delivery, the loss of information gatekeepers, and science-enabled exploitation of attention. The first two are essentially quantitative differences; the latter two are completely new problems. All four are discussed below.

There have always been people with unpopular, obnoxious or hurtful ideas, and some of them are motivated to take their ideas public. Until fairly recently, the ways available to do that were limited in scope. For example, underground newspapers, photocopied newsletters, public-access television and, in the UK, Speakers’ Corner, all reach only a sliver of the population. In those cases, irritating and insulting opinions are absorbed in the marketplace of ideas, largely discarded in favour of more accurate, unifying or helpful speech. Cyberspace has enabled instant and broad distribution of these formerly contained voices, creating potentially huge audiences. And, while many of these ideas are harmless, social media platforms have enabled the weaponisation of ideas, most obviously through the incitement of ethnic violence. Incidents in India and Myanmar are examples of how devastating such speech can be.

The information situation democracies now face was decades in the making and there are no quick solutions

‘Big data’ generally refers to the unprecedented speed at which information is collected by connected devices, generating vast accumulations of data that can be used for ‘actionable insight, improved decision making, and competitive advantage’. Information garnered through shopping loyalty programmes, credit cards, online shopping and social networking has increased available data exponentially, and analysis of these data points – big data – can predict, sometimes with frightening accuracy, political attitudes, affiliations, household income and many other personal details about people. This type of analysis can be used to narrowcast information to receptive audiences, bringing together previously isolated radicals.

The other two changes cyber-enabled information operations have wrought are different not only in scope but in nature from what we have experienced before. The first – the widespread loss of information gatekeepers – is unprecedented and has contributed to the scope and
effectiveness of modern influence campaigns. Since the Second World War, news and information has been curated by trusted experts or commentators. An iconic example is Walter Cronkite’s presentation of the CBS evening news through the 1960s and 1970s. Called the ‘most trusted man in America’, when Cronkite turned against the Vietnam War, public sentiment in the US soon followed. Cronkite retired in 1981, and no journalist since has enjoyed such a high level of trust in the US.

Even the BBC’s reputation has suffered in the new information environment. A recent poll showed a fifth of Britons had no trust in the BBC to tell the truth, while less than half trusted the BBC a ‘great deal’ to tell the truth. People relied on to determine what information is worthy of being broadcast to large portions of the population are now rarer and less universally acknowledged. There has been a widespread loss of faith in government, mainstream media and other traditional institutions, leaving individuals to act as their own filters. They are assisted by algorithms, known and unknown, pushing information that data indicates will be of interest to them. This fragmented information environment makes the idea of building a shared national narrative that would immunise society against hostile influences extremely difficult.

The fourth fundamental change in the information environment is science-enabled exploitation of attention. Of course, entertainers, advertisers, politicians and others have always attempted to build audiences with attention-grabbing techniques. In recent years, the attention economy – which basically translates online views of content into money – has provided the funding to develop strategies that make it almost impossible for humans to turn away. It started as a way to draw eyes for profit, but the same techniques work to expose individuals to information that is specifically designed to feed their biases and prevent objective analysis of facts.

Perhaps the most striking example of cyber-based exploitation of attention is YouTube, where algorithms serve up video after video to viewers based on previously viewed content. If one has the slightest interest in hearing from flat-earthers, climate change deniers, white nationalists or other fringe groups, YouTube’s algorithms will eventually sniff out that interest and deliver responsive content. Combining the modern addiction to screens, an expectation of near-constant stimulation, and reinforcement through games or messages that stimulate parts of the brain that were designed to keep us safe enables these viciously effective attention tactics to succeed.

The science of attention is even more concerning when combined with big data. Facebook experimented with the effect of news feeds on readers’ moods, studying whether a steady diet of bad news might result in less positive posts from readers. It does.

Even in this new information environment, it might be tempting to say ‘so what?’. To some, it sounds like expected social evolution with little impact on national security. Unfortunately, the manipulation and targeted use of information is creating threats to democracy that are just as real as – and perhaps more dangerous than – military threats.
For modern democracies like the US and UK, conventional military aggression is not an existential threat. Kinetic wars are fought abroad and while significant interests may be at stake, the existence of the state is not threatened. By contrast, information aggression strikes at the very heart of democracy, challenging it in ways that encourage anti-democratic, authoritarian responses. If democracies succumb to that temptation, even if the state survives, it might be unrecognisable. The ability of information-capable adversaries to promote narratives that exploit social division, strategically target information, and selectively manipulate the truth is the 21st century’s most credible threat to democracy.

Not many workable ideas have been put forward to address the information exploitation challenge. Democratic populations are rightly nervous about limitations on free speech, and crafting laws that are both broad enough to be effective and narrow enough to be lawful is a struggle. Besides, when the state acts to prevent certain speech it can create a perception that the government is promoting a particular narrative. The idea that ‘elites’ are dictating the correct way to think and believe can increase the credibility of divisive, nationalist narratives. Telling people how to think and what to believe is counterproductive.

While the challenges have made government efforts nonexistent or ineffective, tech companies have acted to filter speech on social media platforms. Facebook, Google, Twitter and others have blocked or taken down content determined to be hateful, dangerous, or otherwise inappropriate. Facing some of the same challenges governments do in trying to draw a line between appropriate and inappropriate speech, these companies have been cautious, but still create controversy. Facebook’s human curators were accused of political bias, so it turned to algorithms. The algorithms must be programmed to make objective assessments of subjective material, which turns out to be remarkably difficult.

The information situation democracies now face was decades in the making and there are no quick solutions. The answer is to have better educated, more critically thinking citizens. It will take years to make meaningful changes this way. To be able to consume information in an informed manner requires education in logical reasoning and critical thinking, but teaching these skills in the abstract is fundamentally different than forcing a single narrative. Any solution must take into account that citizens have the right to think for themselves. The point is not to convince people to draw specific conclusions. It is rather to teach them how to digest academic literature, read scientific studies, analyse arguments and recognise when information might be fabricated or distorted so they can make judgements based on facts rather than falsehoods.

Finland has started a programme in its schools to promote these ideas, but it is too early to measure its success. Education reforms are the long-term solution, but it would be useful to do something now, as well. Some specific issues can be addressed quickly with legal solutions. Three ways law could help are: barring illegitimate sponsors of information; prohibiting the artificial amplification of information; and banning the deceptive manipulation of images/visuals/audio (sometimes referred to as ‘deep fakes’). These are addressed in more detail below.

States should be barred from sponsoring political adverts in other states. Russia sponsored troll farms to weigh in anonymously on national political discourse in the US leading up to the 2016 presidential election, and in the UK during the Brexit campaign. In both cases, the foreign information campaign increased social division and strife. State-sponsored interference in national dialogue is inappropriate. National law and policy should focus on discovering and punishing states – not just individuals – for this type of behaviour, which also violates the principle of nonintervention, a fundamental tenet of international law.

Any specific area of concern is the artificial amplification of information. It would be unduly intrusive on personal rights to try and prevent individuals from forwarding or ‘liking’ social media posts, even if hateful or unprovable. It is a different matter when a post goes viral because it is artificially made popular by the use of bots or fake social media accounts. While it can be difficult to sort out which social media accounts are legitimate and which are not, having sufficient laws in place to punish artificial amplification when it is discovered would be helpful.

Finally, states should consider making it unlawful to engage in the creation of ‘deep fakes’. This technology has already caused real harm to individuals and companies, and it serves no apparently useful social purpose beyond entertainment. As the technology continues to improve, it will create increasing challenges. The key policy aspect will be distinguishing between harmless or entertainment-centred deep fakes and those created to deceive maliciously. For example, Carrie Fisher appearing in Star Wars movies after her death is an acceptable use of deep fake technology, but a faked corporate executive ordering a fraudulent money transfer is not.

Cyber-enabled information operations are a threat to the well-being of free states. For democracies to endure, they will have to come to grips with the modern information environment. Education for more savvy citizens might be the most important, and can eventually guard against adversaries using freedom of speech to weaken the very democracy that made it possible in the first place. In the short term, the three law-based proposals set out here could help buy the time needed for the further development of critical thinking skills to take hold.

Gary Brown is a Senior Associate Fellow at RUSI and Professor of Cyber Law at the College of Information and Cyberspace, National Defense University, Washington, DC.

The views expressed in this article are the author’s, and do not represent those of RUSI or any other institution.

The views and opinions expressed in this article do not necessarily reflect the official policy opinion of the Department of Defense, or any agency of the US Government.