

per Concordiam

Journal of European Security and Defense Issues

■ **LIVING IN A POST-TRUTH WORLD**

Russia's strategy to divide and conquer

■ **HARNESSING THE POWER OF MEMES**

The viral messages that pack a big punch

■ **TARGETING THE PUBLIC'S EMOTIONS**

Social media becomes an indispensable weapon

■ **CURBING THE SPREAD OF FAKE NEWS**

Does blockchain technology offer an antidote?

PLUS

The many obstacles overcome by North Macedonia
Lessons from Serbia on emergency communications
Disinformation and Montenegro's NATO accession



STRATEGIC COMMUNICATIONS

Winning the Information War



10 **The Age of Post-Truth**

By Dr. Ralf Roloff and Dr. Pál Dunay, College of International and Security Studies, George C. Marshall European Center for Security Studies

Communications challenges on Europe's eastern flank.

20 **The Power of Memes**

By Maj. Matthew Schlepner, U.S. Army

Why NATO's member states should embrace the potent digital tool.

26 **Commanding the Trend**

By Lt. Col. Jarred Prier, U.S. Air Force

Social media as information warfare.

36 **Listening Without Prejudice**

By Maj. (Ret.) Susan N. Osembo, Kenya Ministry of Defence

Using blockchain technology to counter propaganda in a 'fake news' era.

42 **A Difficult Passage**

By Dr. Bekim Maksuti and Dr. Sebastian von Münchow

North Macedonia's turn to the West.

46 **Communicating in a Crisis**

By Želimir Kešetović, University of Belgrade, faculty of security studies; Predrag Marić, Republic of Serbia, assistant minister of interior; and Vladimir Ninković, University of Belgrade, faculty of security studies

Lessons from the May Floods in Serbia.

54 **Montenegro's Media War**

By Marija Blagojević, advisor to the president of the Parliament of Montenegro

False narratives defined the battle over NATO membership.

60 **The Fog of Modern Warfare**

By Vanya Denevska, parliamentary secretary, Bulgarian Ministry of Defence

Russia's disinformation campaign in Bulgaria.



departments

in every issue

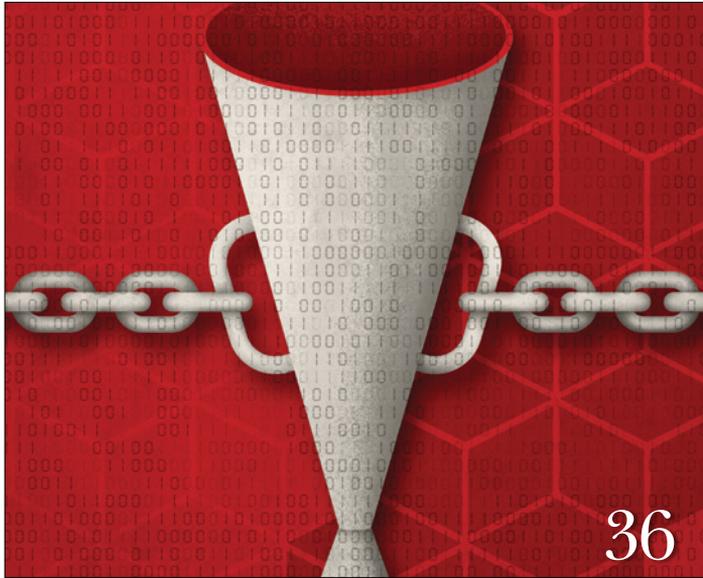
- 4 DIRECTOR'S LETTER
- 5 CONTRIBUTORS
- 7 VIEWPOINT
- 66 CALENDAR

BOOK REVIEW

64 *LikeWar: The Weaponization of Social Media*

Reviewed by: Patrick Swan, per Concordiam contributor

The stakes are perilous for countries — and people — who neglect to address this alternative domain of warfare.



on the cover:

Defense planning must now incorporate communications strategies.
PER CONCORDIAM ILLUSTRATION



GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES

Welcome to the 38th issue of *per Concordiam*. In this edition, we delve into strategic communications in the era of social media, “fake news” and constant technological change. It is critical these days for democratic states to understand the threat posed by malevolent actors who weaponize communications technology. Strategies must be adopted to counter false narratives and to keep the public’s trust in government institutions. Failing to effectively respond to these attacks can sow chaos in societies.

Inside this issue, Lt. Col. Jarred Prier of the U.S. Air Force looks at social media and how it has become a major component of strategic communications for the West’s adversaries and how it is used to divide and weaken democratic societies. Russia, a master at disinformation since the days of the Soviet Union, has become adept at using new media to target online social networks.

Dr. Ralf Roloff and Dr. Pál Dunay, professors at the Marshall Center, examine strategic communications in the post-truth era. Hostile actors spread “fake news” and distorted or out-of-context information to manipulate target audiences in ways that are difficult for democratic societies to counter. Dr. Bekim Maksuti, deputy defense minister of North Macedonia, and Marija Blagojević, advisor to the president of the Parliament of Montenegro, relate how their countries are countering geopolitical disputes and Russian interference in their efforts to join NATO and the European Union. In our Viewpoint feature, Marshall Center professor Joseph Vann provides an overview of modern propaganda and the threat it poses to free nations.

Among the other authors in this edition are Željimir Kešetović, Predrag Marić and Vladimir Ninković, who evaluate Serbia’s emergency response to widespread flooding in May 2014, Vanya Denevska, who explains Russia’s disinformation campaign in Bulgaria, and U.S. Army Maj. Matthew Schlepuner, who focuses on memes and their power in the new information environment. Susan N. Osembo, who served in the Kenyan Ministry of Defence, examines how blockchain technology can be used to fight propaganda.

As always, we at the Marshall Center welcome comments and perspective on these topics and will include your responses in future editions. Please feel free to contact us at editor@perconcordiam.org

Sincerely,

Keith W. Dayton
Director



Keith W. Dayton

*Director, George C. Marshall
European Center for Security Studies*

Keith W. Dayton retired as a Lieutenant General from the U.S. Army in late 2010 after more than 40 years of service. His last assignment on active duty was as U.S. Security Coordinator to Israel and the Palestinian Authority in Jerusalem. An artillery officer by training, he also has served as politico-military staff officer for the Army in Washington, D.C., and U.S. defense attaché in Russia. He worked as director of the Iraqi Survey Group for Operation Iraqi Freedom in Iraq. He earned a Senior Service College Fellowship to Harvard University and served as the Senior Army Fellow on the Council on Foreign Relations in New York. Gen. Dayton has a bachelor’s degree in history from the College of William and Mary, a master’s degree in history from Cambridge University and another in international relations from the University of Southern California.



Marija Blagojević is an advisor to the president of the Parliament of Montenegro. She has been a member of the main board of the Social Democrats of Montenegro, a Parliament councilor in Podgorica, and was a founder of the Women's Political Network of Montenegro. She is a graduate of the University of Belgrade.



Vanya Denevska is parliamentary secretary of the Ministry of Defence of Bulgaria. She is a liaison between the National Assembly minister, parliamentary groups, National Assembly committees and political parties. She is an expert in the formulation and coordination of security and defense policy, helping to review and assess the government's compliance with the laws and regulations governing those policies.



Dr. Pál Dunay is professor of NATO and European Security Issues at the Marshall Center and academic advisor of its Program on Applied Security Studies, European Security Seminar-East, and Senior Executive Summary courses. He was director of the Organization for Security and Co-operation in Europe Academy from 2014 to 2016, course director of the International Training Course in Security Policy at the Geneva Centre for Security Policy from 1996 to 2004 and from 2007 to 2014.



Dr. Bekim Maksuti is deputy minister of defense of the Republic of North Macedonia and a university lecturer on security and defense issues. He earned his master's degree and Ph.D. from the Institute for Security, Defense and Peace Studies at the Ss. Cyril and Methodius University in Skopje. He has served as an assistant professor at the University of Tetovo and as a military officer in the Army of North Macedonia.



Maj. (Ret.) Susan N. Osembo served in the Kenyan Army and is a certified security management professional and alumna of Durham University in England, where she graduated with a master's degree in risk management. She attended the Marshall Center's Transatlantic Civil Security course and specializes in risk management and the protection of critical national infrastructure.



Lt. Col. Jarred Prier, U.S. Air Force, is commander of the 20th Bomb Squadron, Barksdale Air Force Base, Louisiana. He completed a U.S. Air Force fellowship at the Walsh School of Foreign Service at Georgetown University and earned a master's degree from the School of Advanced Air and Space Studies at Air University, Maxwell Air Force Base, Alabama. Prier also holds a master of science degree in international relations from Troy University, Alabama.



Dr. Ralf Roloff is deputy dean for resident programs at the Marshall Center and a professor (apl) at the Universität der Bundeswehr München. He was the senior German professor at the College of International Security Studies at the Marshall Center from 2003 to 2018 and was director of the European Security Seminar from 2015 to 2018. He has been director of the Master in International Security Studies Program at the Marshall Center since 2010.



Maj. Matthew Schleupner serves as a U.S. Army Foreign Area Officer with a focus on Russia and Eastern Europe. He holds a master's degree in international policy from Johns Hopkins School of Advanced International Studies, a master's degree in political science from the University of Toledo, and a law degree from Western Michigan University's School of Law.



Joseph Vann is a professor of transnational security studies and director of the Marshall Center's Program on Countering Transnational Organized Crime. Professor Vann's expertise lies in addressing transnational security challenges, developing national security strategies, and other strategy approaches to solving national security threats. He has more than 35 years of government service.



Dr. Sebastian von Münchow is a lecturer on security studies at the Marshall Center. He studied law at the Free University of Berlin, the Université de Lausanne and the Christian-Albrechts-University Kiel and earned a doctorate in international relations from the University of Vienna. He has worked for the Organization for Security and Co-operation in Europe in Bosnia and Herzegovina and in Kosovo.

**Strategic
Communications**

Volume 10, Issue 2, 2020

Contributing Editors

Dr. Sebastian von Münchow
Professor Joseph Vann

**George C. Marshall
European Center for
Security Studies**

Leadership

Keith W. Dayton
Director

Dieter E. Bareihs
U.S. Deputy Director

Helmut Dotzler
German Deputy Director

Marshall Center

The George C. Marshall European Center for Security Studies is a German-American partnership founded in 1993. The center promotes dialogue and understanding between European, Eurasian, North American and other nations. The theme of its resident courses and outreach events: Most 21st century security challenges require international, interagency and interdisciplinary response and cooperation.

Contact Us:

per Concordiam editors

Marshall Center
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
editor@perconcordiam.org

per Concordiam is a professional journal published quarterly by the U.S. European Command and the George C. Marshall European Center for Security Studies that addresses defense and security issues in Europe and Eurasia for military and security practitioners and experts. Opinions expressed in this journal do not necessarily represent the policies or points of view of these institutions or of any other agency of the German or United States governments. Opinions expressed in articles written by contributors represent those of the author only. The secretary of defense determined that publication of this journal is necessary for conducting public business as required of the U.S. Department of Defense by law.

ISSN 2166-322X (print)
ISSN 2166-3238 (online)

A DOUBLE DOSE ONLINE

Read current and past issues of *per Concordiam*

<https://perconcordiam.com>

Submit articles, feedback and subscription requests to the Marshall Center at: editor@perconcordiam.org



Get the freshest *global security news* updated weekly:

transnational
weekly
<https://www.marshallcenter.org>



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.

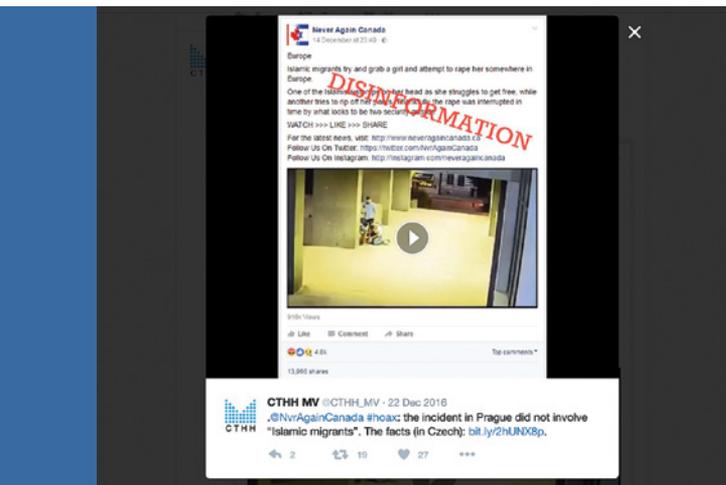
unites populations. Our sense of what threatens us differs from country to country and throughout societies. Lacking a defined threat, our collective defenses against propaganda have been fragmented and universally downgraded.

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



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

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.

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. □



PER CONCORDIAM ILLUSTRATION

THE AGE OF POST-TRUTH

COMMUNICATIONS CHALLENGES ON EUROPE'S EASTERN FLANK

By **Dr. Ralf Roloff** and **Dr. Pál Dunay**

College of International and Security Studies, George C. Marshall European Center for Security Studies

PHOTOS BY AFP/GETTY IMAGES

States cannot enjoy great power status unless they act and operate across a complex power base that includes elements such as military power, a large and competitive economy, innovation, a relatively youthful and educated population, and a model of government that is aspired to by other states. Other factors, such as a language spoken in other countries and cultures, can also be beneficial. It is also essential that the country be able to reach out to others and that its messages carry credibility. A large part of the former Soviet Union remains a community in many ways, with widely used, shared social media platforms and shared internet providers. However, a state that does not invest in a broad power spectrum cannot sit at the “high table.”

Smart states can reallocate resources from their strengths to their weaknesses, called horizontal strengthening. They may also allocate resources to areas of strength to make them even stronger, known as vertical strengthening. For example, China has for some time been the production hub of world industry, but it has successfully

diversified its power base and developed a performant military to become the second largest spender on defense and has also promoted Chinese culture and language.

Russia's predecessor, the Soviet Union, spread an ideology that was not at all credible. Its propaganda was successful only where it was backed by the force of arms.

Russia has major strengths, such as possessing the world's largest arsenal of nuclear weapons, its large land mass, its large oil and gas production, large armed forces, a large and well-trained diplomatic and intelligence service, and a sphere of influence in the former Soviet republics and to some extent elsewhere, such as Syria and the Western Balkans.

Russia's predecessor, the Soviet Union, spread an ideology that was not at all credible. Its propaganda was successful only where it was backed by the force of arms. As former U.S. Ambassador to the Soviet Union George Kennan once noted: "Everyone imposes his own system as far as his army can reach. It cannot be otherwise." Russia, which tripled its total gross domestic product between 1999 and 2013, has used its resources to diversify its activities to areas with perceived weaknesses, compensating for the flaws of its foreign policy outreach. Since 2014, an assertive strategic international communications program has formed part and parcel of Russia's grand (and military) strategy.

It consists of four notable aspects:

1. Russia's external relations can be characterized as pragmatic, in sharp contrast with those of the Soviet Union. This gives more opportunity to communicate various messages without having to adhere to a set of incredible ideological tenets.
2. Strategic communications have been strongly integrated within a revised defense doctrine that has created the impression that it is more confrontation than cooperation. This was unfortunate and alerted Russia's partners in Europe and North America.
3. Strategic communications are on the visible end of a political process that includes a broader array of measures and activities to which the world at large must be prepared to respond.
4. Russia's leadership, due to the background of several of its members, including President Vladimir Putin, favors a more assertive campaign to communicate the country's messages to the world.

Moscow has embraced active measures, the establishment and financing of front organizations, and psychological operations, including generating hate, fear and hope.

A SERIOUS CHALLENGE

The use of strategic communications and their influence is not easy to measure. Russia wants to influence its environment. In this sense, Moscow is not different from any other state. However, its ambitious and assertive posture on the international stage is different. Moscow has embraced active measures, the establishment and financing of front organizations, and psychological operations, including generating hate, fear and hope. Russia has lately also actively engaged in a very broad spectrum of communications means and methods.

Moscow relies on various media sources tailored to different audiences. Cost efficiency is important. Russia gives preference to electronic media, including social media and television. Russian national television is widely available throughout the states of the former Soviet Union, including in the Baltic states. Its influence is noticeable when we look at opinion polls reflecting

Chinese soldiers carry the flags of the Communist Party, the state, and the People's Liberation Army during a military parade in China's northern Inner Mongolia region. China is diversifying its power base, increasing its defense spending, and promoting Chinese culture and language.





sympathy with Russia and the views of the Russian state, which is regularly greater where Russian programming is available. Russian television, first and foremost channels such as Perviy Kanal (Channel One) and RTR Planeta, have the most influence in Russia's immediate neighborhood. Russia also uses international television broadcasting in various foreign languages. Established and generously funded by the Russian state, Russia Today — or RT as it has been renamed — is now available in Arabic, English, French, German and Spanish and is available on satellite and cable packages. RT also has an internet site in all these languages and Russian.

RT is internationally notorious for spreading propaganda and often fake news. French President Emmanuel Macron even called Russian state-backed media outlets RT and Sputnik “agents of influence” that spread falsehoods about him throughout his election campaign — during a press conference with Putin no less. Russia presents this activity more innocently, emphasizing RT's contribution to improving the country's image in the world. But international concerns are not so much about RT's broadcasting, per se, but about it being used as a platform to interfere in the internal politics of other states in combination with other, often more covert measures — an amalgamation of Russian power potential of which television programming is only a part. The question is whether media is a central element or complementary to a package of more clandestine means — a question underlined by RT's relatively unimpressive viewership numbers. For instance, in the United Kingdom, RT has

French President Emmanuel Macron, right, at a press conference with Russian President Vladimir Putin at the Versailles Palace near Paris in 2017. Macron called Russian-run media outlets RT and Sputnik “agents of influence” that spread falsehoods.

never been watched by more than 4,300 households, indicating it is not a source of major influence. Russia also uses internet platforms such as Sputnik (including Sputnik news) and various social media websites to project certain viewpoints. When these sites are compromised or their “shelf lives” expire, they simply disappear and are replaced with new, more credible ones.

The unity of its own messaging, versus divided views in the West, gives Russia an asymmetric advantage for which it is difficult for the West to compensate.

In print media, which has more limited influence, Russia also applies a variety of measures. These include providing sympathetic foreign journalists access to Russian leaders, as well as feeding them Russia's version of different events. Critically, Russia provides journalists



with information in many languages (and of steadily improving quality), enabling Western journalists, often pressed for time, to utilize “ready-made” information rather than investing time and energy on checking facts. Consequently, Russia’s version of the “facts” can benefit from a multiplying effect in the media of other countries.

The unity of its own messaging, versus divided views in the West, gives Russia an asymmetric advantage for which it is difficult for the West to compensate. This contributes to the impression that the West is reactive and hesitant in the face of unfriendly, or outright hostile, Russian strategic communications. In addition, information overload makes it ever more difficult to identify reliable sources of information, especially as social media has disaggregated old patterns of communication and new actors can directly reach out to the population of other countries. Similar concerns appeared in the 1980s in conjunction with satellite television.

These three factors call for attention:

1. Social media has made access more cost effective, lowering the cost of “buying” influence.
2. It is easier to send tailor-made messages.
3. Some social media networks, including widespread ones such as Facebook, facilitate the reinforcement of perceptions by preselecting messages based on what one has previously viewed. Other social media select what messages to emphasize based on which websites have been visited. This results in viewing content that reaffirms prior views, further deepening convictions.

Directors at RT, the state-run television network previously known as Russia Today, monitor video feeds in Moscow. RT is available in Arabic, English, French, German, Russian and Spanish, on satellite and cable packages, and has an internet site in multiple languages.

All of this contributes to a deepening of political division within societies.

A MULTITUDE OF PROBLEMS

The new opportunities for strategic communications involve numerous challenges that require adequate responses. However, finding the most effective responses can be difficult.

Consider:

1. Strategic communications is part of a broader political strategy, sometimes called a grand strategy, and thus its role can only be assessed in light of the relationship between the two. Do states have grand strategies? Are their strategic communications in line with and do they contribute to the grand strategy of the state, or are there discrepancies?
2. The focus of strategic communications has changed over time. Whereas in 2014 Russian strategic communications focused primarily on spreading “fake news,” it has since become more diversified and better integrated with other state activities.
3. The nature of hostile communications activities makes it difficult to react. Rather than spreading

a cohesive alternative view of events/developments, a variation that aims to undermine the still dominant — usually Western — discourse is often disseminated. In other cases, it aims to deprive the West of the monopoly of its message. It also occasionally appears as a “moving target,” often changing the message just to retain media attention.

4. Messages often combine elements of reality with falsehood. In addition, entirely factual information is presented in such a way that unrelated issues are misleadingly made to seem closely related to each other.

Russia’s grand strategy dates to the consolidation of Russian statehood following Putin’s rise to power. Its starting point is that strong statehood is Russia’s only guarantee of respect and international recognition. This is partly a reflection of recent and not so recent history. Because in the 1990s post-communist Russia was a place of chaos as it liberalized its economy and politics, and that time is therefore identified with weak statehood by Russians, a discourse is being built that arbitrarily identifies weak statehood with liberalism and as the cause of chaos. By this logic, strong statehood counters malaise; and if liberalism means weakness, then strength would come with the denial of liberalism. A thorough analysis of this precept would fundamentally disprove the truth of equating weakness with liberalism and strong statehood with its denial. However, what matters to Russia’s leadership is the perception of its people.

Although Russia’s objectives have evolved over the past two decades, some have remained largely unchanged. Russia’s grand strategy prioritizes status over achievement, making it essential to the Russian leadership to depict the country as highly successful. The need for this depiction is plausible, because ostensible political stability — including leadership stability — helps create such an impression. Domestic strength is also portrayed as power internationally (which is not unusual for many states). However, due to the uneven level of Russia’s development, its strategic communications emphasize achievements and deemphasize weaknesses. That is why it is often said that the Russian leadership plays “a weak card strongly.”

Russia’s most important international objectives are to retain its independence and political sovereignty, and to restore its international standing through power and strength. This is underlined by Russia’s belief that when it took a conciliatory attitude toward the West in the 1990s, it was not “rewarded”; on the contrary, its weakness was exploited. Russia feels justified in its more aggressive posture because of its perception of Western encroachment. Russia’s main aspiration is to be a pole in a multipolar international system. To realize this objective, Russia aims to maximize its relative power in the international system. There are limits to how much Russia can strengthen its own position, due to its limited role in the world economy and its weakness as a role model (an

important element of soft power). Therefore, according to Russia’s understanding, it must weaken other centers of power. Russia’s targets may include individual states and multinational organizations that contribute to international cohesion, including alliances. Russia applies various means to weaken states and alliances, however appropriate or proportionate they may or may not be.

Many would like to see Russia integrated into the international system and thus avoid turning Moscow into an alienated pariah or a leader of those nations that coalesce against the West-dominated international order. The question is whether internal progress within Russia can provide a foundation for such developments. The main worries relate to economic matters that are fully subordinated to politics.

Russia has failed to realize its significant potential, even within the post-Soviet space. It enjoys recognition for its symbolic leadership but is less successful in turning leadership into economic opportunity. In Kazakhstan, Chinese investments are seven to eight times larger than Russian investments. The effects of the Western sanction regime, often blamed for economic malaise by Russian leaders, are apparently more lasting than Moscow expected. Furthermore, there is a consensus among macroeconomists that the eventual lifting of sanctions would not result in increased Russian exports. Although Russia will continue to generate modest growth of about 1.5-2% per year, it will not be sufficient to keep up with the competition. According to estimates, sanctions reduce Russia’s gross domestic product growth by approximately 1.2% every year. This will not undermine Putin’s regime; however, it will make it difficult for Russia to realize its socio-economic objectives and deliver on ambitious promises. If social dissatisfaction increases, there is a danger that the regime could “tighten the screws” and further increase reliance on authoritarian measures. Furthermore, Russia insufficiently invests in human potential, including education and health care, further harming sustainability.

Russian interference varies from the disagreeable to the morally questionable, on to the illegitimate and the outright illegal.

The gap between Russia’s performance and its self-claimed status creates a situation where Moscow finds the broad array of communication means indispensable. While Russia has generally not successfully diversified its strengths, it has increased the role of communications substantially. However, the world does not have a problem with Russia’s strategic messaging, nor necessarily with its so-called fake news because such cases can be exposed



and Russia's leadership embarrassed. The problem is with the broad array of measures, ranging from untrue messages to active measures and interference in other countries' domestic processes. Further, Russian interference varies from the disagreeable to the morally questionable, on to the illegitimate and the outright illegal.

RESPONDING TO RUSSIA'S CHALLENGE

The West faces a number of sensitive asymmetries when responding to Russia, ranging from the unity of Russia's messaging against the potential disunity of Western messaging, because it must consider whether to react individually or collectively. As Russia aims to mobilize (and demobilize) public opinion with its messages, the West simply cannot stand idle. Furthermore, the West is united by values, including the freedom of expression and the press, and thus must accept, or at least tolerate, freedom of expression from other countries, including ones that pursue malign objectives with their messaging.

Modern societies are exposed to more information than ever before. We continuously receive news from a wide variety of sources, many of which are not verified regarding their content and intent. The quality and accuracy of print and mainstream electronic media content is expected to be verified. From its onset, social media has been regarded as uncontrolled and thus the most free. However, as developments have illustrated, some freedoms must be limited to safeguard the freedoms of others, and to protect the public interest. For states, it can be difficult to agree on matters such as how to protect the public without depriving it of access to information. Societies also face the problem of protecting people without resorting to censorship, but lack dedicated organizations and resources to respond to threats in a focused and time-sensitive manner. Societies are inadequately prepared to

cope with the information their members receive, and people are inadequately educated and face difficulties in selecting or deselecting the news and interpretation presented by the media. Furthermore, genuine multilingualism is an issue because most people tend to consume news in their first language, potentially creating an informational bias in favor of media content in the mother tongue of its audience. However, in several post-Soviet states, the use of the Russian language remains widespread, and in at least one, Belarus, it is actually used as a first language. This presents a challenge because Russia may have significant media influence in states ranging from Tajikistan to Ukraine. It is questionable whether administrative measures, such as removing Russian channels from cable television packages, are adequate. Such radical steps would go against the instincts of the democratically minded. However, what if two countries are in high-intensity conflict (war) and one intends to undermine the resolve of the other's society to fight? Ukraine, facing this situation with Russia, removed Russian channels with significant news and propaganda content. Moldova followed Ukraine's example with a more limited effort of removing Russian news programs. However, Russian television programs were not banned in those two countries; they remained accessible via internet and satellite and households were not prohibited from owning satellite dishes. Unwelcome exceptional circumstances may make temporary constraints necessary, such as those introduced by Ukraine and Moldova. Though less well-known, the number of available Russian television channels has also been reduced in some other former Soviet republics, such as Tajikistan. In others, such as Georgia, the demand has dropped as Russian fluency has declined, particularly among the younger generation, replaced by interest in media in English and other languages.



The West faces delicate choices beyond administrative measures. As a diverse entity, the West and its constituent states may be exposed to Russian strategic communications to different degrees and, hence, not feel compelled to react to each in the same manner. There is also some division between the United States and its European allies, most notably regarding the use of fabricated messages for active countermeasures. But there are foundational points where consensus prevails: Credibility of public electronic media and trust in the veracity of government communications are essential preconditions. In those countries where people generally trust their government and do not have reason to often doubt its words and deeds, it is more difficult to sow discord between the government and the governed. This point is well illustrated by RT's failure to gain influence in Sweden, where efforts have been made to improve media literacy among the youth, develop resilience and address fake news in a timely manner.

There is also a complex link between the existence of a deeply divided political class and vulnerability to external political influence. When there is a broad political consensus regarding a country's socio-political and socio-economic foundations and its international alignment, there is less room for external interference. Conversely, deep-seated internal divisions, societal cleavages and an unsettled international orientation make a country more vulnerable to the malign influence of external actors. For example, building social cohesion has been unsuccessful in some Western Balkans states. In some cases, the lack of success has ethnic grounds and historic roots. In Bosnia and Herzegovina, Russia is backing the Bosnian Serbs to maintain internal division and put pressure on the Bosnian state. In Serbia, Russia manifests Orthodox Christianity as a civilizational foundation, and in Croatia it appeals to the solidarity of Slavic nations. In Northern Macedonia, deeply divided

Opposite: Estonian riot police respond to a protest near a monument to World War II Soviet soldiers in Tallinn in 2007. Plans to remove the monument brought a strong rebuke from Moscow, inflaming internal divisions within the country.

Center: Lithuania welcomes several hundred German troops in 2017 as part of a multinational NATO battalion to deter Russia. Fake news accounts falsely accused German troops of raping a Lithuanian woman.

Above: Workers in biohazard suits affix a tent over the bench in Salisbury, England, where Russian-British double-agent Sergei Skripal and his daughter were found stricken by a nerve agent in what British authorities called a "brazen and reckless" murder attempt by Russian agents.

internal politics and mutually exclusive agendas have provided Russia with the opportunity to interfere.

Communications are the most visible of an array of Russian influence tools, supported by less visible tools ranging from diplomacy and intelligence to financial credits and investment. A corrupt establishment makes a country more vulnerable to outside influence, particularly in such small and poor countries where corrupting leaders is relatively inexpensive. When the leadership of a country is dependent on Russia, Russia usually pays less attention to achieving and maintaining influence in its media space. Hungary is an example where the multi-channel dependency of the government, complemented by remarkable political stability, makes focusing on bottom-up influence in the society redundant. Russia is satisfied to use Hungarian proxy media channels to widen its influence there. To prevent dependence on Russia, a state needs resilience, which requires good governance (credibility, communication), national unity and low levels of corruption. Media literacy in the society — being able to tell the difference between truth and distorted messages — is an essential component of resilience.

Russia's attempts to increase its influence have had a rather limited effect in some places, many of them in the Nordic and Baltic regions, where Russia has returned to more traditional means of influence. In the Nordic, Russia uses public policy channels to warn the Finnish and Swedish governments against joining NATO. In the Baltics, the situation is more complex due to the existence of large — though shrinking — ethnic Russian minorities. However, in states that have demonstrated proactive determination and where there is a tradition of good governance, such as Estonia — with its large Russian-speaking population influenced by Russian media — Russian influence attempts have become more nuanced. But there is little doubt that dedicated Russian institutions and personnel are waiting for their opportunity.

In recent years, the West has had the opportunity to learn more about how Russian strategic messaging operates by viewing spikes in Russian messaging during relevant events. The first such event was the 2007 crisis with Estonia, when Estonian authorities removed a Soviet World War II monument from the Tallinn city center. Demonstrations by approximately 1% of the city's population were skillfully presented by Russia as much larger and were a prelude to Russia's first large-scale cyber attack. In 2016, the so-called Lisa case was exploited by Russian propaganda when a 13-year-old Russian-German girl went missing and falsely claimed, upon her return, that she was abducted and raped by migrants to avoid being punished. Russian foreign minister Sergey Lavrov called her "Our Lisa," even after the truth had been revealed. In 2017, German forces deployed on the NATO mission in Lithuania, were falsely accused of raping a local woman with the seeming intention of driving a wedge between the German troops and the local population. And in the spring of 2018, Sergei Skripal, a former Russian-British double agent, and his daughter were poisoned with a nerve agent in Salisbury, in the U.K., where they lived in exile. The British and their allies found the evidence convincing that Russia was behind the assassination attempt. The Russian media tried to undermine the British accusations by raising doubts about the provenance of the Novichuk nerve agent and trying to gain access to the crime scene for Russian experts while simultaneously fighting examination by the Organization for the Prohibition of Chemical Weapons. They also asserted that Russian operatives would not have botched the job and left survivors. Rapid dissemination of a large number of varying stories produced a smokescreen intended to obscure what had really happened. In the end, Russia succeeded in confusing opinions (except within the expert community) until much of the public lost interest. Later, however, due to the poor organization of Russian military intelligence, the case was more fully revealed and the results publicized by the British investigative news organization Bellingcat.

What can be learned from these four cases? First, a country's own media must be constantly monitored to be

able to respond to an attack in a timely manner. Second, various hostile activities are often linked. Consequently, when hostile activities begin in one area or via one channel, there is potential spillover. Third, a strategic opponent's messaging must be countered in a timely manner. Fourth, it is essential to remain factual with messaging and countermessaging and not to reciprocate an opponent's lies. Fifth, it must be determined whether it is worth revealing one's own sources and capabilities to convincingly attribute a strategic communications attack to another state. Sixth, the entire exchange must be made transparent to the public — which consists of domestic and international audiences, including the adversary's citizens — to establish that you are acting honestly, ethically and in accordance with the law. Seventh, if communications are simplified to contrasting two rival versions of the facts, the audience will remain divided, which necessitates presenting a message that is reinforced by a superior set of norms, principles and values.

Even bearing in mind current divisions in the West, collective reaction to hostile strategic communication challenges is preferable to individual national responses. This is true of the Skripal poisoning case, in which the British reaction was supported by a massive demonstration of allied solidarity. When a national reaction is necessary due to urgency, as when false rumors were spread about German troops in Lithuania, international institutions can still play a role, though it may have to remain complementary and confined to those areas where they provide genuine comparative advantage. International organizations are often too hesitant in divisive matters and Russia attempts to prevent the establishment of unity in Western institutions.

Both NATO and the European Union have addressed matters of strategic communications under the fast-changing conditions of recent years. Their activity has reflected the potential of the institutions, but also the limits of accord among the member states. NATO has enhanced its capacity to collect and analyze information. It established its Strategic Communications Centre of Excellence in Riga, Latvia, and together with the EU, the European Centre of Excellence for Countering Hybrid Threats in Helsinki, Finland — the first such institution beyond NATO's territory. In Riga, the focus is on in-depth research of communications and the development of methodology for member states. The Alliance does not have large amounts of resources to allocate to this activity and, hence, member state commitment is essential to countering the Russian challenge. NATO has also become more active on the web, setting the record straight regarding Russian misinformation about the Alliance and its policies, and contrasting it with facts.

NATO's position, presented as a rebuttal and in contrast to Russia's, makes it more compelling. The objective is partly to make the Russian media understand that it cannot spread falsehoods without response. NATO also asks such media to correct false stories. While it is

not the prime objective, there is a “name-and-shame” element because a media source that regularly presents counterfactual information and biased assessments will be exposed by Alliance public diplomacy. In one such case, U.S. Gen. Philip Breedlove, then NATO supreme allied commander Europe, declassified satellite imagery to clearly document Russia’s military presence in Ukraine’s Donbas region. NATO’s objective is to present its messages credibly and accurately, avoiding counterpropaganda and clearly contradicting Russia’s disinformation.

Russia ... has taken advantage of its ability to project a unified message, of the West’s commitment to freedom of speech and of the media, and benefited from the asymmetry of open Western media markets versus the tightly controlled Russian one.

The case of the EU is no less peculiar. As in many cases, the EU reacted belatedly to the emerging challenge from Russia due to its complex institutional framework and need for excessive coordination among its institutions and member states. The European Council established the East StratCom Task Force of the European External Action Service in March 2015.

Its main objectives are:

1. Communicating EU policy in the Eastern Partnership.
2. Strengthening the media environment.
3. Forecasting and addressing Russian disinformation with an emphasis on the crisis in and around Ukraine.

Russian strategic communications present a problem for the EU by using nonmilitary means to achieve politico-military goals and being backed by massive resources. Russia invested 191 million euros in Twitter and is also active on Facebook. Russia also takes advantage of the more rapid dissemination of fake news (according to a 2018 study by researchers at the Massachusetts Institute of Technology, fake news travels an average of six times faster than truth), aiming to disorient and influence policymakers and societies and create confusion over what is factual and what information can be believed. Russia uses frequently repeated stereotypes, which have recently entailed comments such as “the EU is a U.S. vassal,” “human rights defenders are targeted in the West” and “the economic

situation in the Baltic states is worse than in Soviet times.” These stereotypes address matters whose details are unknown to most people. Although perhaps insufficiently visible, the EU has a website (<https://euvsdisinfo.eu>) that has published analyses and maintained a database of more than 6,900 cases of disinformation since September 2015. This helps provide access to sources for those who want to understand how the spreading of disinformation works and sends a message to its originators that they cannot get away with their falsehoods for long.

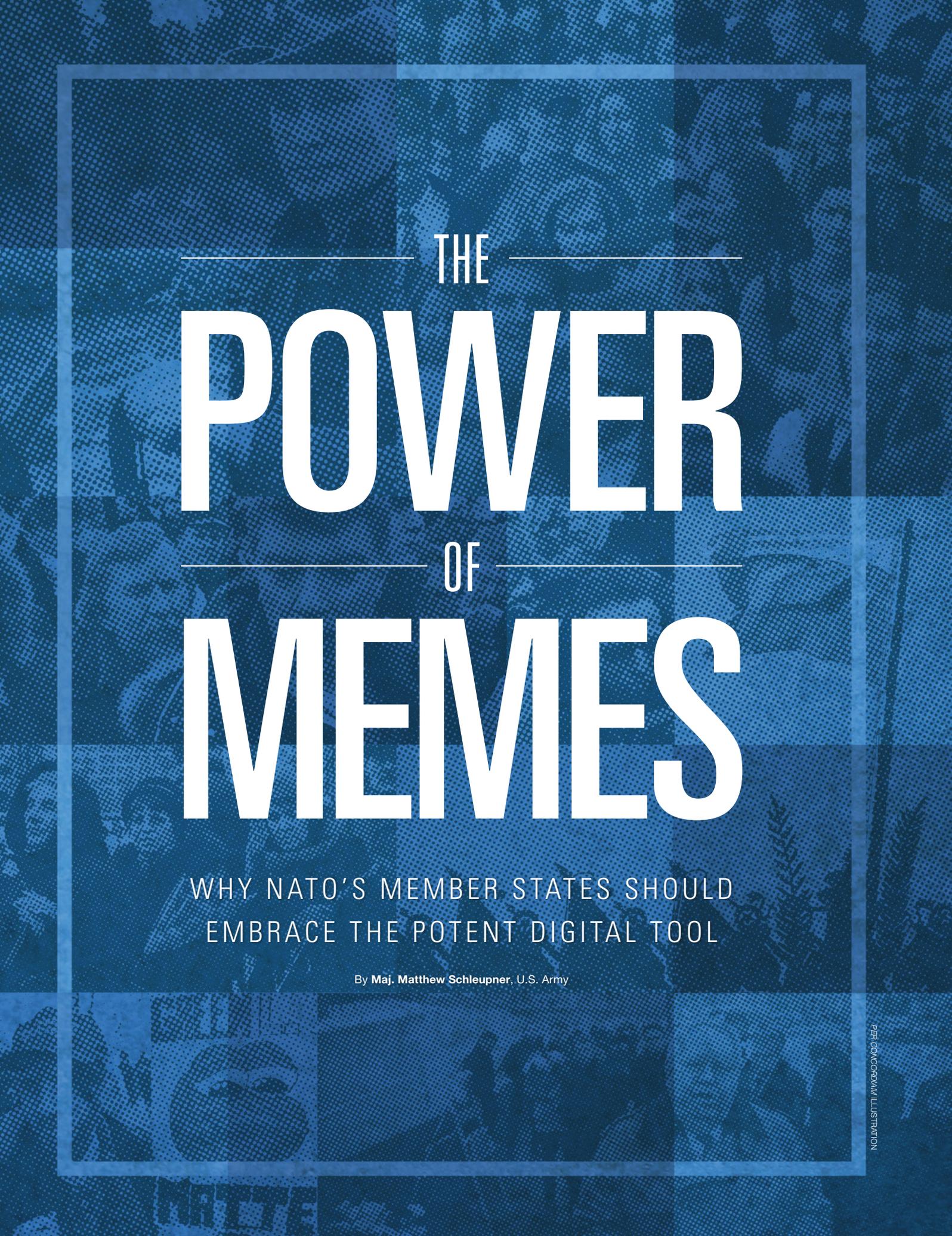
CONCLUSIONS

Russia has not extensively diversified its power base but has broadened its capabilities primarily in strategic communications. Russia has focused on reaching out to the world with an emphasis on its own region and particularly on countries and societies more easily targeted through such means. It has taken advantage of its ability to project a unified message, of the West’s commitment to freedom of speech and of the media, and benefited from the asymmetry of open Western media markets versus the tightly controlled Russian one.

Russia’s primary objective is to increase its influence in the international system and demonstrate its importance. As this can be achieved only partially by demonstrating Russia’s undeniable strengths, it must simultaneously meet two requirements: reconfirm Russia’s power through communications and with this, generate support, particularly in states and societies where Russian influence is historically well-established, or where it can be established, and weaken the influence of the West.

The West’s influence is perceived by Russia to stem partly from its unity, including its own institutions and those global ones where Western influence is strong, such as international financial institutions. Communications is one of many Russian means of influence used to counter the West. Media influence is among the most visible new weapons in the Russian arsenal and, as recent evidence shows, it is part of a spectrum where morally unacceptable, illicit and illegal means coexist. Russia finances certain political movements and parties (as the Soviet Union used to finance Western Communist parties), interferes politically and technically in elections, provides patronage, and makes corrupt deals with foreign countries and their leaders.

The West has remained hesitant, slow and divided in its response to Russia partly because the obvious responses contradict its foundational values, including an array of human rights, and partly because it is more difficult to agree on a coordinated response when the threat is not perceived as existential. In recent years, the West has gradually begun to mount a response. It remains to be seen whether the focus will be on hostile strategic communications or other highly annoying activities, such as election interference, and how the division of labor between national and coordinated, international actions will evolve. □



THE
POWER
OF
MEMES

WHY NATO'S MEMBER STATES SHOULD
EMBRACE THE POTENT DIGITAL TOOL

By Maj. Matthew Schlepner, U.S. Army

In 2017 there were 2.46 billion unique social media users worldwide. By 2021, the number is expected to exceed 3 billion, according to the database company Statista, with 71% of all internet users on social media by then. Most of this growth is coming from the world's developing regions: China, Africa, South Asia — areas where large populations are being introduced to high levels of technology and sophisticated methods of information operations. Beyond this, the reach of these sites makes them indispensable for those trying to relay a message to their citizenry. For example, during the September 2018 referendum in North Macedonia concerning changing the country's name to the Republic of North Macedonia, the Global Engagement Center, the newly authorized lead for the United States government's efforts to counter propaganda and disinformation from international terrorist organizations and foreign countries, estimated that the U.S. Embassy in North Macedonia (based on its follower counts on Facebook, Instagram and Twitter) had the power to reach the entire population of the country simply by using its social media accounts. That is how powerful social media can be.

This power can affect every instrument of military power. The ability of adversaries to use these networks to advance a narrative has grown rapidly, and the form that many of these messages takes is a meme. The meme has become a dominant tool of NATO's adversaries and there exists a void in how to counter that messaging. NATO can compete in this information space by adopting a more proactive mindset, having senior leaders engage on social media, treating messaging as a marketing tool of the Alliance, and adjusting its mindset to allow for more experimentation in messaging.

MEMES AND MEMETIC WARFARE

In his article, "Evolutionary Psychology, Memes and the Origin of War," Keith Henson defines memes as replicating information patterns: "ways to do things, learned elements of culture, beliefs or ideas." A meme is information that "propagates, has impact and persists." Memes can be ideas or symbols, catchphrases, hashtags, or words wrapped in cultural significance. Memetics tries to study this process within a form of neuro-cognitive warfare, a subset of information warfare.

A meme is defined in Richard Dawkins' book, *The Selfish Gene*, as a "self-reproducing and propagating information structure analogous to a gene in biology." The meme, he explains, has evolutionary effects on the human culture and physiology. It has the ability to replicate using hosts and to influence behavior to promote replication. Memetic warfare is certainly not a new concept. One could argue that Benjamin Franklin was the U.S.' first meme maker, creating the poignant "Join or Die" image of a snake cut into pieces, each part representing an American colony. There are thousands of examples similar to this, but Western security institutions still have not wrapped their heads around how to be effective, or as effective as the adversary, in the memetic space.

"Trolling, it might be said, is the social media equivalent of guerrilla warfare, and memes are its currency of propaganda." — Jeff Giese

The only thing new about the memetic revolution is the space in which the narrative is happening — cyberspace. Cyberspace is so open and so vast that the power of the information it contains is multiplied many times over the normal impact. Yet Western institutions did not begin to understand the scope of the problem until U.S. Marine Corps Maj. Michael Prosser's 2005 thesis on memetic warfare as a growth industry and studies afterward by the Defense Advanced Research Projects Agency and others into ongoing memetic warfare. Through its Strategic Communications Centre of Excellence, NATO enlisted well-known social media and technology thinker Jeff Giese to explain the power of the meme and how it should be embraced. In his article, "It's time to embrace memetic warfare," Giese starts not by quoting technology or warfare experts, but by discussing a conversation he had over a beer with a well-known internet troll on ways to attack ISIS through trolling. Every idea they



A protester in Berkeley, California, holds a poster with the likeness of the meme Pepe the Frog. In the 2016 U.S. presidential campaign, a group that supported then-candidate Donald Trump successfully appropriated the meme.

AFP/GETTY IMAGES

developed was low-budget but creative, exploiting the openness and cost efficiency of the internet to attack the weaknesses of ISIS. Giese writes that “trolling, it might be said, is the social media equivalent of guerrilla warfare, and memes are its currency of propaganda.” He argues that NATO needs to conceptually grasp the concept of memes — to not think about memes as a weapon but rather as a tool in “competition over the narrative.” He explains that much of the time discussing memetic warfare is spent confusing it with cyber warfare. He maintains that while cyber warfare is about taking control of information, memetic warfare is about taking control of the dialogue — the psychological space.

NATO AND THE MEME BATTLEFIELD

Strategic messaging in the security space should be viewed as a debate rather than a conversation. There needs to be an aggressiveness to it that seeks to control the narrative space, much like an infantry battalion seeks to hold ground. At the same time,

there must be an awareness that ethical standards preclude democracies from creating a traditional Soviet-style propaganda system. Rather, better ways must be sought for spreading the truth in these modern times. At a time when attention spans are shorter because of technology, and the amount of available information has dramatically expanded, NATO needs to redefine the way it works in the memetic space. It understands the problem; it just isn't very good at trying to solve it. This involves a reframing of NATO's mindset and that of its member states. NATO as an institution, along with its member states, can begin or improve this with three easy steps.

1. Get on social media

There is a hesitancy by senior political and military leaders to be active on social media. Concerns about privacy and security are real. But this is mainly a mindset problem. At the Marshall Center in 2018, leaders from security institutions and NATO/European Union nations, along with



In the world of memes, seizing the narrative and demeaning your adversaries is a total communications victory.

partner nations, gathered to discuss challenges to strategic communications in the 21st century. In their discussions, leaders from NATO and the EU discussed how they are combating false narratives on the internet. NATO representatives said they had set up a page labeled “NATO truths” and “NATO-Russia: Setting the record straight” to combat false narratives on NATO-Russia issues. The page was a direct response to a series of Russian messaging campaigns using memetic warfare techniques. I remember thinking: How many of these leaders are personally active on social media? How many see how quick memetic warfare can work, and how effective it really is?

A new kind of thinking is needed in the age of Twitter and Instagram. It appeared as if Alliance leaders did not understand how social media works. For example, in the 2016 U.S. presidential

campaign, a meme called Pepe the Frog took off among supporters of then-candidate Donald Trump through the Reddit group /r/Donald. The supporters were tremendously successful in appropriating the meme to help their candidate. No fewer than 20 stories appeared in *The New York Times* about Pepe the Frog, and there was an effort by the Pepe the Frog creator to sue trolls on the internet for copyright infringement. If you simply view the comments of an internet news article critical of Russia, China or Iran, you will find them filled with odd statements, usually similar, attacking the article and working to shape the narrative in a way that negates factual reporting. *The New York Times* later reported that the Democratic National Committee used a false-flag campaign in the U.S. Senate race in Alabama between Roy Moore and Doug Jones, replicating what they thought were the techniques

In this authentic photograph, then-U.S. Ambassador to Russia John Tefft speaks to journalists in 2017 at the place in Moscow where Russian opposition leader Boris Nemtsov was gunned down two years earlier. Tefft was the victim of a meme when his image was inserted into an altered photograph to make it appear he had attended a political rally in Russia that he had not attended.

THE ASSOCIATED PRESS

of Russian bots to create viral memes against Moore, then blaming Russia for efforts to interfere in the election.

A senior leader who is not active on social media will have a hard time understating the full effect of this activity. To be active is at least to see the battlespace. I would argue that leaders should be active, but also vocal in messaging against false, viral campaigns. For example, consider how President Donald Trump or U.S. Ambassador to Germany Richard Grenell have fought back against false narratives or have advanced the truth through their own messaging. Other examples of leaders using this type of online voice are former Deputy Prime Minister Matteo Salvini in Italy, Brexit Party leader Nigel Farage in the United Kingdom or President Jair Bolsonaro in Brazil. The list continues to grow. An example of this is when the U.S. Embassy in Russia countered publication of an altered photo of then-U.S. Ambassador to Russia John Tefft that made it appear he was attending

understand that a gap exists in the understanding of this new communications technique. But the strategy is in its infancy, with online trials that fail for various reasons. The strategy here needs to flow from successful marketing principles and from the fact that NATO should not overthink its memetic messaging. Each problem set, each messaging campaign should be different and depend on the market NATO is trying to reach, the hook it is trying to employ, and the total presence it is attempting to achieve. Because information on the internet moves so quickly, the messaging strategy must be flexible, with maximum leeway given to those creating the messaging program. NATO should create a committee in this communications field and not be afraid to discuss and/or employ figures who are successful at memetic messaging.

This could be controversial at times because of the types of people generally associated with spreading memes. But experts in marketing, psychology and technology could be employed for oversight. Still, reaching out to personalities in the social media realm would be an absolute must. To be clear, when I say personalities I mean trolls — from Twitter, Reddit, 4chan and other social media platforms. Even if they aren't directly employed by NATO, their methods must be studied and understood. The power of memes is that they appear organic rather than corporately produced. Understanding what youths in Estonia or Ukraine

find persuasive within their cultural context will be difficult without surveying and employing people in those domains. As Giese points out, there is a sense of guerrilla warfare in the execution of trolling and memetic warfare. So the more NATO can develop a plan to gather bottom-fed information, the better.

3. Don't be afraid to make mistakes

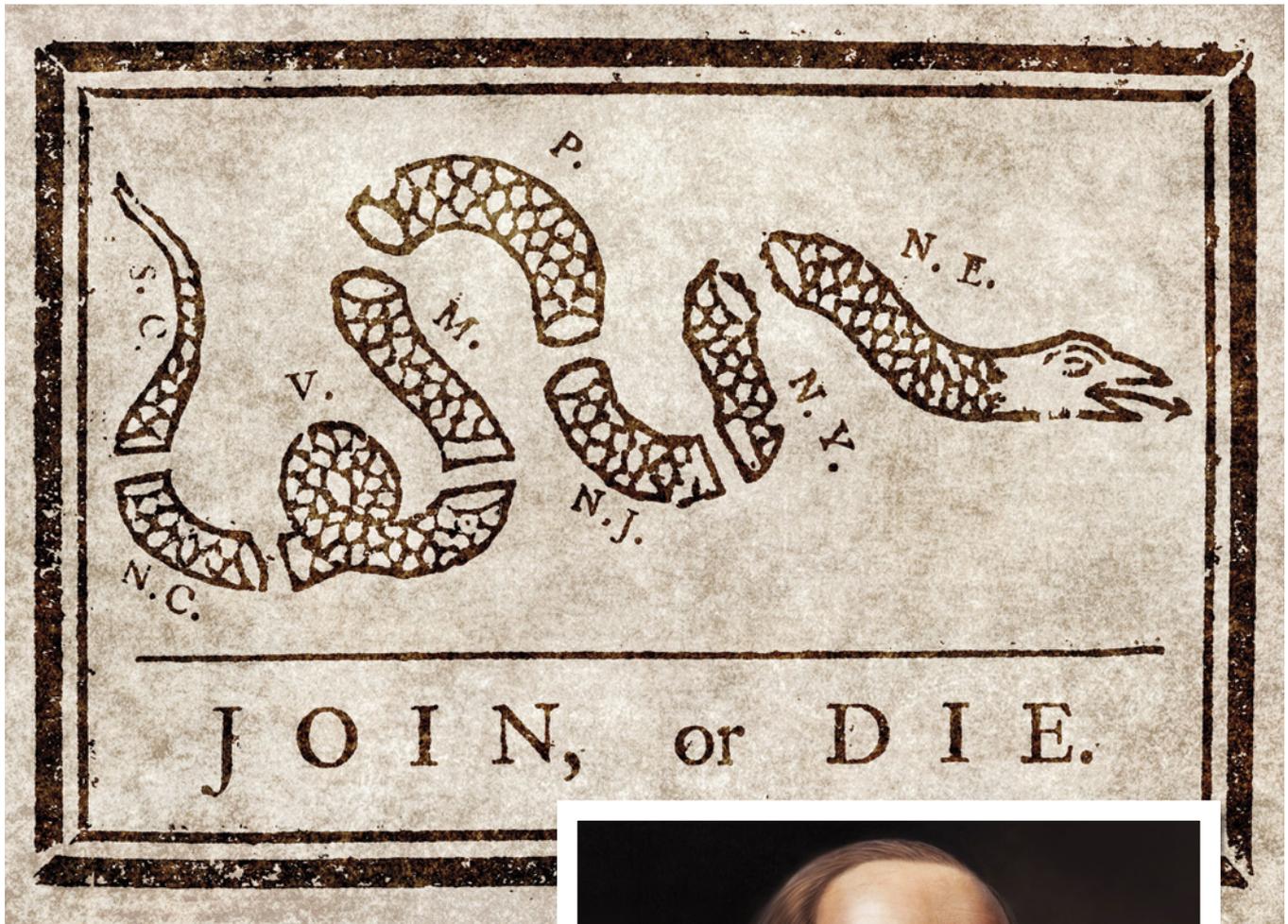
NATO commissioned a series of videos revolving around its 60-year anniversary in 2009 that attempted to adopt a memetic warfare posture, but they did not go viral in the way many expected. The U.S. State Department, in response to the success of ISIS' online recruiting, created the "Think Again, Turn Away" program. But it ended without achieving the success many had hoped for. At least institutions are trying. The field of technology permeates with the theory that you must test and continue to test, always to the point that things break. Moving fast is critical, and that type of thinking can be antithetical to a military and political

The power of memes is that they appear organic rather than corporately produced. Understanding what youths in Estonia or Ukraine find persuasive within their cultural context will be difficult without surveying and employing people in those domains.

an opposition party rally. In response, the embassy distributed a series of obviously altered photos that made it appear Tefft was speaking on the moon, on the ice at a hockey game, and standing next to U.S. Gen. Douglas MacArthur as he landed in the Philippines during World War II. These things seem small, but they set a true narrative and undermine false ones. In the world of memes, seizing the narrative and demeaning your adversaries is a total communications victory.

2. Memetic warfare as marketing

Marketing experts identify four principles necessary for success: define the strategy before the tactics, narrow the market focus, differentiate from the competition, and create a total online presence. Since marketing is a business field focused more on offensive messaging to create business and control what people are saying about a business, this fits well in the memetic model. NATO and other Western security institutions seemingly



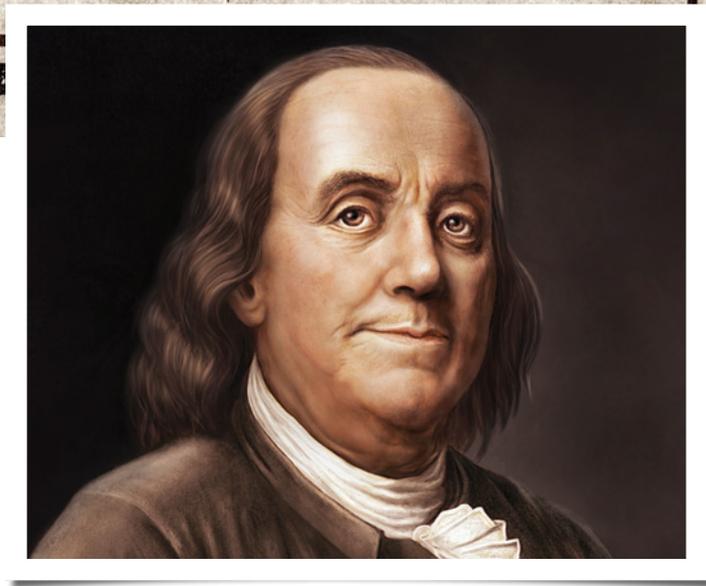
ISTOCK BY GETTY IMAGES

Benjamin Franklin can be considered the United States' first meme maker, creating the poignant "Join or Die" image of a snake cut into pieces, each part representing an American colony.

mindset that values polished and deliberative communications strategies. On the internet, there may be a need to respond to viral memes that have a maximum impact of 10 hours or less.

CONCLUSIONS

Memes are important because they aim to influence our beliefs. Therefore, while there can be an impression that memes are little more than clever, funny, timely messages seeking an aim with no specific end, there is a psychological effect on the reader that is inescapable and aimed at changing beliefs. By shifting our mindset on memetic warfare, dispelling the notion that memetic warfare is some sort of cyber warfare campaign directly against an adversary — but rather a tool to fight propaganda with true information — NATO and member states can take steps to have an effective memetic campaign. This starts with knowing where gaps are and seeking those who are skilled at the



ISTOCK BY GETTY IMAGES

craft to explain them. More resources is key, along with working with private-sector individuals and institutions to build an overarching strategy. Once this is complete, it is critical that flexibility be given to meme specialists to build specific narratives and respond at the pace of the internet. We will not be able to entirely compete with our adversaries in the internet trolling realm because they are unhindered by our norms, but we can understand this and build our strategies around it. It is complicated, but in time we can get better by working smarter. □

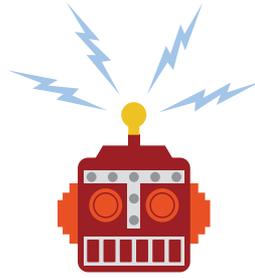
COMMANDING

the TREND

**Social media as
information warfare**

By Lt. Col. Jarred Prier, U.S. Air Force

PER CONCORDIAM ILLUSTRATION



The adaptation of social media as a tool of modern warfare should not be surprising. Internet technology evolved to meet the needs of information-age warfare around 2006 with the dawn of Web 2.0, which allowed internet users to create content instead of just consuming online material. Now, individuals could not only decide what was important and read only that, on demand, but they could also use the medium to create news based on their opinions. The social nature of humans ultimately led to virtual networking. As such, traditional forms of media were bound to give way to a more tailorable form of communication. United States adversaries were quick to find ways to exploit the openness of the internet, eventually developing techniques to employ social media networks as a tool to spread propaganda. Social media creates a point of injection for propaganda and has become the nexus of information operations and cyber warfare. To understand this, we must examine the important concept of the social media trend and look briefly into the fundamentals of propaganda. Also important is the spread of news on social media, specifically, the spread of “fake news” and how propaganda penetrates mainstream media outlets.

Twitter, Facebook and other social media sites employ an algorithm to analyze words, phrases or hashtags to create a list of topics sorted in order of popularity. This “trend list” is a quick way to review the most discussed topics at a given time. According to “Trends in Social Media: Persistence and Decay,” a 2011 study conducted at Cornell University, a trending topic “will capture the attention of a large audience for a short time” and thus “contributes to agenda setting mechanisms.” Using existing online networks in conjunction with automatic bot accounts (autonomous programs that can interact with computer systems or users), agents can insert propaganda into a social media platform, create a trend, and rapidly disseminate a message faster and cheaper than through any other medium. Social media facilitates the spread of a narrative outside a particular social cluster of true believers by commanding the trend.

It hinges on four factors:

1. a message that fits an existing, even if obscure, narrative
2. a group of true believers predisposed to the message
3. a relatively small team of agents or cyber warriors
4. a network of automated bot accounts

The existing narrative and the true believers who subscribe to it are endogenous, so any propaganda must fit

that narrative to penetrate their network. Usually, the cyber team is responsible for crafting the specific message for dissemination. The cyber team then generates videos, memes or fake news, often in collusion with the true believers. To effectively spread the propaganda, the true believers, the cyber team and the bot network combine to take command of the trend. Thus, an adversary can influence the population using a variety of propaganda techniques, primarily through social media combined with online news sources and traditional forms of media.

Twitter makes real-time idea and event sharing possible on a global scale. A trend can spread a message to a wide group outside someone’s typical social network. Moreover, malicious actors can use trends to spread a message using multiple forms of media on multiple platforms, with the ultimate goal of garnering coverage in the mainstream media. Command of the trend is a powerful method of spreading information whereby, according to a February 2017 article in *The Guardian*, “you can take an existing trending topic, such as fake news, and then weaponize it. You can turn it against the very media that uncovered it.” Because Twitter is an idea-sharing platform, it is very popular for rapidly spreading information, especially among journalists and academics; however, malicious users have also taken to Twitter for the same benefits in recent years. At one time, groups like al-Qaida preferred creating websites, but now “Twitter has emerged as the internet application most preferred by terrorists, even more popular than self-designed websites or Facebook,” Gabriel Weimann notes in his book, *Terrorism in Cyberspace: The Next Generation*.

Three methods help control what is trending on social media: trend distribution, trend hijacking and trend creation. The first method is relatively easy and requires the least amount of resources. Trend distribution is simply applying a message to every trending topic. For example, someone could tweet a picture of the president with a message in the form of a meme — a stylistic device that applies culturally relevant humor to a photo or video — along with the unrelated hashtag #SuperBowl. Anyone who clicks on that trend list expecting to see something about football will see that meme that has nothing to do with the game. Trend hijacking requires more resources in the form of either more followers spreading the message or a network of bots designed to spread the message automatically. Of the three methods to gain command of the trend, trend creation requires the most effort.

It necessitates either money to promote a trend or knowledge of the social media environment around the topic and, most likely, a network of several automatic bot accounts. In 2014, Twitter estimated that only 5% of its accounts were bots; that percent now tops 15%. Some of the accounts are “news bots,” which retweet trending topics. Some of the accounts are for advertising purposes, which try to dominate conversations to generate revenue through clicks on links. Some bots are trolls, which, like a human version of an online troll, tweet to disrupt civil conversation.

For malicious actors seeking to influence a population through social media trends, the best way is to build a network of bot accounts programmed to tweet at various intervals, respond to certain words or retweet when directed by a master account. Figure 1 illustrates the basics of a bot network. The top of the chain is a small core group. That team is composed of human-controlled accounts with a large number of followers. The accounts are typically adversary cyber warriors or true believers with a large following. Under the core group is the bot network. Bots tend to follow each other and the core group. Below the bot network is a group consisting of the true believers without a large following. These human-controlled accounts are a part of the network, but they appear to be outsiders because of the weaker links between the accounts. The bottom group lacks a large following, but they do follow the core group, sometimes follow bot accounts, and seldom follow each other.

Enough bots working together can quickly start a trend or take over a trend, but bot accounts themselves can only bridge the structural hole between networks, not completely change a narrative. To change a narrative — to conduct an effective influence operation — requires a group to combine a well-coordinated bot campaign with essential elements of propaganda.

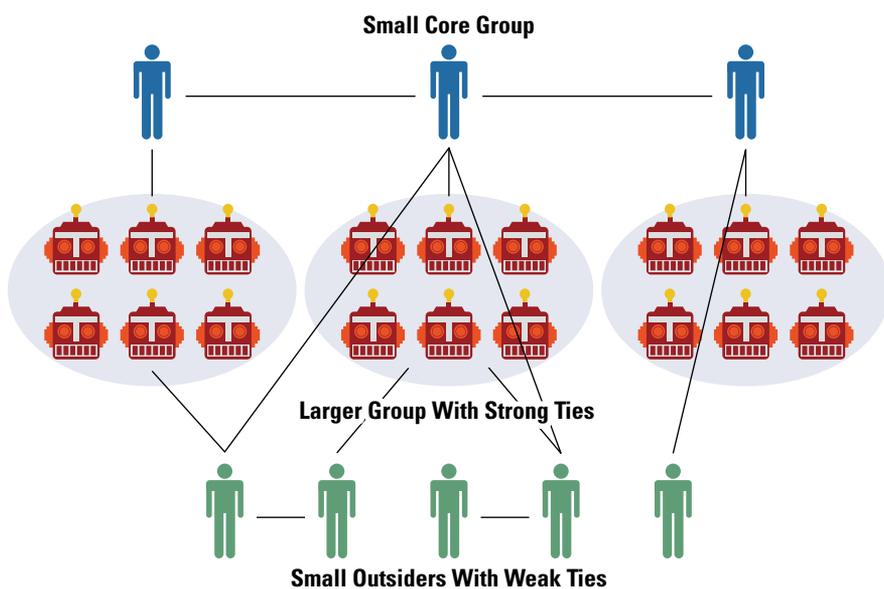
PROPAGANDA PRIMER

For propaganda to function, it needs a previously existing narrative to build upon, as well as a network of true believers who already buy into the underlying theme. Social media helps the propagandist spread the message through an established network. A person is inclined to believe information on social media because the people he chooses to follow share things that fit his existing beliefs. That person, in turn, is likely to share the information with others in his network, with others who are like-minded, and with those predisposed to the message. With enough shares, a particular social network accepts the propaganda storyline as fact. But up to this point, the effects are relatively localized.

The most effective propaganda campaigns are not confined just to those predisposed to the message. Essentially, propaganda permeates everyday experiences, and those targeted with a massive media blitz will never fully understand that the ideas they have are not entirely their own. A modern example of this phenomenon was observable during the Arab Spring as propaganda spread on Facebook “helped middle-class Egyptians understand that they were not alone in their frustration,” Thomas Rid writes in *Cyber War Will Not Take Place*. In short, propaganda is simpler to grasp if everyone around a person seems to share the same emotions on a particular subject. In other words, propaganda creates heuristics, which is a way the mind simplifies problem solving by relying on quickly accessible data. In *Thinking, Fast and Slow*, Daniel Kahneman explains that the availability heuristic weighs the amount and frequency of information received, as well as the recentness of the information, as more valuable than the source or accuracy of the information. Essentially, the mind creates a shortcut based on the most — or most recent — information available, simply because it can be remembered easily. The lines in Figure 2 show the formation of opinions temporally, with bold arrows influencing a final opinion more than light arrows. The circled containers indicate a penetration point for propaganda exploitation. As previously described, mass media enables the rapid spread of propaganda, which feeds the availability heuristic. The internet makes it possible to flood the average person’s daily intake of information, which aids the spread of propaganda.

One of the primary principles of propaganda is that the message must resonate with the target. When people are presented with information that is within their belief structure, their bias is confirmed and they accept the propaganda. If it is outside of their network, they may initially reject the story, but the volume of information may create an availability heuristic. Over time, the propaganda becomes

Figure 1. Illustration of a bot network Source: Lt. Col. Jarred Prier, U.S. Air Force



normalized and even believable. It is confirmed when a fake news story is reported by the mainstream media, which has become reliant on social media for spreading and receiving news. Figure 3 maps the process of how propaganda can penetrate a network that is not predisposed to the message. This outside network is a group that is ideologically opposed to the group of true believers. The outside network is likely aware of the existing narrative but does not necessarily subscribe to the underlying beliefs that support the narrative.

Command of the trend enables the contemporary propaganda model to create a “firehose of information” that always permits the insertion of false narratives. Trending items produce the illusion of reality, in some cases even being reported by journalists. Because untruths can spread so quickly, the internet has created “both deliberate and unwitting propaganda” since the early 1990s through the proliferation of rumors passed as legitimate news, according to Garth Jowett and Victoria O’Donnell in *Propaganda & Persuasion*. The normalization of these types of rumors over time, combined with the rapidity and volume of new false narratives over social media, opened the door for fake news.

The availability heuristic and the firehose of disinformation can slowly alter opinions as propaganda crosses networks by way of the trend, but the amount of influence will likely be minimal unless it comes from a source that a nonbeliever finds trustworthy. An individual may see the propaganda but still not buy into the message without turning to a trusted source of news to test its validity.

SOCIAL NETWORKS AND SOCIAL MEDIA

As social media usage has become more widespread, users have become ensconced within specific, self-selected groups, which means that news and views are shared nearly exclusively with like-minded users. In network terminology, this

Figure 2. Model of individual opinion option

Source: Alan D. Monroe, *Public Opinion in America*

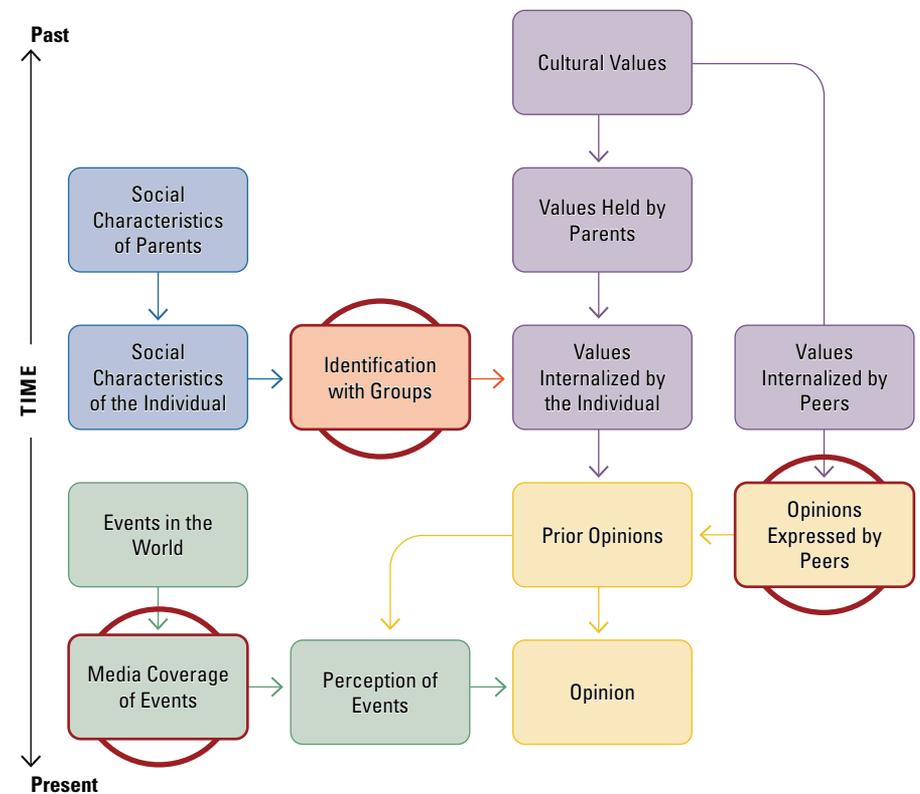
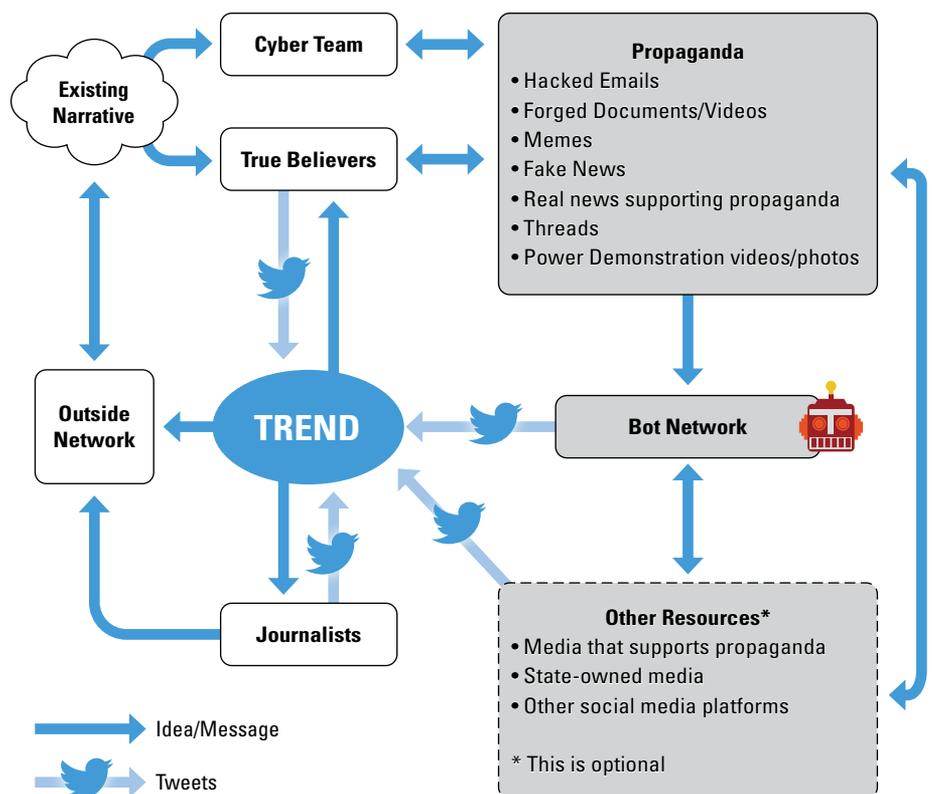


Figure 3. How propaganda spreads via the trend Source: Lt. Col. Jarred Prier, U.S. Air Force



group phenomenon is called homophily. More colloquially, it reflects the concept that “birds of a feather flock together.” Homophily within social media creates an aura of expertise and trustworthiness where those factors would not normally exist. People are more willing to believe things that fit into their worldview. According to Jowett and O’Donnell, once source credibility is established in one area, there is a tendency to accept that source as an expert on other issues as well, even if the issue is unrelated to the area of originally perceived expertise. Ultimately, Tom Hashemi writes in a December 2016 article for the War on the Rocks website, this “echo chamber” can promote a scenario in which your friend is “just as much a source of insightful analysis on the nuances of U.S. foreign policy towards Iran as regional scholars, arms control experts, or journalists covering the State Department.”

If social media facilitates self-reinforcing networks of like-minded users, how can a propaganda message traverse networks where there are no overlapping nodes? This link between networks is only based on that single topic and can be easily severed. Thus, to employ social media effectively as a tool of propaganda, an adversary must exploit a feature within the social media platform that enables cross-network data sharing on a massive scale: the trending topics list. Trends are visible to everyone. Regardless of who follows whom on a given social media platform, all users see the topics algorithmically generated by the platform as being the most popular topics at that particular moment. Given this universal and unavoidable visibility, “popular topics contribute to the collective awareness of what is trending and at times can also affect the public agenda of the community,” according to the Cornell University study. In this manner, a trending topic can bridge the gap between clusters of social networks. A malicious actor can quickly spread propaganda by injecting a narrative onto the trend list. The combination of networking on social media, propaganda and reliance on unverifiable online news sources introduces the possibility of completely falsified news stories entering the mainstream of public consciousness.

Fake news consists of more than just bad headlines, buried ledes or poorly sourced stories; it is a particular form of propaganda composed of a false story disguised as news. On social media, this becomes particularly dangerous because of the viral spread of sensationalized fake news stories. A prime example of fake news and social media came from the most shared news stories on Facebook during the 2016 U.S. presidential election. A story stating that the pope had endorsed Donald Trump for president received over 1 million shares on Facebook alone, not to mention Twitter, according to BuzzFeed. The source was a supposedly patriotic American news blog called Ending the Fed, a website run by Romanian businessperson Ovidiu Drobot. Fake news stories from that site and others received more shares in late 2016 than did traditional mainstream news sources (see Figure 4).

It is important to recognize that more people were exposed to those fake news stories than what is reflected in the “shares” data. Over time, those fake news sources become trusted sources for some people and as people learn to trust them, legitimate news outlets become less trustworthy.

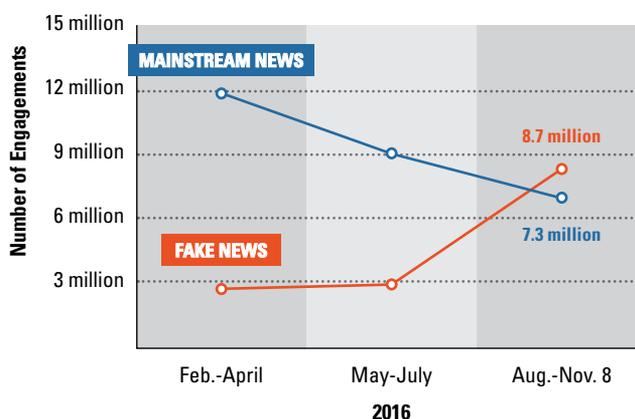
RUSSIA: MASTERS OF MANIPULATION

Russia is no stranger to information warfare. The Soviet Union originally used the technique of *aktivnyye meropriyatiya* (active measures) and *dezinformatsiya* (disinformation). According to a 1987 State Department report on Soviet information warfare, “active measures are distinct both from espionage and counterintelligence and from traditional diplomatic and informational activities. The goal of active measures is to influence opinions and/or actions of individuals, governments, and/or publics.” In other words, Soviet agents would try to weave propaganda into an existing narrative to smear countries or individuals. Active measures are designed, as retired KGB Gen. Oleg Kalugin once explained, “to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the U.S. in the eyes of the people in Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs.” Noted Russia analyst Michael Weiss says, “The most common subcategory of active measures is *dezinformatsiya*, or disinformation: feverish, if believable lies cooked up by Moscow Centre and planted in friendly media outlets to make democratic nations look sinister.”

Russia’s trolls have a variety of state resources at their disposal, including the assistance of a vast intelligence network. Additional available tools include RT (Russia Today) and Sputnik, Kremlin-financed television news networks broadcasting in multiple languages around the world. Before the trolls begin their activities on social media, the cyber-warrior hackers first provide hacked information to Wikileaks, which according to then-CIA director Mike Pompeo is a “nonstate hostile intelligence service abetted by state actors like Russia.” In intelligence terms, WikiLeaks operates as a “cutout” for Russian intelligence operations — a place to spread intelligence information through an outside organization — similar to the Soviets’ use of universities to publish propaganda studies in the 1980s. The trolls then take command of the trend, spreading the hacked information on Twitter, while referencing WikiLeaks and RT to provide credibility. These efforts would

Figure 4. Total Facebook engagements for top 20 2016 U.S. election stories

Source: Lt. Col. Jarred Prier, U.S. Air Force



Russian-Germans protest in Berlin after the spread of a false story about a Russian-German girl named Lisa being raped. The sign reads, "Lisa, we are with you."

REUTERS





A sign of support is placed outside a pizza shop in Washington, D.C., after a fake news story prompted a man to fire a rifle inside the business. The man told police he decided to “self-investigate” a conspiracy theory that Hillary Clinton was running a child sex ring from the business.

THE ASSOCIATED PRESS

be impossible without an existing network of American true believers willing to spread the message. The Russian trolls and the bot accounts also amplified the voices of the true believers. Then, the combined effects of Russian and American Twitter accounts took command of the trend to spread disinformation across networks.

DIVISION AND CHAOS

One particularly effective Twitter hoax occurred as racial unrest fell on the University of Missouri campus. On the night of November 11, 2015, #PrayforMizzou began trending on Twitter as a result of protests over racial issues at the university (known colloquially as Mizzou) campus. However, “news” that the Ku Klux Klan (KKK) was marching through the campus and the adjoining city of Columbia started developing within the hashtag — altering its meaning — and shooting it to the top of the trend list. A user with the display name “Jermaine” (@Fanfan1911), warned residents, “The cops are marching with the KKK! They beat up my little brother! Watch out!” The tweet included a picture of a black child with a severely bruised face; it was retweeted hundreds of times. Jermaine and a handful of other users continued tweeting and retweeting images and stories of KKK and neo-Nazis in Columbia, chastising the media for not covering the racists creating havoc on campus.

An examination of Jermaine’s followers, and the followers of his followers, showed that the original tweeters all followed and retweeted each other, and were retweeted automatically by approximately 70 bots using the trend-distribution technique, which used all of the trending hashtags at that

time within their tweets, not just #PrayforMizzou. Spaced evenly, and with retweets from real people who were observing the Mizzou hashtag, the numbers quickly escalated to thousands of tweets within a few minutes, including tweets from the Mizzou student body president and feeds from local and national news networks — taken in by the deception — supporting the false narrative. The plot was smoothly executed and evaded the algorithms Twitter designed to catch bot tweeting, mainly because the Mizzou hashtag was being used outside of that attack. The narrative was set as the trend was hijacked, and the hoax was underway.

Shortly after the disinformation campaign at Mizzou, @Fanfan1911 changed his display name from Jermaine to “FanFan” and the profile picture from that of a young black male to a German iron cross. For the next few months, FanFan tweeted in German about Syrian refugees and focused on messages that were anti-Islamic, anti-European Union, and anti-German Chancellor Angela Merkel, reaching a crescendo after reports of women being raped on New Year’s Eve 2016 by refugees from Muslim countries. Some of the reports were false, including a high-profile case of a 13-year-old ethnic-Russian girl living in Berlin who falsely claimed that she was abducted and raped by refugees.

Once again, Russian propaganda dominated the narrative. Similar to previous disinformation campaigns on Twitter, Russian trolls were able to spread disinformation by exploiting an underlying fear and an existing narrative. They used trend-hijacking techniques in concurrence with reporting by RT. To attempt to generate more attention in European media to Russia’s anti-Merkel narrative, Russian Foreign Minister

Sergey Lavrov accused German authorities of a “politically correct cover-up” in the case of the Russian teen. Aided by the Russian propaganda push, the anti-immigration narrative began spreading across traditional European media.

INFLUENCING THE 2016 PRESIDENTIAL ELECTION

According to the U.S. Office of Director of National Intelligence (ODNI) report on Russian influence during the 2016 presidential election, “Moscow’s influence campaign followed a messaging strategy that blends covert intelligence operations — such as cyber activity — with overt efforts by Russian Government agencies, state funded media, third-party intermediaries, and paid social media users, or ‘trolls.’” Russian propaganda easily meshed with the views of “alt-right” networks and those of U.S. Sen. Bernie Sanders’ supporters on the left wing of the Democratic Party. In a September 2016 speech, candidate Hillary Clinton described half of candidate Trump’s supporters as a “basket of deplorables,” and said that the other half were just people who felt the system had left them behind, who needed support and empathy. The narrative quickly changed after Trump supporters began referring to themselves as “Deplorable” in their social media screen names.

Before the “deplorables” comment, the Russian trolls primarily used an algorithm to rapidly respond to a Trump tweet, with their tweets prominently displayed directly under Trump’s if a user clicked on the original. After the Clinton speech, a search on Twitter for “deplorable” was all one needed to suddenly gain a network of followers numbering between 3,000 and 70,000. Once again, FanFan’s name changed — this time to “Deplorable Lucy” — and the profile picture became a white, middle-aged female with a Trump logo at the bottom of the picture. FanFan’s followers went from just over 1,000 to 11,000 within a few days. His original network from the Mizzou and European campaigns changed as well: Tracing his follower trail again led to the same groups of people in the same network, and they were all now defined by the “Deplorable” brand. In short, they were now completely in unison with a vast network of other Russian trolls, actual American citizens, and bot accounts from both countries on Twitter, making it suddenly easier to get topics trending. The Russian trolls could employ the previously used tactics of bot tweets and hashtag hijacking, but now they had the capability to create trends.

Coinciding with the implementation of the strategy to mask anti-Trump comments on Twitter, WikiLeaks began releasing Clinton campaign chairman John Podesta’s stolen emails. The emails themselves revealed nothing truly controversial, but the powerful narrative created by a trending hashtag conflated Podesta’s emails with Clinton’s use of a private email server while she was secretary of state. Secondly, the Podesta email narrative took routine issues and made them seem scandalous. The most common theme: bring discredit to the mainstream media by distorting the stolen

emails into conspiracies of attempted media “rigging” of the election to support Clinton. The corruption narrative also plagued the Democratic National Committee, which was hacked earlier in the year by Russian sources, according to the ODNI report, and then revealed by WikiLeaks. Another of Podesta’s stolen emails was an invitation to a party at the home of a friend that promised pizza from Comet Ping Pong pizzeria and a pool to entertain the kids. It was turned into a fake news conspiracy theory (#PizzaGate) inferring that the email was code for a pedophilic sex party. That influenced a man to go to Comet Ping Pong, armed with an AR-15 rifle, prepared to free children from an underground child sex trafficking ring.



Often, the mainstream media would latch onto a story with an unsavory background and false pretenses, thus giving more credibility to fake news

The #PizzaGate hoax, along with other false and quasi-false narratives, became common within right-wing media as another indication of the immorality of Clinton and her staff. Often, the mainstream media would latch onto a story with an unsavory background and false pretenses, thus giving more credibility to fake news; however, the #PizzaGate hoax followed the common propaganda narrative that the media was trying to cover up the truth and that the government failed to investigate the crimes. The trend became so sensational that traditional media outlets chose to cover the Podesta email story, which gave credibility to the fake news and the associated online conspiracy theories promulgated by the Deplorable Network. The WikiLeaks release of the Podesta emails was the peak of Russian command of the trend during the 2016 election. Nearly every day #PodestaEmail trended as a new batch of supposedly scandalous hacked emails made their way into the mainstream press.

Based on my analysis, the bot network appeared to be between 16,000 and 34,000 accounts. The cohesiveness of the group indicates how a coordinated effort can create a trend in a way that a less cohesive network could not. To conduct cyber attacks using social media as information warfare, an organization must have a vast network of bot accounts to take command of the trend. With unknown factors, such as the impact of fake news, the true results of the Russian influence operation will likely never be known. As philosopher Jacques Ellul said, experiments undertaken to gauge the effectiveness of propaganda will never work because the tests “cannot reproduce the real propaganda situation.”

Adrian Chen, *The New York Times* reporter who originally uncovered the St. Petersburg troll network in 2015, went back to Russia in the summer of 2016. Russian activists he interviewed claimed that their purpose “was not to brain-wash readers, but to overwhelm social media with a flood of fake content, seeding doubt and paranoia, and destroying the possibility of using the Internet as a democratic space.” The troll farm used similar techniques to drown out anti-Putin trends on Russian social media. A Congressional Research Service Study summarized the Russian troll operation succinctly in a January 2017 report: “Cyber tools were also used [by Russia] to create psychological effects in the American population. The likely collateral effects of these activities include compromising the fidelity of information, sowing discord and doubt in the American public about the validity of intelligence community reports, and prompting questions about the democratic process itself.”

For Russia, information warfare is a specialized type of war, and modern tools make social media a weapon. According to a former Obama administration senior official, Russians regard the information sphere as a domain of warfare on a sliding scale of conflict that always exists between the U.S. and Russia. This perspective was on display during the Infoforum 2016 Russian national security conference, where senior Kremlin advisor Andrey Krutskikh compared Russia’s information warfare to a nuclear bomb, which would “allow Russia to talk to Americans as equals,” in the same way that Soviet testing of the atomic bomb did in 1949.

THE FUTURE OF WEAPONIZED SOCIAL MEDIA

Smear campaigns have been around since the beginning of politics, but the novel techniques recently employed have gained credibility after the attacks trended on Twitter. The attacks, often under the guise of a “whistleblower” campaign, make routine political actions seem scandalous.

Just like the Podesta email releases, several politicians and business leaders around the world have fallen victim to this type of attack.

Recall the 2015 North Korean hacking of Sony Studios. The fallout at the company was not because of the hacking itself, but from the release of embarrassing emails from Sony senior management, as well as the salaries of every employee. The uproar over the emails dominated social media, often fed by salacious stories like the RT headline: “Leaked Sony emails exhibit wealthy elite’s maneuvering to get child into Ivy League school.” Ultimately, Sony fired a senior executive because of the content of her emails. In another example from May 2017, nine gigabytes of email stolen from French presidential candidate Emmanuel Macron’s campaign were released online and verified by WikiLeaks. Subsequently, the hashtag #MacronLeaks trended to number one worldwide. This influence operation resembled the #PodestaEmail campaign with a supporting cast of some of the same actors. During the weeks preceding the French election, many accounts within the Deplorable Network changed their names to support Macron’s opponent, Marine LePen. These accounts mostly tweeted in English and still engaged in American political topics as well as French issues. Some of the accounts also tweeted in French, and a new network of French-tweeting bot accounts used the same methods as the Deplorable Network to take command of the trend.

In his book *Out of the Mountains*, David Kilcullen describes a future comprising large, coastal urban areas filled with potential threats, all connected. The implications are twofold. First, networks of malicious nonstate actors would be able to band together to hijack social media. Although these groups may not have the power to create global trends, they can certainly create chaos with smaller numbers by hijacking trends and creating local trends. With minimal resources, a

Table 1. Russia case study analysis in 2016 U.S. election Source: Lt. Col. Jarred Prier, U.S. Air Force

Types	Examples
Propaganda narratives	<ul style="list-style-type: none"> • Anything discrediting Hillary Clinton • News media hides information • Politicians are rigging the system • Global elite trying to destroy the world • Globalism is taking jobs and destroying cultures • Refugees are terrorists • Russian foreign policy is strong on anti-terrorism • Democrats and some Republicans want WWII with Russia
True believers	Alt-right, some Bernie Sanders supporters, followers of InfoWars and Breitbart, 4Chan and /pol/ users
Cyber warriors	Hackers and professional trolls
Bot network	Large, sophisticated network of leveraged cyber warriors and true believer accounts to create the "Deplorable Network"



Russian journalist Roman Shleykov, seen here at the *Novaya Gazeta* newspaper offices in Moscow, is one of at least 200 journalists worldwide who've been targeted by the Russian government-aligned hacking group known as Fancy Bear. THE ASSOCIATED PRESS

small group can create a bot network to amplify its message. Second, scores of people with exposure to social media are vulnerable to online propaganda. In this regard, state actors can use the Russian playbook. Russia will likely continue to dominate this new battlespace. It has intelligence assets, hackers, cyber warrior trolls, massive bot networks, state-owned news networks with global reach, and established networks within the countries Russia seeks to attack via social media. Most importantly, the Russians have a history of spreading propaganda. After the 2016 U.S. elections, Russian trolls worked toward influencing European elections. They have been active in France, the Balkans and the Czech Republic using active measures and coercive social media messages, as Anthony Faiola describes in a January 2017 article for *The Washington Post*.

CONCLUSION

Propaganda is a powerful tool and, used effectively, it has been proven to manipulate populations on a massive scale. Using social media to take command of the trend makes the spread of propaganda easier than ever before for both state and nonstate actors.

Fortunately, social media companies are taking steps to combat malicious use. Facebook is taking action to increase awareness of fake news and provide a process for removing the links from the website. Twitter has started discreetly removing unsavory trends within minutes of their rise in popularity. However, adversaries adapt, and Twitter trolls have attempted to regain command of the trend by misspelling a previous trend once it is taken out of circulation.

The measures enacted by Facebook and Twitter are important for preventing future wars in the information domain. However, Twitter will also continue to have problems with trend hijacking and bot networks. As demonstrated by #PrayforMizzou, real events happening around the world will maintain popularity as well-intending users want to talk about the issues. Removing the trends function

could end the use of social media as a weapon but doing so could also devalue the usability of Twitter. Rooting out bot accounts would have an equal effect since that would nearly eliminate the possibility of trend creation. Unfortunately, that would have an adverse impact on advertising firms that rely on Twitter to generate revenue for their products.

With social media companies attempting to balance the interests of their businesses and the betterment of society, other institutions must respond to the malicious use of social media. In particular, the credibility of our press has been put into question by social media influence campaigns. For instance, news outlets should adopt social media policies for their employees that discourage them from relying on Twitter as a source. This will require a culture shift within the press and, fortunately, it has gathered significant attention at universities researching the media's role in influence operations. It is worth noting that the French press did not cover the content of the Macron leaks; instead, the journalists covered the hacking and influence operation without giving any credibility to the leaked information.

Finally, elected officials must move past the partisan divide of Russian influence in the 2016 U.S. election. This involves two things: first, both political parties must recognize what happened — neither minimizing nor overplaying Russian active measures. Second, and most importantly, politicians must commit to not using active measures to their benefit. Certainly, the appeal of free negative advertising will make any politician think twice about using disinformation, but a foreign influence operation damages more than just the other party, it damages our democratic ideals. The late U.S. Sen. John McCain summarized this sentiment well at a CNN Town Hall: “Have no doubt, what the Russians tried to do to our election could have destroyed democracy. That’s why we’ve got to pay . . . a lot more attention to the Russians.”

This was not the cyber war we were promised. Predictions of a catastrophic cyber attack dominated policy discussion, but few realized that social media could be used as a weapon against the minds of the population. Russia is a model for this future war that uses social media to directly influence people. As technology improves, techniques are refined and internet connectivity continues to proliferate around the world, this saying will ring true: He who controls the trend will control the narrative — and, ultimately, the narrative controls the will of the people. □

This is an abbreviated version of an article published in *Strategic Studies Quarterly*, Vol. 11, No. 4.



LISTENING

Without

PREJUDICE

USING BLOCKCHAIN TECHNOLOGY TO COUNTER PROPAGANDA IN A 'FAKE NEWS' ERA

By Maj. (Ret.) Susan N. Osembo, Kenya Ministry of Defence

Joseph Goebbels, the Reich minister of propaganda in Nazi Germany from 1933 to 1945, is credited by many authors as the father of modern-day propaganda. The 1950 article, *Goebbels' Principles of Propaganda*, has 19 principles he used to conduct propaganda campaigns, according to the article's author, Yale psychology Professor Leonard Doob. These principles are still widely used, albeit through a more pervasive medium — the internet — and have led to a “fake news” crisis. It is difficult to attribute the term fake news to a specific person or organization because it quickly evolved in meaning and context and wasn't used much before the 2016 United States presidential election. At least 100 fake news websites that were reporting false stories about the U.S. election were discovered to have been registered in Veles, North Macedonia, according to the BBC. People in Veles were using the election, a hot and contested topic, to generate advertising revenue by driving internet traffic to their websites.

There has since been a proliferation of fake news, primarily of a political nature, appearing on social media and in the traditional news media. The BBC has questioned whether fake news is propaganda or online opinion, and whether people deliberately put out news to earn money online or if news agencies are simply making mistakes. Whichever the case, it is in the best interests of every government to understand and confront the fake news phenomenon. France, Malaysia, Singapore and the United Kingdom, among other countries, have embarked on efforts to enact regulations to curtail the fake news menace.

There have been various proposals on how to deal with fake news. The Brookings Institution proposes measures that would support investigative journalism, reduce financial incentives for fake news and improve digital literacy among the public. The idea of supporting investigative journalism to combat fake news is echoed by Bruce Mutsvairo and Beschara Karam in their book *Perspective of Political Communication in Africa*.

The BBC suggests third-party fact-checkers review social media and the use of algorithms to detect fake news. Bruce Bartlett, in his book *The Truth Matters: A citizen's guide to separating facts from lies and stopping 'fake news' in its tracks*, also supports fact-checking through the use of journalistic links to credit sources and give credibility to the news. The BBC further points to the importance of educating people about fake news and how to spot it. From these suggestions, it is clear that the problem isn't really the proliferation of fake news, but the lack of a system, especially on the internet, to separate fake news from the truth. This article attempts to discuss the possibility of blockchain technology as the missing link between online audiences and their ability to differentiate true and reliable sources of news from fake news.

THE SYSTEM ENSURES THAT ONLY VALID TRANSACTIONS ARE POSTED, I.E., A BLOCK CAN ONLY BE ADDED TO THE CHAIN AFTER IT HAS BEEN VERIFIED BY USERS IN THE BLOCKCHAIN NETWORK.

BLOCKCHAIN

In very simple terms, blockchain technology can be described as a master ledger that contains a series of transactions and that is distributed among a series of nodes (computers). Each node in a blockchain network is independent and is considered a “peer,” i.e., of equal status, authority and privileges over transactions in the network. Peer-to-peer networks do not have the inherent dangers associated with a centralized system, which, when attacked, compromises every computer in that network.

Blockchain technology has three distinct advantages that are relevant to the discussion of fake news: self-regulation, verifiability and trust. Each peer node has a private key that is used to approve transactions. Further, for a transaction to be approved, there must

be a consensus of nodes. It is therefore extremely difficult for a rogue node to invent a transaction and approve it because there are usually thousands of nodes in different geographical locations around the world, and infiltration of all such nodes is almost impossible and would also require an extra powerful computer. Because of this, blockchains are self-regulatory, a key aspect for an independent media and for countering fake news. Also, a transaction can only be posted on the master ledger if nodes verify such a transaction. The system ensures that only valid transactions are posted, i.e., a block can only be added to the chain after it has been verified by users in the blockchain network. And lastly, the element of trust is underscored by the fact that the master ledger records all changes. Every node has access to the distributed master ledger, and any new transaction or change is added as a new “block.” All details of all changes made from the time the original block was established are available to anyone in the network.

BLOCKCHAIN APPLICATION

Although blockchain technology can be applied in many ways, this article focuses on four applications that make it a unique solution for dealing with fake news. First, blockchain can improve the media's self-governance based on the system's transparent nature. Because all transactions in a blockchain are available to everyone on the network, and because it is almost impossible for a transaction to be approved without consensus, blockchain makes it difficult for fake news to exist and thrive.

Second, blockchain can guarantee the anonymity of whistleblowers or news sources, thus encouraging people with information to come forward and share their stories without fear of reprisals. While blockchain transactions are available for all to see, the users' identity can be anonymous. A critique of this application is that it may also encourage people to come forward with fake news, which defeats the purpose of using blockchain to counter fake news. However, this is mitigated in three ways. First, a time stamp and location of a blockchain transaction can be used to verify information. Second, blockchain transactions must be validated by nodes before approval. In simple terms, a fake story is unlikely to be approved if other nodes detect it is false. It is therefore unlikely for a random person to fabricate fake news and have that validated in a blockchain network. Third, through blockchain a person can have an online identity, anonymous or otherwise, that is identifiable with the use of a private key. It is therefore possible for an anonymous source to prove its identity to the media. For example, a spy wanting to disclose confidential information anonymously can verify his or her identity to media sources. This enables the media to also verify the legitimacy of the spy's sources.

The third blockchain application relevant to combating fake news is the ability to have direct transactions without a middleman, i.e., directly between nodes. This reduces possible journalistic distortions to favor one side of the news. For example, a government can release news directly to the public without going through media agencies (keeping in mind that the information must be verified by other nodes in the blockchain network to minimize the effects of government propaganda). Further, in the current era of smartphones, the public can be news sources apart from the traditional news media. Blockchain ensures that the public can share local news with others while limiting the emergence of fake news from nontraditional media.

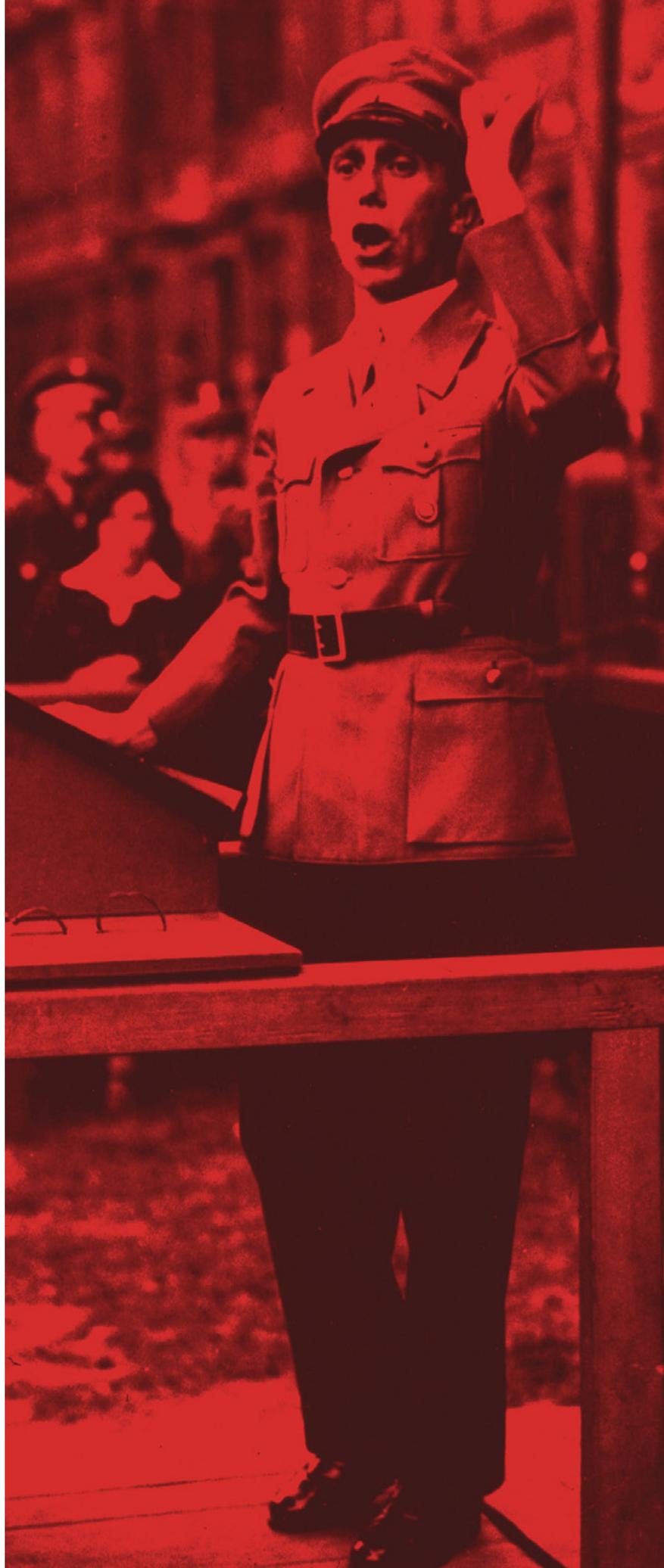
Lastly, because blockchain information is verified, both the government's and the media's ability to predict news and events is greatly improved, helping them prepare for every eventuality. For example, verified news reports on certain weather conditions or patterns can help humanitarian relief efforts. Predictability also enhances the utilization of resources on identified priorities.

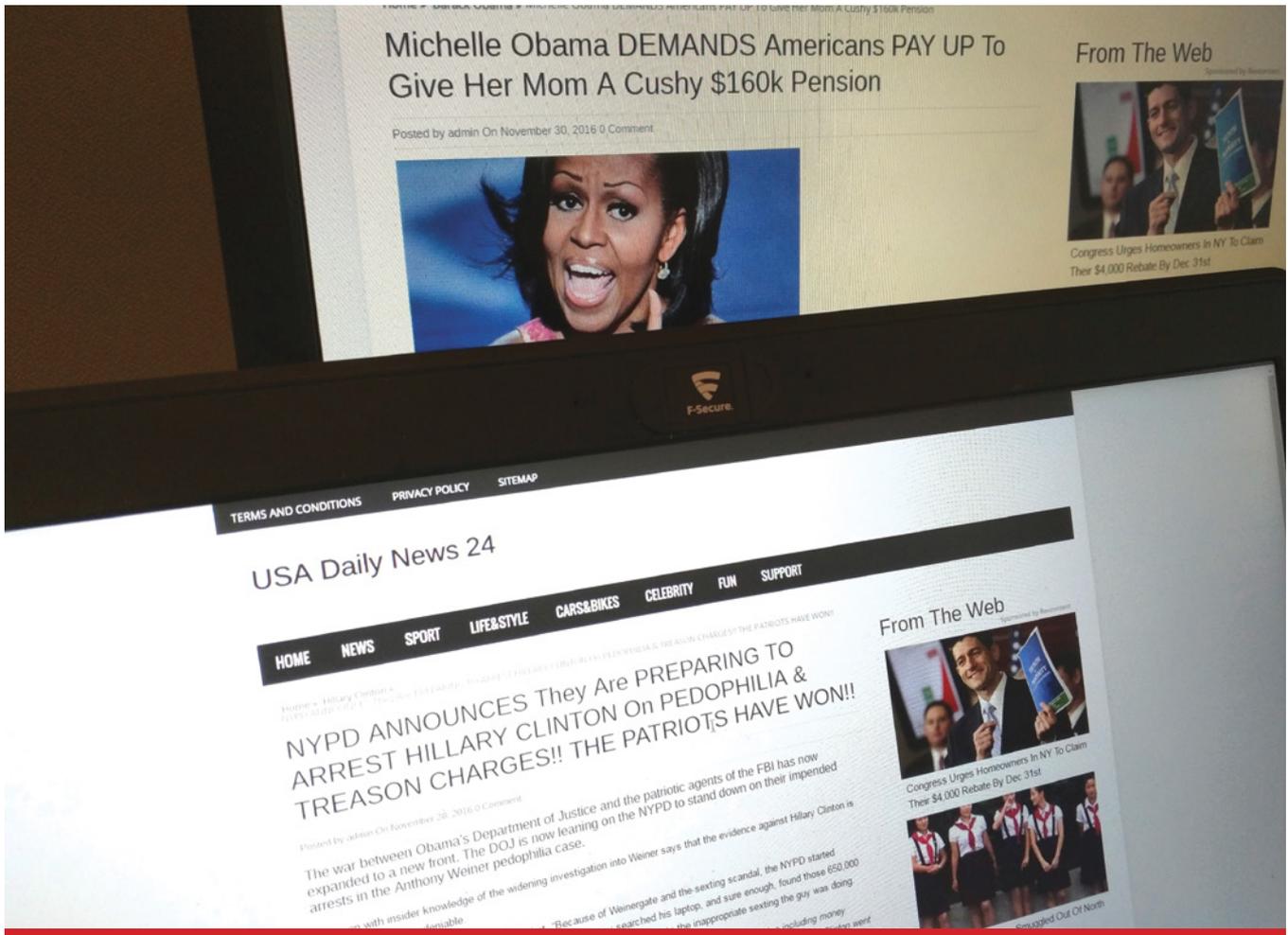
PROPAGANDA PRINCIPLES

Modern-day fake news operates on the same propaganda principles ascribed to and documented by Goebbels. Therefore, it is important when discussing fake news to analyze the principles that Goebbels used to spread propaganda within Nazi Germany and abroad.

A key tenet of Goebbels' principles is that there must be a central body, with access to intelligence information, in charge of propaganda. The fewer people with access to that intelligence, the easier it is to manipulate the public. Blockchain promotes validation and transparency of information within the blockchain network and therefore easily counters this principle. Also, blockchain provides an option for anonymity, ensuring that people with confidential information can share it freely without fear of reprisals, although this increases the danger of divulging confidential intelligence into the public domain without consideration of the consequences. According to the BBC and CNN, for example, the U.S. claimed that a Wikileaks' release of confidential diplomatic

Joseph Goebbels, the German minister of propaganda from 1933 to 1945, is considered the father of modern-day propaganda tactics. Here, he addresses storm troopers in Berlin in 1934. THE ASSOCIATED PRESS





This 2016 photograph shows bogus stories from USA Daily News 24, a fake news site registered in Veles, North Macedonia. An analysis found roughly 200 U.S.-oriented sites registered in Veles, which emerged as an unlikely hub for distributing disinformation on Facebook.

cables endangered U.S. operations and foreign policy efforts. Even Goebbels noted the importance of taking into account the consequence of propaganda before effecting it. A key question that arises, given the peer-to-peer nature of blockchain, is whose responsibility it will be to determine the timing of news and the consequence of releasing that news at a specific time, i.e., will it make the situation better or worse?

According to Goebbels, “black propaganda,” which is propaganda with disguised sources, can be considered more credible than “white propaganda,” which openly reveals its origins. In other words, propaganda supporting a government may be more believable if it comes from a source other than the government. This is also linked to his principle of propaganda being credible. Blockchain’s transparency makes it difficult for people to believe rumors when a credible and verifiable news system is in place.

Goebbels had two principles relevant to attention-grabbing headlines. First, that propaganda must be projected through an attention-grabbing medium and must provoke the targeted audience. Second, propaganda must label people with distinctive phrases and slogans that are easy to remember and that evoke the desired responses from the

audience. This has indeed been a legacy of fake news, which uses attention-grabbing headlines to arouse people’s emotions and increase their probability of clicking on a link. Because a majority of online advertisement revenues are based on the pay-per-click model, attention-grabbing headlines are designed to drive maximum online traffic. This commercial incentive is not inherently a bad thing, given that the news media needs to generate revenues to exist, but blockchain can ensure that the information being passed along is real. A challenge that may arise is where a misleading headline links to a true story. It is not clear whether blockchain transactions would include the verification of headlines. Unlike transactions such as bitcoin sales that are easy to verify and approve, approval of media stories and headlines may be more complicated since news depends on context and may be limited to the knowledge of a local population. Of course, opportunities exist for local media blockchains that could verify local stories, but that would involve getting a critical mass of local people and organizations on board. This involves the creation of an incentive that would motivate people to contribute to the blockchain.

SHORTCOMINGS

While blockchain addresses most fake news concerns, it is by no means a silver bullet. A major blockchain weakness also happens to be its greatest strength: It is a distributed system, in which each node has equal power and privilege. There is no central authority or figure to determine the timing of news, which can have real and devastating consequences.

BLOCKCHAIN TECHNOLOGY ALSO OFFERS A POSSIBLE SOLUTION BECAUSE IT PROMOTES SELF-REGULATION OF THE MEDIA AND VERIFIABILITY AND TRUST OF NEWS SOURCES.

Also, blockchain doesn't have a remedy for every type of propaganda. For instance, one of Goebbels' principles is that propaganda may be facilitated by leaders with prestige. These leaders can be viewed as credible news sources. For example, any official statement by a country's head of state can be new information that cannot be verified because that official is also deemed as a news source. While blockchain may later identify a false claim, and take away such a person's credibility, there remains the possibility of fake news being passed on as truth by leaders with prestige.

Additionally, blockchain assumes that there are no political or social enmities across societies and that access to information is indiscriminate. In a world divided by religion, politics, and economic, social and cultural metrics, access to information by one party may give that party an undue advantage. Therefore, access to validated news may end up being used with adverse repercussions.

Another of Goebbels' principles is that credibility determines the truth or falsity of propaganda. Expediency, and not morality, matter because truth sometimes damages credibility, i.e., some truths may

appear to be untrue because of strong beliefs held by people. Therefore, there is a chance that people may still refuse to believe truth even when it has been verified because it goes against a deep-seated belief. In his book, *The Knights of Bushido: A History of Japanese War Crimes During World War II*, Edward Russel notes that there are some people who refuse to believe facts even when presented with evidence. Hugo Mercier and Dan Sperber also note in their book, *The Enigma of Reason*, that human reasoning is biased and sometimes the bias overpowers rational thinking. Therefore, blockchain may help curb but will not totally erase the believability of fake news.

Lastly, a credible local and international media blockchain, or different blockchains, requires incentives for the media and the public to use it. Recent research by the Brookings Institution shows that most online users get their news through social media. Therefore, it is important to find ways to integrate blockchain with social media or to get people to shift from social media to a particular blockchain for their news. There is also a need to create an incentive that is strong enough to encourage global collaboration by media outlets.

CONCLUSION

The proliferation of fake news has largely been blamed on echo chambers on social media platforms where users reinforce and encourage their beliefs, whether true or false. Fake news has also thrived in the absence of a system to validate news sources and in the 24/7 news cycle, and through traditional media and social media. Various solutions have been proposed to deal with the fake news crisis, including support for investigative journalism and fact-checking.

Blockchain technology also offers a possible solution because it promotes self-regulation of the media and verifiability and trust of news sources. Blockchain counters most of the principles of propaganda advanced by Goebbels that promote the proliferation of fake news. However, blockchain still faces challenges in combating fake news. Blockchain is a peer-to-peer network with no centralized decision-making authority, and it may favor one person or group over another if verified information about an opposing person or group is not made available to the opposing person or group. There is also no guarantee that people will believe the truth if it contrasts with a deep-seated belief. There should also be incentives that encourage media outlets and the public to come together to provide and consume news through blockchains. Regardless of these challenges, blockchain technology presents an exciting opportunity for combating fake news in an era where anyone with a mobile phone can be an instant journalist. □





People in Skopje wave the Macedonian and European Union flags at a rally before a referendum in 2018 on whether to change the country's name to "Republic of North Macedonia." AFP/GETTY IMAGES

A DIFFICULT PASSAGE

North Macedonia's turn to the West

By Dr. Bekim Maksuti and Dr. Sebastian von Münchow

IN March 2019, U.S. Army Gen. Curtis Scaparrotti, then NATO supreme allied commander Europe, reported that Russian disinformation campaigns and support to anti-NATO factions had increased over the previous months. Appearing before the U.S. House Armed Services Committee, he expressed concerns “about the Balkans and the increased malign influence over the past year.” Heightened Russian involvement and meddling has occurred in North Macedonia as the country of more than 2 million inhabitants has worked to achieve NATO membership, just as Russian activity was seen in other Western Balkan states as they moved toward joining NATO.

North Macedonia is located in a sometimes uneasy neighborhood in Southeastern Europe bordering Serbia, Greece, Bulgaria, Albania and Kosovo. While the citizens represent nine recognized ethnicities, Macedonian and Albanian are predominant, with Albanians residing mostly in the country's western part. Since independence from Yugoslavia in 1991, North Macedonia has had to overcome many difficulties with NATO and European Union member states on its path to membership in those institutions. The major concern was the decadeslong naming dispute with Greece, which the Greek prime minister and the newly elected prime minister of Macedonia settled in 2018 when they signed the Prespa Agreement changing Macedonia's name to North Macedonia.

Previously calling itself the Republic of Macedonia, it was the third nation after Slovenia and Croatia to declare its sovereignty from the Socialist Federal Republic of Yugoslavia in 1991, and Yugoslav troops were peacefully removed. The United Nations Security Council decided to launch the United Nations Protection Force in December 1992 to monitor and report any developments in the areas along the border and within the newly formed state. In 1995, the mission turned into the United Nations Preventive Deployment Force, which operated until 1999. Both missions are still regarded as having helped ease disintegration tensions and prevent aggressive Serbian engagement in Macedonia. In 1993, Macedonia

became a U.N. member under the name the Former Yugoslav Republic of Macedonia (FYROM) as a result of its disputes with Greece. Athens argued that its northern region is also called Macedonia and that using that name illegitimately claimed the cultural and historical heritage of ancient Macedonia, including Alexander the Great.

In February 1994, tensions rose when the Greek government closed the harbor of Thessaloniki to Macedonian trade. The economic impact was severe because more than 75% of Macedonia's external trade transited the harbor. The embargo was lifted when the EU hinted at initiating judicial measures against Greece due to unfair trade sanctions. After several years and changes of governments, relations between the two countries normalized, although the naming conflict remained unsettled, and Athens continued to make clear that it would use its veto powers to block Skopje's accession to the EU or NATO.

The crisis in Kosovo that began in February 1998 opened another chapter. Armed conflict and the NATO air campaign against Yugoslavia in 1999 caused waves of Kosovo-Albanian refugees to seek protection in Macedonia. The war ended in the summer of 1999, but in early 2001 the more than 500,000 ethnic Albanian citizens of Macedonia began asking for more rights regarding language, education and political representation, and a limited armed conflict ensued. A massive diplomatic intervention by the U.S. ended the hostilities. The Ohrid Framework Agreement was signed in August 2001, stipulating a just distribution of powers and rights between majority and minority citizens. Since that time, there has been a coalition of parties representing the strongest votes of each community. Notwithstanding, and avoiding generalizations, ethnic Albanians are considered to identify more with the U.S., NATO and the EU, whereas ethnic Slavic Macedonians, representing the majority, are divided on the matter.

Skopje applied for membership to the EU in March 2004 and had already attained the official status of an EU candidate country by 2005. Efforts were also made to join NATO, but due to Athens position, the 2008 NATO summit called for the resolution of the naming dispute as a *conditio sine qua non* for joining the Alliance.

During the Nikola Gruevski-led governments of the VMRO-DPMNE (Internal Macedonian Revolutionary Organization – Democratic Party for Macedonian National Unity) between 2006 and 2016, Macedonia turned inward. A phased Euro-Atlantic integration fatigue among Brussels, Washington and Skopje followed. When Macedonia made international headlines, it was usually about shootouts, road blockades, wiretapping scandals, corruption and reemerging tensions between the major ethnicities. The construction of huge statues of Alexander the Great and his family members in Skopje's city center refueled the disputes between Greece and Macedonia. However, after a politically troubled winter, a Social Democrat-led government was formed in early 2017.

New Prime Minister Zoran Zaev came into office at the end of May 2017 and made it clear that he wanted to settle the naming question with his counterpart, Greek Prime Minister Alexis Tsipras. Following new negotiations, in June

2018 the heads of state signed the Prespa Agreement, named after a lake between Greece and Macedonia. Under the terms of the agreement, Skopje would accept the new name, Republic of North Macedonia, but this stipulation was not accepted by nationalist-minded protagonists from the ethnic majority population. Citizens of Albanian background were mostly neutral since they did not consider themselves stakeholders in a dispute over Hellenic heritage. A referendum was held on the proposed name change in September 2018. Zaev expressed his strong belief in a European Macedonia before the referendum: "We want the future; we want a European Macedonia! It is our responsibility to secure a future for our children and their children."

It was during this time that Moscow began to fear losing its role as a major actor in Macedonia after enjoying 10 years of special attention from the previous, rather nationalistic government. After Macedonian voters opted for a change of government in 2018, the Kremlin acted. Fearing that the dispute settlement between Skopje and Athens would lead to North Macedonia's full integration into trans-Atlantic security structures, the Kremlin tried all angles to create division within Macedonia and encourage ethnic Slavic Macedonian affinity toward Russia, ranging from touting Slavic brotherhood to advocating for the benefits of united Orthodox Christianity. Russia fueled the inner-Macedonian ethnic friction between a strong Albanian minority and a Slavic Macedonian majority.

Moscow's communication strategy was composed of two essential parts: propaganda and disinformation — with propaganda being the selective usage of information or arguments to promote or undermine a political actor or a political aim, and disinformation being politically driven communication designed to generate a certain atmosphere within the public. Both were used by Russia to intervene in North Macedonia's Western-integration process. This communication strategy was generally targeted against NATO and the EU. The main aim was to undermine the credibility of political actors, especially the government, and to disturb the functionality of state institutions. Russia's communication strategy did not necessarily create new facts or falsehoods but rather concentrated on already existing distrust of and resentment against European and Western societies. The Kremlin knew that a nation under distress and suffering weak institutions, oligarchic structures, politicized media and a high level of corruption is particularly vulnerable to these kinds of attacks. As an example of Russia's influence campaign, Russia Today (an international television network funded by the Russian government and directed at audiences outside of Russia) published on its website several reports with anti-NATO and anti-EU views during the period when the naming referendum was being debated.

Russia tried to make use of its power and influence in Greece as well. In July 2018, the Greek government expelled two Russian diplomats and barred two others from entering the country, accusing them of interfering in Greek politics by supporting members of the opposition. Russia opposed the Prespa Agreement by offering bribes and encouraging demonstrations against it. Moscow became less subtle and raised its voice openly when prospects of Euro-Atlantic integration



Workers hang a sign in February 2019 with the country's new name after it was changed to North Macedonia. THE ASSOCIATED PRESS

became far more likely. The Russian government had already warned Macedonia that its membership in NATO would have a negative impact on regional security and bilateral relations. Oleg Scherbak, then Russian ambassador to Macedonia, threatened during a press conference that if war broke out between NATO and Russia, as a NATO member, Macedonia would be a legitimate target.

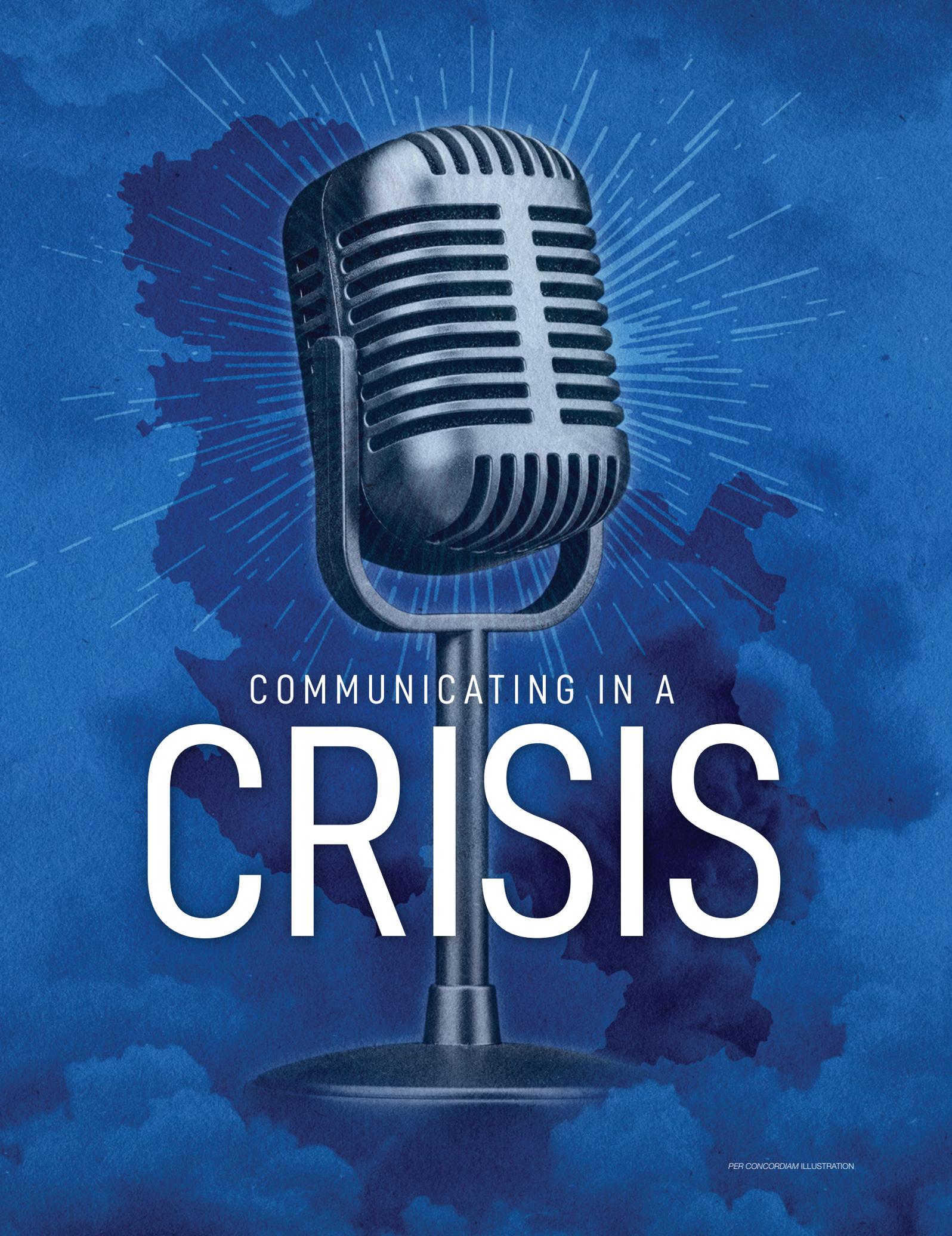
Russia's strategic communications against the referendum may have worked. A boycott of the referendum urged by Russian-supported nationalists lowered voter participation to 36%, falling far short of the necessary quorum of 50%. While the Western-minded ethnic Albanian population was almost unanimously in favor of the new name, the majority ethnic Macedonian population remained divided. Nevertheless, over 90% of votes cast favored the name change to North Macedonia.

The lack of a quorum moved the issue to the Parliament in Skopje on January 11, 2019, where 81 of 120 representatives, just barely the two-thirds majority required, voted in favor of the change. Local politicians representing all Macedonian communities, Western diplomats and representatives from both of the Brussels-based transnational institutions reacted with relief. The Greek Parliament's approval followed two weeks later. And in February 2019, the Republic of Macedonia was renamed the Republic of North Macedonia. Greece signaled it would no longer block North Macedonia's

ambitions to join NATO. NATO's commitment and willingness have already been demonstrated by allowing North Macedonia to send observers to official sessions.

At the NATO summit in London in December 2019, North Macedonia's chances of becoming the Alliance's 30th member were high until the political turmoil of Spain's parliamentary election resulted in a postponement of the process. Before NATO convened in England to talk about the next steps, the European Council met in Brussels, where the start of membership negotiations was on the agenda. Disappointingly, France blocked the launch of negotiations. But the government policy of North Macedonia remains that there is still no alternative to EU membership.

In sum, North Macedonia's decision in favor of a new name was primarily a decision in favor of Euro-Atlantic integration. And even though Russia interfered, the path toward becoming a Western-oriented country was chosen. Of utmost importance will be inner unification of the country so that there is a strong consensus among all ethnicities and political parties in support of the chosen path. Building North Macedonia into a strong NATO and EU member state should be understood as an opportunity to challenge Russian influence in Europe. Like Russia's failed efforts in Montenegro in 2016, Russian President Vladimir Putin failed to achieve his goals in Skopje. The people of North Macedonia chose a different path for themselves and their children. □



COMMUNICATING IN A

CRISIS

Lessons from the May Floods in Serbia

By **Želimir Kešetović**, University of Belgrade, faculty of security studies; **Predrag Marić**, Republic of Serbia, assistant minister of interior; and **Vladimir Ninković**, University of Belgrade, faculty of security studies

Numerous case studies show that crisis communication can prevent the onset or escalation of a crisis, impact its course, and reduce or increase the duration and severity of consequences as well as the degree of potential reputational damage to crisis actors. Therefore, an organization's communication with the public is among the key elements of crisis management.

Even though literature deals mainly with crisis communications in the corporate sector, the observations hold true for the public sector as well. Legal responsibility and accountability, as well as public scrutiny, have made those who implement public policy important actors of crisis communications, especially in a sensitive field such as emergency management. However, in practice, there are significant differences in the implementation of crisis communications in various political contexts, not only on a technical, normative or operational level, but also on a more abstract, symbolic, meaning-making and meaning-shaping level.

In Serbia, public institutions and units in charge of crisis/emergency management are undergoing a transformation. The state administration is gradually adopting the concept of public service and the doctrine of "new public management" that argues that ideas used in the private sector may be successfully implemented in the public sector. Countries in transition undergo a deep transformation in all areas of governance, undertaking efforts to implement democratic institutions and overcome the burden of authoritarianism. This process includes changes in the value system, state and public priorities, and structures.

By its very nature, transition is a source of vulnerability. A move from a centrally planned economy to a market economy, accompanied by the reconfiguration of social structures and status arrangements, often becomes a source

of disappointment and frustration to the public. For security, legal and ethical reasons, citizens need to be aware of risks, informed during an ongoing crisis and updated about recovery efforts. The public's security is directly dependent on the speed and accuracy of information. During emergency situations, uniform information with synchronized and harmonized responses is critical. Inadequate responses by the government and rescue agencies can exacerbate an emergency, cause a reputational crisis and increase the possibility of turning a crisis into a disaster. Therefore,



A truck passes by a flooded open coal mine pit in Kostolac, 70 kilometers east of Belgrade, Serbia, in July 2014, two months after devastating floods hit the country. THE ASSOCIATED PRESS

adequate and timely communication among various levels of decision-makers — national, regional and local, as well as the public and private sectors — is of the utmost importance.

The significance of an informed public and the problems stemming from the lack of it were visible during the

May 2014 floods that hit Serbia and neighboring countries. According to media reports, many people — without any apparently justifiable reason — did not comply with evacuation orders. The public reaction — either panic or a controlled response — to a situation greatly depends on the capacity and capability of crisis managers to share information with citizens in a timely and appropriate manner, which was not always the case. Additionally, politics and the media (including the internet and social media) were occasionally part of the problem, rather than part of a solution.

Politicization and sensationalism were unfortunately prevalent in the media. Local authorities were an important, but not always visible, piece in that chaotic puzzle of untimely, sensationalist and often confusing information. Sector for Emergency Management, a specialized unit of the Serbian Ministry of Interior, coordinates the activities of all state and civil society institutions involved in emergency and disaster management at all levels of political territorial organization. The sector has operational and expert bodies for coordinating and managing crisis response. They are permanent bodies established for municipalities and cities by their respective assemblies, for administrative districts by the national emergency

management headquarters, and for the autonomous provinces and republics by their respective governments. If needed, headquarters establishes auxiliary teams to execute specific tasks related to protection and rescue.

To assess the perception of their own communication efforts and relationships with the media and political actors, a questionnaire consisting of 25 questions was sent to the emergency management headquarters of 31 municipalities and nine cities affected by the floods and in which a state of emergency was called. The results are arguably skewed — the survey was not anonymous, and the respondents received the questionnaire through a state institution — but they may give an initial insight into the communication practices of local self-government units and their relationships with the media, policymakers and the public.

RISK, CRISIS AND DISASTER COMMUNICATION

Contemporary society is not only a “risk society,” but an informational society as well. We rely on written and verbal messages on a nearly constant basis to evaluate the world and the risks associated with living in it, according to risk and crisis communications expert Pamela Ferrante Walaski. Linguistics and communication theory in the late



People sit in a boat after being evacuated from their houses by Serbian Army soldiers in the town of Obrenovac, 30 kilometers southwest of Belgrade, on May 16, 2014. REUTERS

20th century showed that messages do not only have a semantic, but also a pragmatic function, which particularly comes to prominence in communicating risks and crises. We now know that messages are often used to influence their recipients to behave in a certain way, as well as to change their perception. Risk and crisis communications is the process of communicating information, with a view toward influencing the public to prepare and respond better and more efficiently during a negative event. The first attempts to systematize knowledge in this field may be traced to the Three Mile Island nuclear accident in the United States in 1979. However, a turning point occurred with the introduction of the World Wide Web and other forms of digital communication, triggering a substantial increase in the volume and type of messages available to the general public, according to Walaski.

A successful risk communication should pave the way for smooth implementation of disaster communications, as well as help the institutions in crisis by strengthening their reputation and building trust with various publics in the pre-crisis period.

Crisis communications are often lumped together with emergency and disaster communications because the differences are rather small. In practice, there is not much of a distinction — the public will need to be assured that the institutions know what they are doing, and the public will need to be reached through the media. In the case of natural disasters, some observers have suggested adopting a comprehensive approach that incorporates risk and crisis communications into a hybrid form known as CERC — Crisis, Emergency Risk Communications. In each of the four phases of emergency management (i.e., mitigation, preparedness, response and recovery), communication has different goals and implements various strategies. The mitigation and preparedness phases greatly overlap with risk communications because they are aimed at educating and informing the recipients about potential emergencies or disasters. Communications during disaster response provide critical information that the public can act upon to survive the disaster and access relief assistance, whereas in the post-disaster recovery phase, the focus is on informing the public of the types of recovery assistance, according to communications Professor Timothy Coombs. The aim of disaster communications is to get individuals and communities to act.

Disaster communications represent a logical continuation of risk communications that aim to “help risk bearers,

those who must face the consequences of the risk, become more comfortable with the risk,” Coombs writes. “Part of the risk communication process is explaining risks to risk bearers and trying to understand their concerns about the risks.” Risk communications are a dialogue between risk creators and risk bearers, in which state institutions often serve as an intermediary. Risk communications educate and inform the public about the sources of risk in their surroundings, the probability of a disaster and the consequences of a potential disaster before they seem relevant, i.e., when everything is still “normal.”

Therefore, in theory, efforts invested in risk communications during normal times should build trust between stakeholders through dialogue and make the public better educated and informed about potential disasters, which would result in improved readiness. A successful risk communication should pave the way for smooth implementation of disaster communications, as well as help the institutions in crisis by strengthening their reputation and building trust with various publics in the pre-crisis period.

CRISIS COMMUNICATIONS IN THE PUBLIC SECTOR

Risk and crisis communications may be considered subfields of risk and crisis management, which according to Walaski include common themes of evaluation and control of risks and crises to bring about a successful outcome, or at least to minimize the damage from an event. Crisis management and crisis communications have been viewed mainly within the paradigm of corporative security. However, not only are organizations and big corporations placed at risk by emergency situations, crises and disasters, but so are their surroundings. As Coombs states: “At its heart, crisis management is about making the world a safer place.” This holds true for large-scale, fundamental crises that lead to emergency situations, which can consequently become disasters — be it natural or man-made. As far as disaster management by public organizations is concerned, the communicative aspects of crises have been neglected for many years. However, the increased number and magnitude of crises, as well as public criticism toward governmental crisis communication, has placed the topic firmly on the agenda, according to Pauliina Palttala, a disaster management expert.

“In general, the management of natural disasters and public health emergencies has always included a significant communication component in the form of warnings, risk messages, evacuation notifications, messages regarding self-efficacy, information regarding symptoms and medical treatment,” according to a paper in the *Journal of Health Communication* by Barbara Reynolds and Matthew Seeger. Different kinds of crises, however, manifest different forms of threat and different communication exigencies. For instance, floods are usually accompanied by recommendations that residents drink bottled water or boil water to avoid waterborne pathogens. In the case of flood risks and other potential natural disasters, it is impossible to establish a dialogue with the forces of nature. The public will look to state, regional and local authorities to provide them with



Aerial view of a flooded area of Obrenovac on May 19, 2014. THE ASSOCIATED PRESS

enough information and to instruct them on how to better prepare and respond more efficiently if the disaster strikes. If that is lacking, a natural disaster may trigger a reputational crisis for all levels of government. This holds true even more in countries in transition where the level of trust in the government and politicians is often very low.

A low level of trust makes communication efforts ineffective, while lack of communication or insistence on one-way communication in normal times decreases the level of trust. This vicious circle may be broken, although it takes time for trust to be built. While the transition from trust to distrust is often rather abrupt and is reflected in a crisis of confidence, the regaining of trust appears to be a slow and gradual process, according to a paper by Wouter Poortinga and Nick Pidgeon in the journal *Risk Analysis*. The ability to establish constructive communication will be determined by whether the audience perceives the communication and communicator to be trustworthy and credible. This is not to say that uncritical, emotional acceptance is desirable, at least not in democratic societies.

Along a continuum between unconditional trust and total rejection, a healthy type of distrust can be found — critical trust. For police work, including the work of emergency response units, a high level of trust is a necessary precondition for citizens to accept and cooperate with them. Without this acceptance and cooperation, the police cannot be efficient and effective. The existence of trust in institutions, in particular first responders, becomes evident during emergencies and disasters. For instance, if community members are told to evacuate or to shelter in place, they will be more compliant if they believe the suggested behavior will work. So, if the risk communication was effective

(which serves not only to inform and educate the public, but also to build mutual trust), emergency directions should produce better results than if no attention was given to risk communications in the community before the crisis, according to Coombs. During the May floods, one of the main problems that Sector for Emergency Management encountered was noncompliance with orders for evacuation in the flooded areas. Indeed, noncompliance, i.e., the question: “How do we get people to behave appropriately during disasters,” has been identified as one of the largest gaps in international emergency management research, according to Linda Shevellar and Rebecca Riggs in a paper for *The Australian Journal of Emergency Management*. The answer to this question is complex and the findings of a pilot project by the two authors, who interviewed individuals who acted contrary to official messaging during floods in rural Australia, offer a good starting point for analyzing noncompliance during Serbia’s May floods. Among the identified drivers in their study were: the pull of attachment, the need for control, the moving from hardships toward pleasure and the power of identity.

Another issue that often becomes salient during emergencies is the spread of rumors. Nowadays, rumors can reach far more people than just 10 years ago, thanks to social networks that have become the main source of information, particularly for young people. According to communications Professor Kathleen Fearn-Banks, “The Internet is a great source of information and news, but it is an even greater source of misinformation and rumor. Opinion, guesses, assumptions as well as rumor present tragic consequences to people who are victimized because Internet users often believe everything they read is true.”

“ *The Internet is a great source of information and news, but it is an even greater source of misinformation and rumor.*”

- *Communications Professor Kathleen Fearn-Banks*

Various studies have shown that the most trusted source of information is other people, especially friends, whether real or Facebook ones, and that makes combating rumors and misinformation particularly difficult. As pointed out earlier, crisis communications during an emergency are aimed at helping the public take the correct action. However, Coombs writes, through the “new media,” or social media, the audience is starting to collect and exchange their own information and act on it as they see fit. In addition, it is difficult to enact laws against untrue or misleading information on various sensationalist websites, according to Walaski. In the case of natural disasters, there is frequently speculation regarding the withholding of information about casualty numbers, the spread of contagious diseases, and the inhumane conditions in which evacuees

must temporarily reside. Regardless of the genesis of the rumors, Walaski writes, it is crucial to treat their existence as a crisis and elevate their seriousness to prompt some type of action.

Because public institutions are often the subjects of communication during emergency situations, the politicization of their management and communication efforts is almost inevitable. This is even more prominent in countries where public institutions with important roles in emergency management are led by political appointees. The politicization in Serbia was visible in the way opposition parties and media unaffiliated with the government (in the case of Serbia, mainly weekly magazines, news websites and blogs) viewed the protection and rescue efforts of state and local authorities.



The damage is visible in Krupanj, southwest of Belgrade, on May 20, 2014, after the western Serbian town was hit with floods and landslides, cutting it off for four days. AFP/GETTY IMAGES



A Serbian police officer wades through a flooded street in the town of Lazarevac, south of Belgrade, on May 15, 2014. REUTERS

At the end of a crisis, theory says that it is important to adopt the “lessons learned.” Some communication efforts can be evaluated, but other more vague and symbolic ones are difficult to assess. Recently, there have been efforts to create “scorecards” or “indicators” that take into account the crisis phases and stakeholders. But their practical usefulness is yet to be evaluated.

MAY FLOODS — EVENTS AND MEDIA REPRESENTATION

May 14, 2014, marked the start of the heaviest flooding in Serbia and the region (including Bosnia and Herzegovina and Croatia) in the past 120 years, since the beginning of meteorological measurement. Within a day, the flood had caused three casualties, knocked out power and isolated several towns and villages.

On May 15 at 11 a.m., Serbian Prime Minister Aleksandar Vučić declared an emergency for the entire country. Flooding disrupted production in two coal mines supplying major power plants — Thermal Plant Nikola Tesla in Obrenovac and the Thermal Plant Kostolac. The highway connecting Belgrade with the third-largest city in Serbia, Niš, and with Macedonia and Bulgaria was flooded. The main railway line, connecting Belgrade with the Montenegrin port of Bar, was also interrupted. The worst affected municipalities — Loznica, Šabac, Sremska Mitrovica, Obrenovac and Kostolac — were near the river Sava and its tributaries (the Drina, the Kolubara, the Tisa and the Mlava). The Sava reached its peak near Šabac on May 18. A state of emergency was declared in nine cities and 31 municipalities.

The situations in Šabac, Obrenovac and Kostolac were the most dramatic. In those municipalities, important facilities were threatened by floodwaters: Zork, a chemical factory

in Šabac, and the coal-fueled thermal power plants and coal mines in Obrenovac and Kostolac that provide electricity for more than 60% of Serbia. In some areas, heavy rains triggered landslides. In the municipality of Krupanj, torrents, mudslides and landslides created infrastructure damage, and in Mali Zvornik, a hill threatened to slide into the river Drina and cut its flow. On May 20, a three-day mourning period was declared by the government. By May

Serbians are passionate users of social networks, in particular Facebook. This inevitably led to various rumors, many of which were related to conspiracy theories about the real scale of the disaster.

21, 32,000 people had been evacuated, 20,000 of them from Obrenovac. The role of local self-governing units (LSGUs) during floods and other natural disasters and emergency situations is detailed in legal and strategic documents (Law on Emergency Situations, Law on Local Government, National Security Strategy, National Protection and Rescue Strategy in Emergency Situations.). Even the Constitution of the Republic of Serbia stresses the importance of the role of local governments in the management of natural disasters. In cases when emergency situations exceed local capacities

— when a state of emergency is declared on a regional and/or national level — the local authorities will still be the main communicators and points of contact for the population.

During emergencies, the media frequently focused on the communication shortcomings of LSGUs, particularly on Obrenovac — the municipality that is nearest to Belgrade and where the biggest electrical energy provider in Serbia is based. Chronologically, the first issue that appeared in the media during the floods was the late activation of sirens, the early warning system, and the late call to evacuate the inhabitants of Obrenovac and the surrounding villages of Draževac, Veliko Polje, Konatice and Poljane. According to the reports, the alarm sirens were activated on May 16 around 5 a.m., when the flood wave had already entered the ground floor of a number of buildings in Obrenovac.

Even more problematic was the confusing information regarding evacuation. In a report by the head of the Department for Emergency Management of Belgrade, as well as in the conclusions of the emergency management of Obrenovac, it is stated that the Obrenovac emergency management headquarters ordered the evacuation of Draževac, Konatice, Poljane, Veliko Polje and a part of the village Piroman on May 15 at 10 a.m., while the evacuation of the hamlet of Šljivice was ordered the same day at 3 p.m. The report also states that on May 15 a negligible number of inhabitants were evacuated due to massive noncompliance, and that only after the president of Serbia visited the villages and spoke directly with the locals did the number increase. However, after the floods, in an interview for the CINS investigative journalism network, the mayor of Obrenovac stated that the orders from Belgrade City Headquarters for the evacuation of Poljane and Veliko Polje were given by telephone at 12 p.m. and 1:30 p.m. respectively, when the villages were already under water.

These examples show that there were obvious communication problems between various levels of governance, in this case between regional (Belgrade), municipal (Obrenovac) and local (emergency units in villages). That caused delays in crisis response and ineffective evacuation efforts, which in turn resulted in the inefficient use of human and material resources.

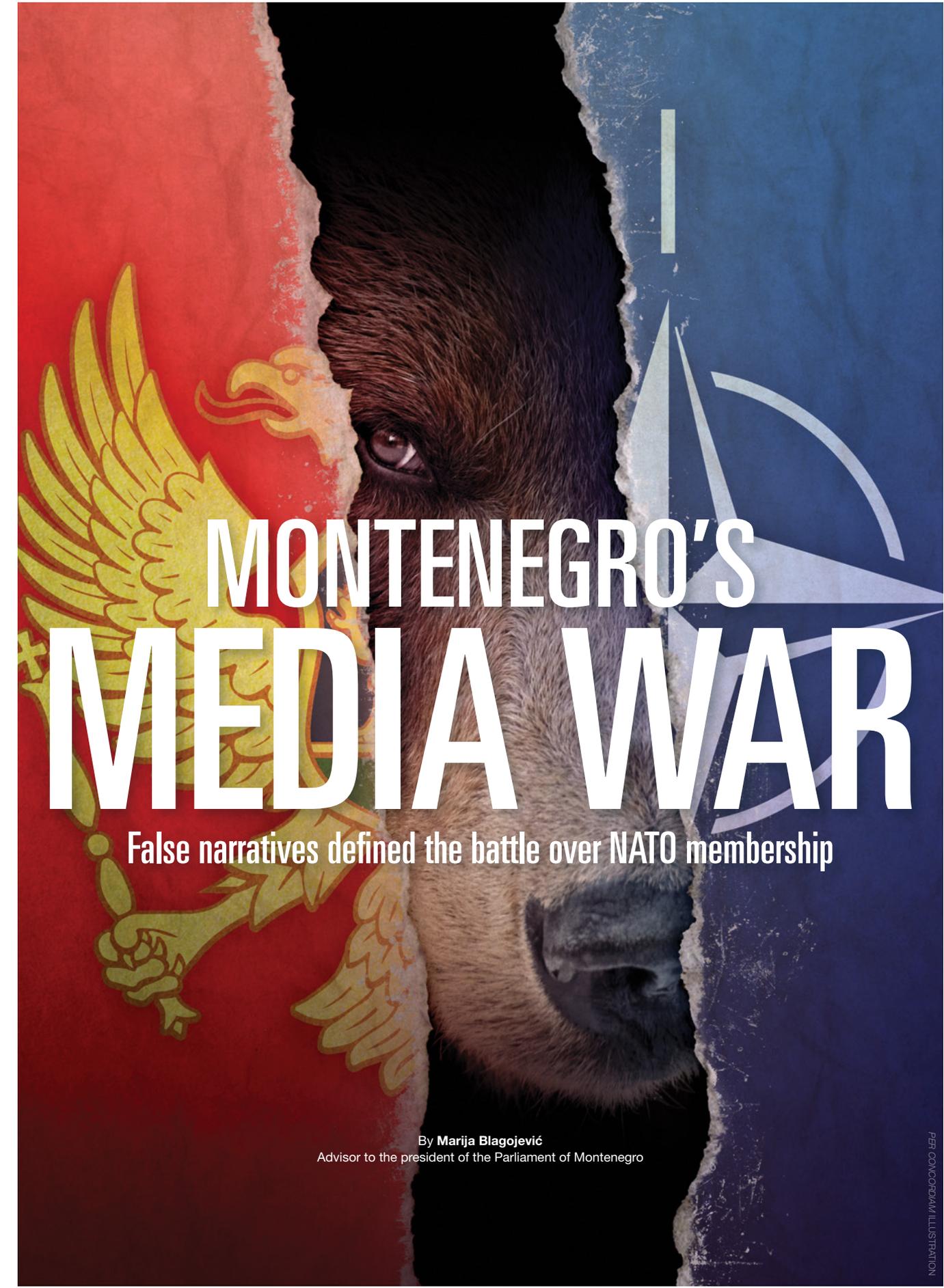
Serbians are passionate users of social networks, in particular Facebook. This inevitably led to various rumors, many of which were related to conspiracy theories about the real scale of the disaster. Interestingly, 15 people who shared and spread such news on Facebook (which had first appeared on various blogs and news portals) were interrogated by the police for the spread of panic during the

state of emergency. Criminal charges were filed against nine of them. One well-known case involved a Belgrade-based reality program participant and makeup artist, who was charged for a Facebook post in which she stated that “corpses are floating down the river Sava but the Ministry of Interior is covering it up.” Other Facebook posts were in a similar vein: “There were three hundred casualties only the first day. Unfortunately, now the number is much higher,” and “Two days ago 250 corpses were found, yesterday 98 more, but the Government doesn’t want to create the panic,” and “TV Pink is a disgrace. They give space to the liar who claims there have been only 12



Rescuers and emergency response teams attend an international field exercise organized by the Serbian Ministry of the Interior and NATO's Euro-Atlantic Disaster Response Coordination Centre in Mladenovac, Serbia, in October 2018. REUTERS

casualties in Obrenovac. Yesterday evening I spoke with my colleague from the faculty who said that thousands of bodies float in the river Sava. I trust him because he himself was evacuated in a boat. This morning I got the same information from another friend. Those people did not drown, but they were killed by electric shock. The sirens were late; the water already entered the town.” Several people who were detained and interrogated for spreading panic complained about their treatment by the police, and there were discussions about whether Facebook, blogs and forums are regarded as mass media under the public information law. In addition, the government was accused of a heavy-handed approach to the (mostly online) media users who questioned and criticized the efforts of local and national authorities during the floods. □



MONTENEGRO'S MEDIA WAR

False narratives defined the battle over NATO membership

By Marija Blagojević

Advisor to the president of the Parliament of Montenegro

PERI CONCORDIAM ILLUSTRATION

On June 5, 2017, Montenegro became the 29th member of NATO. Its accession was preceded by a campaign by the government and nongovernmental organizations that advocated membership, and by a campaign by those who opposed joining the Alliance. An important part of the anti-NATO campaign was reflected in narratives pushed by Russia that often found their way into mainstream media in Montenegro. The consequences of these narratives remain to this day.

Montenegro's 2011 census (the country's first after gaining independence) put the country's population at 620,029. About 45% of the population declared themselves Montenegrins, while 29% said they were Serbs, 9% Bosniaks, 5% Albanians, 3% Muslims and less than 1% Croatian. The three major religious groups in the country are Orthodox Christians (72%) — who are divided between the Serbian Orthodox Church (SOC) and the Montenegrin Orthodox Church; Muslims (19%) and Catholics (3%). The remaining population belongs to other religious groups, are atheists/agnostics or did not declare a religious affiliation.

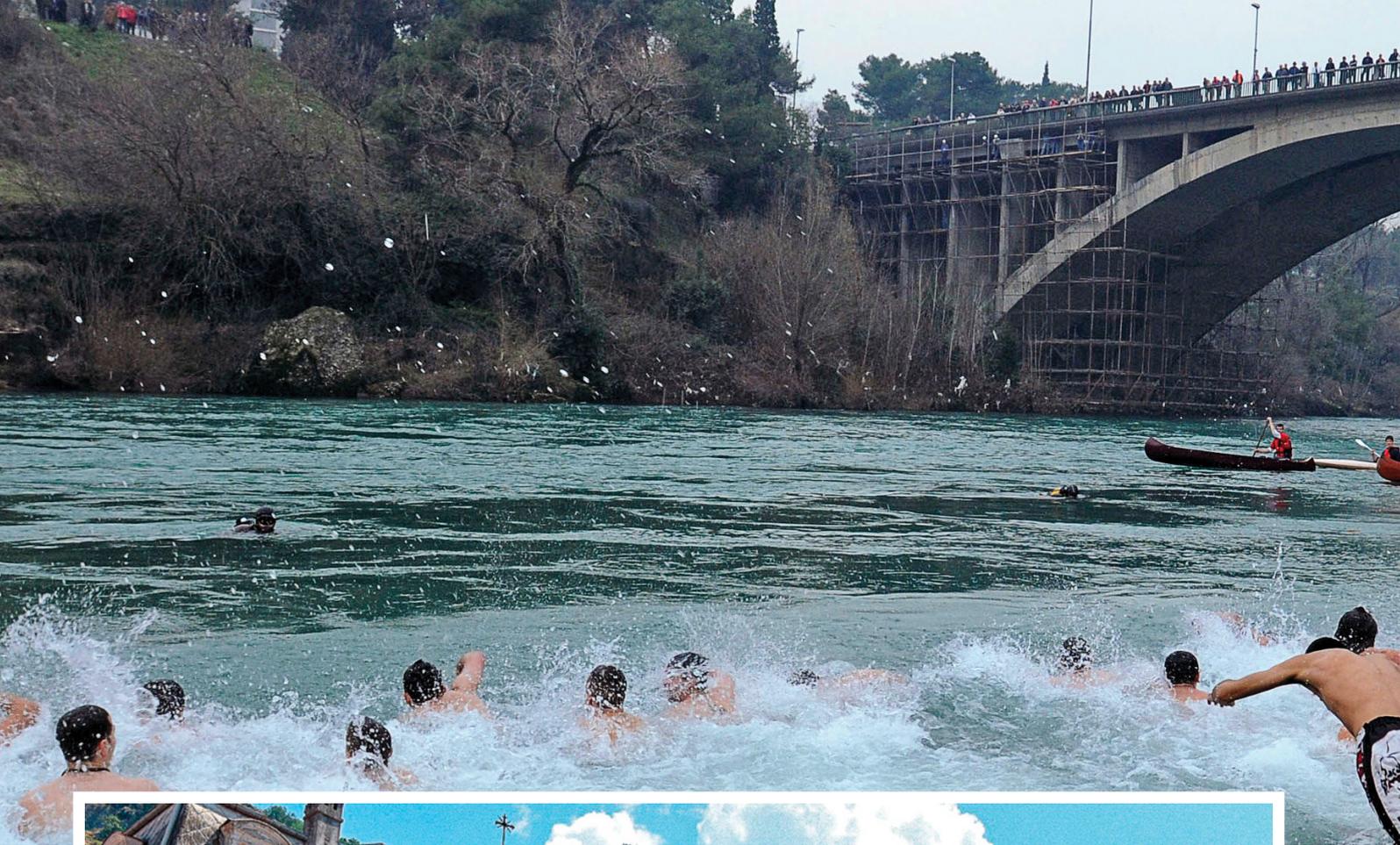
A brief history lesson is needed to fully understand the reasons behind Russia's interference in Montenegro's efforts to realize its most important foreign policy goal since gaining independence in 2006. The relationship between Montenegro and Russia goes back to the reign of Tsar Peter the Great. Ties between the two royal families were strong, as were economic and cultural relations. Russia was a patron of Montenegro and pushed the belief that the two countries were "Orthodox brothers" since the dominant population of Montenegro then and today is Orthodox Christian. Russia has a long history of pursuing its geopolitical goals in the Balkans. But Montenegro's access to the Adriatic Sea has always added an incentive for Russia to interfere. Montenegro gained access to the Adriatic Sea after the Congress of Berlin in 1878, when its sovereignty was recognized by those countries that had not previously accepted it. Diplomatic relations with Russia continued when Montenegro became one of Yugoslavia's federal units.

After the restoration of Montenegro's statehood in 2006,

the two countries established diplomatic relations. At that time, Montenegro clearly defined its entry into NATO and the European Union as its most important foreign policy priorities. This, however, did not imply being closed to investment by other stakeholders, and it was precisely this time after independence that saw major economic growth, especially in construction. Russia's investment impact grew to become the most visible of any country's.

Montenegrin Honor Guard members in Podgorica inspect NATO and Montenegrin flags before a ceremony marking NATO accession. REUTERS







Tourists visit a church in Montenegro's medieval walled city of Kotor, an Adriatic seaport cradled in a spectacular fjord-like bay. Tourism is an important economic sector in the country, and Russians account for about a quarter of all tourists.

GETTY IMAGES

Orthodox Christian believers compete for a wooden cross tossed into the river Ribnica, in Podgorica, marking the Orthodox Epiphany. Russia pushes the narrative that the countries are "Orthodox brothers" because both have large Orthodox Christian populations.

THE ASSOCIATED PRESS

In the 2018 policy brief "Assessing Russia's Economic Footprint in Montenegro," authors Milica Kovačević and Marija Mirjačić report that Russia accounted for one-seventh of the direct foreign investment in the 10 years after independence. They add that, based on data from the Central Bank of Montenegro, the total value of investments originating directly from Russia over this period was approximately 1.3 billion euros, or 31% of Montenegro's gross domestic product. Since 2006, Russia has consistently been among the three leading investors in the country, along with Norway and Italy. The investment was especially visible in the field of tourism, Montenegro's most important economic sector. According to the authors, the number of Russian tourists in Montenegro increased from 61,000 in 2006 to 316,000 in 2016 (about 25% of all tourists who visited that year).

After Montenegro defined EU and NATO integration as its main foreign policy objectives and began harmonizing its foreign policy with EU policy, Russia's sphere of political influence narrowed considerably but remained present

Montenegro has accused Russia of interfering in its 2016 parliamentary elections and of attempting to force a violent regime change.

through certain opposition groups. The opposition's impact grew after Russia's 2014 annexation of Crimea, when Montenegro joined EU sanctions against Russia.

Montenegro has accused Russia of interfering in its 2016 parliamentary elections and of attempting to force a violent regime change. On the day of the election, a number of Serbian citizens were arrested and 14 people were indicted, including two Russian citizens, one of whom is a former member of Russian military intelligence and former deputy military attaché at the Russian Embassy in Poland. He was subsequently declared persona non grata and expelled from Poland on espionage charges. Others indicted were a police general from Serbia and a former commander of the Serbian Gendarmerie, as well as two leading politicians and members of the largest opposition group. The "coup attempt" had its epilogue in May 2019 when a Montenegrin court, after a yearlong trial broadcast on TV, convicted all the accused.

After Montenegro received a formal invitation from the Alliance on December 2, 2015, the pressure intensified. While Russia made public statements that could be interpreted as threatening, the real "war" was being waged in narratives spread through the media. The intention was to reduce public support.

The results of a poll in November 2015 from the Center for Democracy and Human Rights showed that 49.5% of the population supported NATO accession. The percentages changed over the years from 36% in 2008 to 50.5% in June 2016. It also varied within ethnic groups. A majority of Montenegrins, Albanians, Bosniaks and Muslims supported accession, while a majority of Serbs were against it.

Montenegro has several daily newspapers: *Pobjeda* and *Dnevne novine*, which are perceived as pro-government, and *Vijesti* and *Dan*, perceived as government critics. Russia's state-run website Russia Beyond produces a monthly supplement distributed in the Balkans. There is daily news from Serbia available in Montenegro in publications such as *Politika*, *Večernje novosti*, *Blic*, *Kurir* and *Danas*.

The article "Pro-Russian Montenegrins Publish New Anti-Western Media" on the investigative news website Balkan Insight states that all Belgrade-based sites heavily reuse content produced in Russia by Russian media — specifically, the news agency Sputnik, the online outlet NewsFront and the website Russia Beyond. The article

points out that Russian outlets appeared in the Balkans as Montenegro was negotiating its way toward NATO membership. They opened a headquarters in Belgrade and engaged co-contributors from Podgorica. Some analysts think Russia's media strategy is to feed Montenegrin outlets with pro-Moscow news in Serbian, giving it more impact because it is republished in a local context. Several narratives were widely used, among them:

The 'NATO aggressor' narrative

This is the most common anti-NATO narrative used in Serbia and Montenegro, as well as the Republic of Srpska (a constituent part of Bosnia and Herzegovina), since the 1999 Kosovo conflict. NATO bombed then-Yugoslavia, of which Montenegro was a part. The airstrikes lasted 78 days. NATO countries tried to obtain authorization from the United Nations Security Council but were opposed by China and Russia, which indicated they would veto such a proposal. NATO launched a campaign without U.N. authorization, characterizing it as a humanitarian intervention. Yugoslavia described it as an illegal war of aggression against a sovereign country and a violation of international law.

The fact that the humanitarian intervention, which has often been described as legitimate but not legal, lacked U.N. approval is the core of the "aggressors" narrative, which is constantly repeated in pro-Russia media and was widely used in the pre-accession period.

Articles with headlines such as "Aggressor in peacemaker attire" would imply that Montenegrins should not join the "aggressors" and should never "forget what they did." It was stated that NATO and its leader, the U.S., were and remain the "alpha and omega" of all evil in the world. The narrative argues that membership in NATO would be against the interests of the country's most valuable ally, Russia.

There were also subnarratives, such as "NATO occupier" and "depleted uranium." Both were intended to show the consequences of accession. The occupier narrative was used to suggest that sovereignty would be lost by joining NATO; that territorial integrity would be endangered. Articles about NATO bases being established in Montenegro were also part of this subnarrative. Headlines in the Serbian media included one that said, "Here's where the NATO bases in Montenegro will be," making it appear inevitable. Another headline said, "The Government of Montenegro releases NATO tax payments indicating the intention to build a base." The idea was to make Montenegrins think that they would have no say in deciding their destiny after joining NATO. This narrative intentionally played on Montenegrin pride, because one of the main arguments of the independence movement in 2006 was that Montenegro should separate from Serbia so it could independently decide its own priorities and be responsible for its sovereignty and territorial integrity.

The depleted uranium subnarrative was also widespread and may have been the most sensitive because it relates to people's health. Headlines such as "Montenegro and NATO: Drought of depleted uranium," and "It's enough to say — Bread, salt and uranium for enemies," and "NATO bombs

still kill Serbs," and "NATO bombs perpetually threaten health," and "Due to the depleted uranium in Kosovo, 300 KFOR soldiers have died," aimed at convincing the public that there were harmful consequences from exposure to the remnants of the uranium-tipped munitions used by NATO in 1999. In these articles, attempts were made to correlate exposure to depleted uranium munitions with an increase in cancer patients in Serbia and in soldiers who served during the campaign. However, not a single article cites relevant research confirming such a correlation.

'Russian military power' narrative

A sampling of headlines that supported a "Russian military power" narrative include: "The billions are pouring: Here's a new weapon the Russian army gets in 2015," "A renaissance of the Russian military industry — nothing without a firm hand," "NATO anxiety due to Russian intervention," "Russian weapons and military equipment at a Paris fair," "Russian army is getting hyper-weapons," "Russian hunter Su-35 carries the title of the king of the sky," "NATO generals: The Russian army is well-armed and very strong," "Russian weapons for the 21st century," and "Russia richer by two missiles: Zircon and Skif." The narrative was meant to show that the Russian armed forces are inviolable and to cast doubt on NATO's ability to protect Montenegro. One of the government's main arguments for accession was precisely that, because of its size, Montenegro must be part of the collective NATO defense system. That's why opposition articles portrayed Russia as possessing the most modern artillery, surface-to-air missiles, combat planes and helicopters. The narrative also portrayed Russia's actions in Syria as heroic. Contributing to the success of this narrative was a lack of news about NATO military forces and the equipment they possess.

'Superiority of Russian medicine' narrative

This is one of the subtlest narratives. It is related to everyday life, and its purpose was to show Russian superiority in something that affects everybody. The intention was also to show a human side that is not exclusively tied to competing with others. This narrative succeeds because, in the former Yugoslavia, certain fields of medicine, such as ophthalmology, have traditionally been associated with Russian experts who are present in the region and considered very accomplished.

Some of the headlines related to this narrative include: "Express Diagnosis and Treatment without Medicines," "Dr. Nikolai Nauar Nafi: Health Without Chemistry, Treatment Without Side Effects" and "Why Russian Alternative Medicine Is So Successful." Contributing to this narrative were the penetration of Russian medical and cosmetic products into the Montenegrin market, accompanied by marketing that emphasized natural ingredients. This was intended to counter the perception that everything progressive and modern comes from the West and to show that Russia is out front of the West in this arena.

These narratives are current even today, although most of the articles referenced were written from 2015 to 2017. To understand the effects of these narratives, consider research



by the National Institute of Democracy in Washington that was conducted in Montenegro, Bosnia and Herzegovina, Serbia and North Macedonia and published in early 2019, which among other things, includes citizens' attitudes and media reporting on foreign influences.

The research shows that, even though Montenegro is a NATO member, 45% of its residents have a favorable opinion toward Russia, 41% have a favorable opinion toward China, 40% are favorable toward the EU, 29% toward the U.S. and 25% toward NATO. The respondents said their opinions were mostly influenced by media, as well as friends and family. When asked which state or international institution supports their country the most, the EU was mentioned by 45% of the respondents and Russia by 13%. A solid majority of 58% said the country should continue on its European path even if it means spoiling good relations with Russia. In relation to the narratives above, it is interesting that 47% found Russia's military superior to NATO's, 37% did not and 17% said they did not know.

When asked if the country would become a better place to live if it gave up EU integration and turned toward Russia, 43% responded that it would, while 46% said it would not and 11% didn't know. Half of the respondents believe the

country's economic development is linked to Russia. When asked whether the country could reach its economic development goals if it chose Russia as its key trade and investment partner, 51% responded positively. However, 59% said the country would be able to reach its economic development goals if it chooses to maintain the EU as its key trade and investment partner.

When asked where they would seek medical treatment or surgery, 21% said Russia, the single biggest percentage of any country. Another 28% named a country in the EU, and 20% said the U.S. When asked whether they pay attention to the sources of the media they consume, 54% said they did not.

Of course, not all the survey results are the product of these narratives, but some are certainly concerning and show the impact that even subtle propaganda can have. The results show how important it is to clearly explain the benefits of NATO, for example, or any important goal, as well as the importance of deterring fake news. □

NATO Secretary-General Jens Stoltenberg, right, and Montenegrin Prime Minister Milo Đukanović take their seats during a meeting of the North Atlantic Council and Montenegro at NATO headquarters in Brussels.

THE ASSOCIATED PRESS



THE FOG OF MODERN WARFARE

RUSSIA'S DISINFORMATION CAMPAIGN IN BULGARIA

By **Vanya Denevska**, parliamentary secretary, Bulgarian Ministry of Defence

In early 2018, Russian hybrid actions were stepped up to hinder the European integration of Western Balkan countries by exploiting historic relations and issues, as well as the unity of the Orthodox Church. For instance, the Russian Orthodox Church posted a video on its website of Russian Patriarch Kirill expressing his resentment of statements by Bulgarian President Rumen Radev, who had spoken of the roles that countries other than Russia had played in Bulgaria's liberation from Ottoman rule. Kirill called Radev's statements "false historical interpretations." Later, the Russian news agency Tass circulated a speech in which Kirill emphasized that Bulgaria was liberated by Russia and not by "Poland, nor Lithuania, nor other countries," overlooking the fact that soldiers from those countries had died in the fighting.

The messaging was part of a well-structured Russian hierarchical system that plans, develops and implements strategies for the coordinated use of military and nonmilitary instruments. Established lines of propaganda and disinformation are legitimized through Russia's Ministry of Foreign Affairs, though the Kremlin has always denied its participation in activities aimed at molding public opinion. The techniques used in these disinformation campaigns include: distorting facts; degrading the image of targeted individuals and organizations; and launching entirely false allegations to confuse the public. Electronic, printed and broadcast media that are financially dependent on Moscow and political functionaries are actively involved in these campaigns. In the runup to the 2019 European elections in Bulgaria, Russia created Facebook pages to promote the

pro-Russian Bulgarian Socialist Party (BSP). The pages are a source of fake news and are popular, with names such as "Let's return Bulgaria to the Bulgarians." These sites have anonymous owners and have become sources from which the disinformation stream starts. Subsequently, they are quoted by other media and on social networks. Through the sharing of trending commentary, an illusion is created that false claims are real facts. The goal is to provoke discussion in the official media that grows into a divisive public debate.



Bulgarian President Rumen Radev speaks during the United Nations General Assembly in September 2019. THE ASSOCIATED PRESS

The techniques used in these disinformation campaigns include: **distorting facts;** **degrading the image of targeted individuals and organizations;** and **launching entirely false allegations to confuse the public.**

For example, tempers rose across social networks over an outbreak of African swine fever shortly after the European Parliament elections. Cornelia Ninova, leader of the BSP, accused Prime Minister Boyko Borisov of mocking people's concerns about the virus. The outbreak became part of a disinformation campaign to politicize problems and weaken the pro-European government of Bulgaria. Those targeted are often individuals or organizations disturbed by Russia's influence in former Soviet satellite states. The disinformation is concealed as official assessments and analysis of real events and processes.

It is quite clear that there was an intensification of Russian disinformation during the May 2019 European Parliament elections. The good news is that voters rejected the ugly face of Eurasianism. Two weeks before the elections, most polling agencies found even support for the two biggest parties in Bulgaria — GERB (pro-Europe) and BSP

(pro-Russian) — while some polls, perhaps in bad faith, heralded support for pro-Soviet sentiments. For example, the main motto of the nationalist Ataka party's election campaign was to remove the sanctions imposed on Russia. In the end, the parties questioning the pro-European direction for Bulgaria — the BSP, Ataka, ABV, Vuzrazhdane and Volya — suffered defeat.

Russia's information operations are aimed at undermining Bulgarians' public awareness about Bulgaria's Euro-Atlantic choice and, consequently, influencing the political decisions of the Parliament and the government more directly. In the past three years alone, hundreds of cases of Russian interference in Bulgaria's internal affairs, directly or indirectly, have occurred — through parliamentary and nonparliamentary political parties, leading politicians, key figures in the state administration, pro-Russian electronic and print media, websites, pro-communist Russophile organizations, Orthodox activists, internet trolls, oligarchs and criminal groups. Published reports by various analysts highlight the following topics in the media space:

- Bulgaria's EU and NATO membership.
- Sanctions and countersanctions in connection with Russia's war in Ukraine.
- Attitudes toward Syria and the Middle East.

The larger news sites in Bulgaria are positioned in the center and with a slight inclination toward Moscow, but Russian propaganda dominates among the smaller sites on the Bulgarian internet. There are hundreds of sites that spread Russian propaganda. Analysis of these sites shows that the 10 most popular are without clear owners and that they generate millions of clicks. This means that a large-scale misinformation and propaganda war is being waged against Bulgaria.

Disinformation campaigns were launched in 2019 around local elections in Bulgaria. During the campaign season, prosecutors announced



Germany's Manfred Weber of the European People's Party appears at a rally in Sofia, Bulgaria, in May 2019, days before European Parliament elections. THE ASSOCIATED PRESS



an investigation into a Russian citizen accused of acquiring state-secret intelligence. As a result, a Russian diplomat, the first secretary at the Russian Embassy in Sofia, was recalled and left the country. Additionally, the chairman of the Russophile Movement, Nikolai Malinov, was accused of espionage. It later became clear that despite the accusation against Malinov, a judge had allowed him to travel to Russia to receive the Friendship Order at a special ceremony in the Kremlin. Prosecutors claim Malinov has worked for the benefit of two Russia-based organizations for nearly nine years. During searches, investigators found a note prepared by Malinov, written in Russian, in which he described the need for Bulgaria's geostrategic reorientation toward Russia. The note included measures to achieve that end and asserted that the reorientation should be based on Orthodoxy, Slavic culture and traditions. It advocated for efforts to create nongovernmental organizations, internet sites, a television channel, a think tank and a political party. Subsequently, Russian oligarch Konstantin Malofeev, who is reportedly close to Russian

President Vladimir Putin, was banned from entering Bulgaria for 10 years. Also exiled was Russian Gen. Leonid Reshetnikov, who is accused of coordinating Russian espionage operations in Bulgaria. The real winner in the 2019 election was the status quo: the major political parties and ruling coalition strengthened their positions. No changes are anticipated, and Bulgaria's pro-EU and pro-NATO orientation is expected to remain stable.

In conclusion, similar influence campaigns by Russia can be expected. For example, on May 9, 2019, large numbers of pro-Russian Bulgarians celebrated the Day of Victory, even though Bulgaria lost World War II. The holiday was instituted when communist Bulgaria was politically subservient to the Soviet Union and officially cancelled in 1989 when the Soviet Union fell. The intensity of the Russian hybrid attacks and disinformation campaigns can be expected to increase. New ways to hide the source and the real intentions of operations will be created to expand the audience and provoke public debates in Bulgaria and around the world. □

People protest an exhibition backed by Russia's embassy in Bulgaria titled "75 years since the liberation of Eastern Europe from Nazism," in Sofia, Bulgaria, in September 2019.

REUTERS

'WAR BY OTHER MEMES'

AUTHORS: P.W. Singer and Emerson T. Brooking

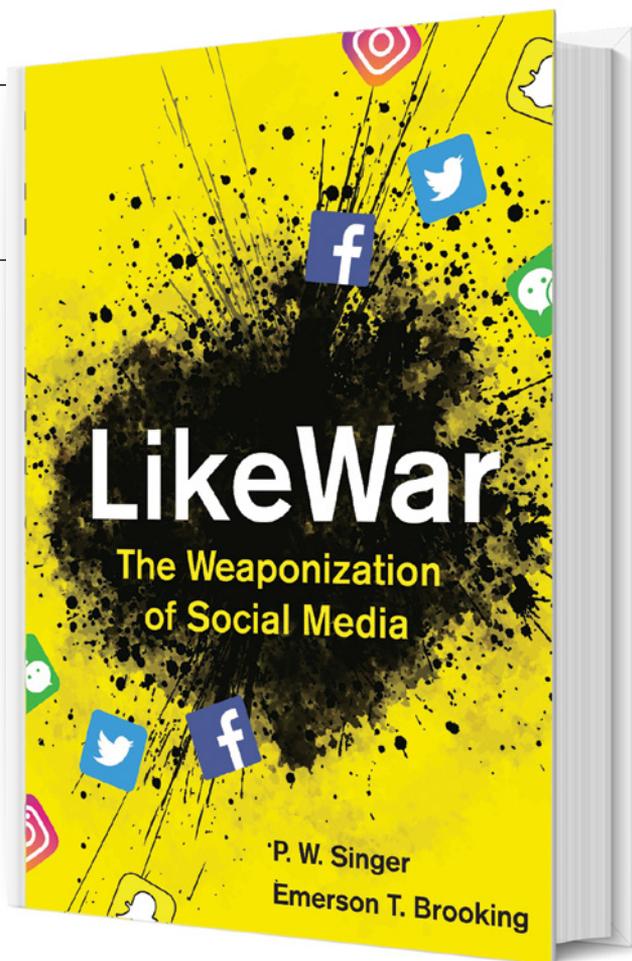
PUBLISHED BY: Eamon Dolan/Houghton Mifflin Harcourt

REVIEWED BY: Patrick Swan, *per Concordiam* contributor

If war is, as Prussian military theorist Carl von Clausewitz so memorably phrased it, “politics by other means,” then authors P.W. Singer and Emerson T. Brooking view today’s digital battlefield as “war by other memes.” Since its inception, social media has been brutally weaponized to attack and destroy reputations through viral posts designed to set and control a narrative. But that is trivial compared to what the authors address in their short, punchy treatise, *LikeWar: The Weaponization of Social Media*, where they outline the perilous stakes for countries — and people — who neglect to address this alternative domain of warfare.

The authors focus primarily on two types of digital warriors — nonstate actors engaging in an ideological or religious cause and state actors seeking to obtain a more favorable position for their country. On the first of these, Singer and Brooking describe how the self-declared Islamic State (ISIS or Daesh) hashtagged its 2014 invasion of northern Iraq #AllEyesOnISIS. They “choreographed [a] social media campaign to promote it, organized by die-hard fans and amplified by an army of Twitter bots. ... There was even a smartphone app, created so that jihadi fans following along at home could link their social media accounts in solidarity.” They add: “It became the top-trending hashtag on Arabic Twitter.” In a visceral demonstration of weaponized social media, “ISIS videos also showed the gruesome torture and execution of those who dared resist. And then it achieved its real-world goal: #AllEyesOnISIS took on the power of an invisible artillery bombardment, its thousands of messages spiraling out in front of the advancing force.”

Singer and Brooking explain that Mosul’s abrupt fall to ISIS showed that there was another side to computerized war. Back to Clausewitz in this regard: While the nature of war is unchanging — one force seeking to compel another to submit to its will — war’s character most certainly has changed. When a national army bolts in the face of the enemy more because of what they’ve seen on their smart phones than from kinetic contact, a change in the character of war is afoot. A populace can adapt to artillery fire and aerial bombing, but ISIS “telegraphing” its pending arrival through



social media made people feel that they were directly in the crosshairs. “The Islamic State, which had no real cyberwar capabilities to speak of,” the authors observe, “had just run a military offensive like a viral marketing campaign and won a victory that shouldn’t have been possible. It hadn’t hacked the network; it had hacked the information on it.”

To Singer and Brooking, ISIS targeted the “spirit of a nation’s people” and thus the most important center of gravity in a war. Defeat the center of gravity, goes the thinking, and a nation will capitulate. But the norm is quite the opposite. History is replete with nations defying an opponent long after the people have resigned themselves to defeat, because the authoritarian rulers have been all too willing to fight to the last civilian. Still, the authors are correct that attacking an adversary, regardless of the center of gravity, does not necessarily require massive bombing runs or reams of propaganda. “All it takes is a smartphone and a few idle seconds,” Singer says. “And anyone can do it.” Call it the democratization of war. Singer and Brooking sum up the facets of this new

warfare thusly: The internet has become a battlefield, and battlefields change how conflicts are fought and what war means. Everyone is now part of this war.

And yet, the democratization of war cuts many ways. Singer and Brooking relate how a group of 17 citizens in Raqqa, Syria, banded together to tell the story of their city's destruction. ISIS had enforced a news blackout of independent reporting by murdering any journalists they discovered. The Raqqans themselves filled the void — through social media posts. “They did so via an online news network they called Raqqa Is Being Slaughtered Silently. It was as much an act of resistance as reporting. Their belief, as one member put it, was that ‘truth-telling’ would prove to be more powerful than ISIS’ weapons.” Then, when a coalition of forces routed ISIS from Raqqa, these social-media citizen journalists showed how the once invincible ISIS had become the invisible ISIS, chased from its strongholds and shamed on its social media accounts. If citizens can fight back by waging social media war, nations can fight even more effectively if they take the challenge seriously and bring cyber force to bear.

Still, what about the gray area, the so-called hybrid war that some nations wage, where stealthy activities conceal direct culpability for destabilizing activities that run short of formal war? This can be as nefarious, if not as bloody, as the ISIS campaign. Singer and Brooking quote Ben Nimmo, who outlines the “4 Ds” of such an approach: dismiss the critic, distort the facts, distract from the main issue, and dismay the audience. Has Russia invaded Crimea? “Pshaw. What little green men? The idea is preposterous.” Did Russian-backed insurgents shoot down a commercial airliner? “It must have been the Ukraine government.” The authors state: “The point of such a barrage of dissembling is to instill doubt — to make people wonder how, with so many conflicting stories, one could be more ‘right’ than any other.”

Singer and Brooking note that the key to success for employing a weaponized social media network is to convey messages with three traits — simplicity, resonance and novelty. These “determine which narratives stick and which fall flat.” ISIS is coming and the army is fleeing. There are no images of fighters in Russian uniforms so how can one say Russia is involved in Crimea? These traits are key because “to control the narrative is to dictate to an audience who the heroes and villains are; what is right and what is wrong; what’s real and what’s not.”

This is precisely why nations should take the weaponization of social media seriously. From places such as Europe or North America, images of the ISIS invasion of Mosul — a ragtag rabble of wannabe warriors driving pickup trucks — looked ludicrous and their narrative fell flat. But for a disheartened and internally divided army, it was enough to lose confidence and flee, leaving behind a population unprotected and petrified. However, while a social media war may advance in a one-sided fashion, the fight can eventually be joined and reversed. Singer and Brooking state:

“Victory requires an appreciation of the nature of virality and the whimsical ways of the attention economy, as well as a talent for conveying narrative, emotion, and authenticity, melded with community-building and a ceaseless supply of content (inundation). And because it all takes place on the open internet, each of these conflicts becomes a global tug-of-war with an unknown number of players.”

In the case of the Malaysia Airlines Flight 17 shot down over Ukraine, the Russians engaged their legion of internet bots to muddy its culpability. However, a global online citizenry, using solely open-source material, debunked conclusively the Russian denials. They provided the demonstrative evidence showing the surface-to-air missile’s origination from stockpiles within the Russian state. Nevertheless, although individuals may congregate in a virtual community to assist on a case-by-case basis, they are no substitute for the immense resources a country can bring to bear on a social media campaign.

However, some of the solutions that Singer and Brooking call for also offer insidious problems. They would have nations (and individuals and even social media companies) stigmatize anyone who spreads “lies, hate, and other societal poisons” via social media platforms. Who exactly gets to define “dangerous speech?” Singer and Brooking conclude specifically that “Silicon Valley must accept more of the political and social responsibility that the success of its technology has thrust upon it.” But should the legally and politically unaccountable private companies running social media platforms, which have credibly been accused of mimicking the heavy-handed practices of authoritarian governments to silence legitimate political speech, be vested with such responsibility? This is a recipe for rampant abuse. Opportunistic authoritarian governments or democratic governments on shaky footing may be all too happy to brand domestic political opponents as having engaged in “dangerous speech” that must be eradicated.

The weaponization of social media is a grave concern. Singer and Brooking present many viable actions, and one that perhaps needed more thought. Their cure to obliterate “dangerous speech” serves more to poison the “drinking water” from which all users of the internet imbibe. A better course is a barrage of transparency and truthfulness, along with a healthy dose of ridicule, to counter disinformation campaigns. The people of Raqqa knew this, as did the cyber citizens who exposed the culprits behind the airliner downing in Ukraine. Governments can do this, as well as citizens, and social media companies can provide the platform, not to censor, but to join the fight for the facts.

Singer and Brooking are on much sounder footing with their concluding advice: We are all in this war. “If we want to stop being manipulated, we must change how we navigate the new media environment. When in doubt, seek a second opinion — then a third, then a fourth. If you’re not in doubt, then you’re likely part of the problem.” □

Resident Courses

Democratia per fidem et concordiam
Democracy through trust and friendship



Registrar

George C. Marshall European Center for Security Studies
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
Telephone: +49-8821-750-2327/2229/2568
Fax: +49-8821-750-2650
<https://www.marshallcenter.org>
registrar@marshallcenter.org

Admission

The George C. Marshall European Center for Security Studies cannot accept direct nominations. Nominations for all programs must reach the center through the appropriate ministry and the U.S. or German embassy in the nominee's country. However, the registrar can help applicants start the process. For help, email requests to: registrar@marshallcenter.org

PROGRAM ON APPLIED SECURITY STUDIES (PASS)

The Marshall Center's flagship resident program provides graduate-level education in security policy, defense affairs, international relations and related topics such as international law and counterterrorism. A theme addressed throughout the program is the need for international, interagency and interdisciplinary cooperation.

PASS 20-19

Sept. 9 -
Nov. 24, 2020

September							October							November							
S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	
			1	2	3	4	5					1	2	3	1	2	3	4	5	6	7
6	7	8	9	10	11	12	4	5	6	7	8	9	10	8	9	10	11	12	13	14	
13	14	15	16	17	18	19	11	12	13	14	15	16	17	15	16	17	18	19	20	21	
20	21	22	23	24	25	26	18	19	20	21	22	23	24	22	23	24	25	26	27	28	
27	28	29	30				25	26	27	28	29	30	31	29	30						

PROGRAM ON COUNTERING TRANSNATIONAL ORGANIZED CRIME (CTOC)

This resident program focuses on the national security threats posed by illicit trafficking and other criminal activities. The course is designed for government and state officials and practitioners who are engaged in policy development, law enforcement, intelligence and interdiction activities.

CTOC 20-07

Mar. 17 -
Apr. 8, 2020

March							April							July							
S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	
1	2	3	4	5	6	7					1	2	3	4				1	2	3	4
8	9	10	11	12	13	14	5	6	7	8	9	10	11	5	6	7	8	9	10	11	
15	16	17	18	19	20	21	12	13	14	15	16	17	18	12	13	14	15	16	17	18	
22	23	24	25	26	27	28	19	20	21	22	23	24	25	19	20	21	22	23	24	25	
29	30	31					26	27	28	29	30			26	27	28	29	30	31		

PROGRAM ON TERRORISM AND SECURITY STUDIES (PTSS)

This program is designed for government officials and military officers employed in midlevel and upper-level management of counterterrorism organizations and will provide instruction on both the nature and magnitude of today's terrorism threat. The program improves participants' ability to counter terrorism's regional implications by providing a common framework of knowledge and understanding that will enable national security officials to cooperate at an international level.

PTSS 20-05

Feb. 11 -
Mar. 12, 2020

February							March							August							September							
S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S	
						1	1	2	3	4	5	6	7							1				1	2	3	4	5
2	3	4	5	6	7	8	8	9	10	11	12	13	14	2	3	4	5	6	7	8	6	7	8	9	10	11	12	
9	10	11	12	13	14	15	15	16	17	18	19	20	21	9	10	11	12	13	14	15	13	14	15	16	17	18	19	
16	17	18	19	20	21	22	22	23	24	25	26	27	28	16	17	18	19	20	21	22	20	21	22	23	24	25	26	
23	24	25	26	27	28	29	29	30	31					23	24	25	26	27	28	29	27	28	29	30				
														30	31													

PTSS 20-18

Aug. 6 -
Sept. 3, 2020

PROGRAM ON CYBER SECURITY STUDIES (PCSS)

The PCSS focuses on ways to address challenges in the cyber environment while adhering to fundamental values of democratic society. This nontechnical program helps participants appreciate the nature of today's threats.

PCSS 20-02

Dec. 3 - 19, 2019

December						
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

SEMINAR ON REGIONAL SECURITY (SRS)

The seminar aims at systematically analyzing the character of the selected crises, the impact of regional actors, as well as the effects of international assistance measures.

SRS 20-03

Jan. 14 -
Feb. 7, 2020

January						
S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

February						
S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

SENIOR EXECUTIVE SEMINAR (SES)

This intensive seminar focuses on new topics of key global interest that will generate new perspectives, ideas and cooperative discussions and possible solutions. Participants include general officers, senior diplomats, ambassadors, ministers, deputy ministers and parliamentarians. The SES includes formal presentations by senior officials and recognized experts followed by in-depth discussions in seminar groups.

SES 20-15

June 22 - 26, 2020

June						
S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

Alumni Programs

Christopher Burelli

Director, Alumni Programs
Tel: +49-(0)8821-750-2706
christopher.burelli@marshallcenter.org
Languages: English, Slovak, Italian, German

Alumni Relations Specialists:

Drew Beck

Western Balkans,
Francophone Africa

Languages: English, French

Tel: +49-(0)8821-750-2291
ryan.beck@marshallcenter.org

Christian Eder

Western Europe

Languages: German, English

Tel: +49-(0)8821-750-2814
christian.eder@marshallcenter.org

Marc Johnson

Eastern Europe, Caucasus,
Central Asia;
Cyber Alumni Specialist

Languages: English, Russian,
French

Tel: +49-(0)8821-750-2014
marc.johnson@marshallcenter.org

Frank Lewis

Visegrád Four, Baltics, Middle
East, South and East Asia;
Counterterrorism Alumni
Specialist

Languages: English, German

Tel: +49-(0)8821-750-2112
frank.lewis@marshallcenter.org

Donna Janca

Americas, Anglophone Africa,
Eastern Balkans, Mongolia;
CTOC Alumni Specialist

Languages: English, German

Tel: +49-(0)8821-750-2689
nadonya.janca@marshallcenter.org



mcalumni@marshallcenter.org

VE DAY 75

VE Day on 8 May 2020 marks 75 years since the end of World War II in Europe.

Per Concordiam takes this occasion to remember the Allied forces that sacrificed so much to deliver peace to so many.

