Modern
PROPAGANDA

A most exquisite and indispensable fifth-generation warfare tool

By **JOSEPH VANN**, Marshall Center | PHOTOS BY THE ASSOCIATED PRESS

The art of propaganda is in the midst of a phenomenal revolution that few appreciate. We are witnessing an evolution in the sophistication of propaganda that is practically unfathomable. Making matters worse, there is no single vantage point from which to observe and assess its effects. It can be argued that the propaganda produced in the first two decades of the 21st century has evolved the art form beyond anything previously seen. Simply put, propaganda now represents one of the most formidable weapons in the arsenal of statecraft.

Although propaganda has always existed, today's campaigns represent one of the most sophisticated and underappreciated threats to the national security of countries. Detailing this threat across civil society is difficult because it is extremely hard to define and harder still to provide a strategic perspective that resonates with the public. To simplistically frame the nature of modern propaganda, a brief scene-setter is required to convey why modern propaganda needs to be appreciated as a critical national security concern. What we may fail to appreciate, however, is the elevated role and importance that modern propaganda techniques will play in defining great power competition and setting the conditions for future conflict.

With great theoretical energy, strategists have examined and developed military concepts over the ages. Much of the energy has been devoted to the ultimate, kinetic end of the spectrum of war. Over the ages, we have been showered with an endless supply of quotes from notable military figures and scholars that define the art of warfare from the gritty business of close-quarter killing, to the surreal and clinical dispensing of threats using precision weapons launched from unmanned aerial vehicles thousands of kilometers from their ground-based pilots. What is missing and most needed in today's complex world of globalization and maligned state actors is a dedicated focus on the extreme left-of-center,

This building in St. Petersburg is believed to house a "troll factory." Russia employs an army of trolls to target political enemies.

pre-conflict phases of statecraft (left-of-center referring to all activities, on a spectrum of conflict, prior to actual conflict). This is the most fertile ground for propaganda to flourish.

A basis for understanding developments in modern propaganda can be drawn by comparing it to the concepts of the Revolution in Military Affairs (RMA) that informed our understanding of advances in military technology and practices. Propaganda has been going through its own revolution. To inform our understanding of the current revolutionary stage of modern propaganda, it is helpful to make parallels with one of the most important RMA shifts in modern times, known as network-centric warfare. Although its initial debut in the late 1990s was somewhat dampened by the tactical emphasis and requirements of the post-9/11 global war on terror, network-centric warfare has continued to develop, albeit with amorphous properties. The same holds true for propaganda.

Network-centric warfare shifted our thinking away from platform-centric thinking to viewing the threat environment as networks consisting of actors that are constantly evolving and adapting in response to conditions. The network-centric warfare approach was envisioned as a better way to leverage new technology by networking together a "system of systems." This was a new form of task organizing to achieve interoperability and better performance in delivering kinetic solutions. Minus the end state of delivering kinetic solutions, modern propaganda is a nearly perfect example of network-centric warfare and a major tool when it comes to fifth-generation warfare.

A tweet posted by the Czech Republic's Center Against Terrorism and Hybrid Threats shows what the unit claims was an attempt to spread disinformation in Prague.

Though the concepts and definitions that shape our understanding of fifth-generation warfare are imprecise and evolving, it should be viewed as a continuation in the RMA. Presently envisioned, fifth-generation warfare combines the selective employment of traditional warfighting capabilities enabled by advances in network-centric warfare and, in particular, information technologies. The fifth-generation warfare world will be skewed toward gaining greater access to time-sensitive information and to realizing advantages in information dominance for improved decision-making. In this regard, modern propaganda is taking on a much greater role in the left-of-center realm of statecraft.

Following almost an exact parallel to the way network-centric warfare evolved, modern propaganda has become highly net-centric. During the Cold War, political boundaries were clearly defined, and propaganda attribution could be associated with a limited number of well-known print media and broadcast channels used to disseminate propaganda. Messages from these sources were immediately viewed with deserved skepticism. Today it is very different because there is no agreed-upon adversary that
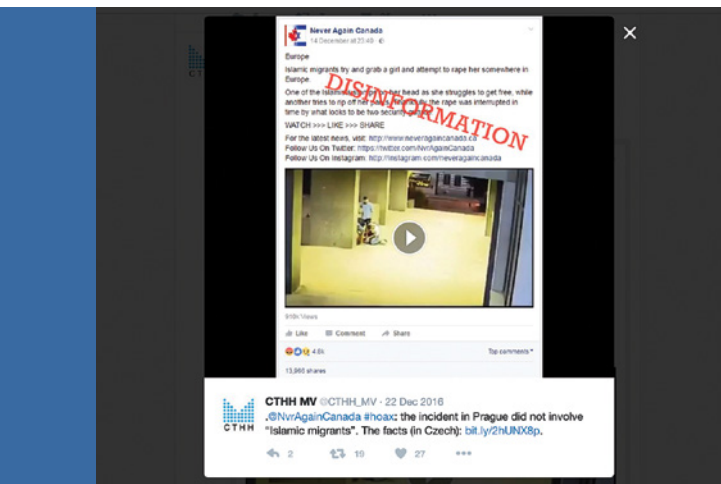
unites populations. Our sense of what threatens us differs from country to country and throughout societies. Lacking a defined threat, our collective defenses against propaganda have been fragmented and universally downgraded.

Enter "new media," a nearly perfect analogue to network-centric warfare's "system of systems" concept. In this context, new media refers to the ability to deliver and share information using various forms of technology. Social media platforms such as Facebook, YouTube, WhatsApp, Messenger, WeChat, Instagram, QQ, Tumblr, Qzone, TikTok and Twitter are just a small sample of some of the most popular interactive platforms making up new media. Unlike old media, consisting of noninteractive media such as magazines, newspapers and television, new media is a modern phenomenon. It connects our globalized populations in ways never imagined during the Cold War. The size and scale of new media is impressive. Consisting of resilient, redundant, self-healing, high-performing networks that are carefully monitored to deliver content — not inspect content. While serving to bring good into the world, new media provides immeasurable means to deliver propaganda and shape public opinion. Nefarious propaganda activities conducted by recognized adversaries exploit civilian new media platforms that are relatively free from government oversight. The ease by which adversaries can create internet personas to effectively mask their identity and their malign propaganda activities adds to the challenge.

Senior leaders and policymakers are quick to confess to being technically illiterate about new media technology. While great users of social media, and by extension new media, their knowledge of the extent to which the technology can be manipulated for nefarious purposes is acutely scant. In aggregate, senior leaders underappreciate both the threat and exploitable vulnerabilities inherent in new media platforms.

New media platforms are also unique in the way they enable modern propaganda methodologies to target audiences with precision, brute force, or a mix of both. Depending on the objective, modern propagandists can employ a variety of social media platforms differently to reinforce messages. However, like network-centric warfare, modern propaganda is not platform-centric. If one new media platform underperforms or fails, others are either brought into play or are already in play to fill the void. In this regard, modern propaganda is highly network-centric in the way technologies and methodologies are used and adapted to exploit conditions. Modern propaganda effectively uses a system-of-systems construct.

A modern propaganda strategy can be expected to be carried out very similarly to a military campaign plan. A notional example would start with determining a desired end state and conducting reconnaissance to determine the most exploitable vulnerabilities. This approach would be a version of the military phase of preparation of the battlespace. Free social media apps with exploitable features

may be used to gain access to needed targeting information. Or, a shell company can be established to purchase targeting information from big data companies that sell information collected by monitoring the online activities of internet users. These companies determine user profiles and habits with great specificity and market the information to paying customers. User profiles can reveal preferences for types of news stories and media outlets, and this may provide enough information to target, divide and influence segments of the population based on assessed political affiliations.

Aggregated data from mouse-cursor activity may offer insights as to the levels of education and search preferences of users. This information is highly precise and automatically generated by big data collectors. Big data is neither static nor bounded by any particular field. If activity takes place on the web, it is captured. Targeting doesn't need to be focused only on the political spectrum. By carefully making use of information mined from big data and choreographing modern propaganda techniques with new media platforms, adversaries can target users across the social spectrum. Based on a target's social media profile and regular use of search engines, adversaries can target audiences no matter how they surf the internet. If you are connected, you are vulnerable.

Once reconnaissance provides enough information, the battle plan can take shape and operations can be launched. Depending on the country, the next phase would be the employment of cyber warriors. Using a military analogy and depending on the tasks, the attackers would range from a platoon, company, battalion to even a division level in terms of numbers. Options may include an orchestrated "astroturfing" campaign (posting bogus comments on websites) designed to change public perception in a desired way. This may be enough to realize the objective. If not, it may require a coordinated attack. Examples would be to employ a "sock puppet" operation (concocting fake online identities) to create a false narrative followed up with larger numbers of sock puppet commenters to substantiate the false narrative with supporting commentary.

If more persuasion is needed, a combination of "trolls" and "concern trolls" might post inflammatory material that can be used in tandem and brought into play to add a new dimension that sows discord and excites emotions. Depending on the desired effects, the propagandist can raise the stakes by using memes to grab or distract attention. In this scenario, only a limited number of tactics are mentioned. In a real, modern propaganda campaign plan, the number of tactics could easily be tenfold greater. Once designed, much of this activity becomes automated, allowing for greater reach and dissemination without the need to monitor every interaction. If properly choreographed and executed by a highly trained cyber army, the impact can be devastating. We are already witnessing this being practiced by state and nonstate actors. It would be irresponsible to not expect and plan for this type of activity during steady-state operations and the nonkinetic shaping phases of fifth-generation warfare.

In conclusion, modern propaganda has evolved into an exquisite and serious weapon that represents a new national security threat. It will likely become the weapon of choice for the shaping phases of statecraft and the preparation of the battlefield. Pre-conflict cyber warfare will be weighted toward new propaganda methods to create disharmony and influence opinion well before the public realizes anything is amiss. Countries will invest more in growing their numbers of cyber warriors because they are affordable and cost-effective and need little in the way of special military equipment, uniforms or facilities. New media platforms will continue to be exploitable and serve as ideal delivery platforms. The amorphous nature of the internet and associated technologies will continue to make attribution of nefarious activities challenging. The commercial nature of the internet makes governance and self-policing problematic. In democratic countries, new media's profit-driven endeavors are relatively free from intrusive government oversight.

This may change, but it is likely to be slow in coming because of concerns that government regulations will overreach into the privacy and free speech domains. Leaders and policymakers need to recognize modern propaganda for what it is — information warfare. Finally, to limit our vulnerabilities to modern propaganda, we need to better recognize our mirror-imaging tendencies when assessing adversaries. Our biggest vulnerability is our naiveté. The fact that we wouldn't do something that breaks ethical standards doesn't mean that our adversaries will refrain from doing so. We have more than enough evidence of maligned modern propaganda activities to paint a clear and unmistakable picture of what we can expect in the future. As we learned in the aftermath of 9/11, there is a terrible price to pay when you fail to imagine. □