Information War 2022

Musings of a Senior Officer on Russian Information Warfare and Recent Events

Extract of foreword published by *Praxis: Journal of International Issues* in 2023

Spc. Thomas Sarsfield, U.S. Army

Today's generation of professionals grew up in an age of social connectedness. Everything they said, did, and typed, was immortalized by the camera on their phones and imprinted onto an enormous online record. But, because sometimes the story wasn't good enough for them with facts alone, disinformation through fake news websites gripped Western society and shaped its development from 2016 forward.

As was shown, a few silver-tongued wordsmiths and a solid team of social media bots buttressed by cash infusions to a friendly party could do more to influence an adversary's policies than traditional means of state interaction. The politically illiterate and misinformed, yet tech savvy electorate of many countries, found themselves increasingly falling prey to ostensibly independent yet fundamentally propagandistic "news" sites bankrolled primarily by the Russian government.[1] Indeed, a wave of fake news penetrated deeper and faster than real news.[2] One result was that by 2016 established traditional journalism behemoths, long the platforms for debate in American if not international society, were finding themselves on the losing side of an information insurgency that sought to sow social discord by undermining confidence in traditional news through fake news. One such venerated institution, the *Washington Post*, in response to the dramatic rise and influence of fake news, once proclaimed on its website banner that "Democracy Dies in Darkness." By this it meant that the press's traditional role of watchdog over political policy makers was rapidly eroding because of the changed information environment that made discerning truth from fiction increasingly difficult. Though democracy hasn't died yet since then, it has nonetheless become extremely dysfunctional due primarily to the unmitigated chaos of the information environment.[3]

We saw this information chaos during the 2021 Berlin riots, when a series of provocative tweets about right-wing reactionary Adolf Aduederman being arrested by the German Federal Police rippled throughout German social media. Within an hour of the original tweet about Aduederman's arrest, thousands of Twitter accounts—many subscribed to each other to give the impression they were not fake accounts to unsuspecting readers—had retweeted it with "#FreierAduederman." Soon it was picked up by several alternative, right-wing online media outlets heavily funded by the state-owned Russian oil enterprise Gazprom.

His angry supporters took to the streets by the hundreds, chanting and throwing rocks outside of the

FICTION

Bundestag. International audiences gawked at videos of armor-clad police tapping their riot shields with batons and hurling tear gas at demonstrators.

Despite numerous press statements and a public announcement from Chancellor Torsten Buchberger that Aduederman was not arrested, his conspicuous absence from social media only fueled suspicion and outrage. On the third day of unrest, a video purporting to show Special Deployment Commandos raiding Aduederman's house days earlier incited hundreds more to pour into the streets of Berlin. Similar protests erupted in other cities, including Frankfurt and Bonn.

Yet Aduederman had not been arrested. In the early hours of August 29, 2021, he announced through Twitter that he was alive and well. He claimed that he had taken an "abrupt leave of absence" from social media to go camping because a "reputable informant" had tipped him off to the planned arrest. The video of Special Deployment Commandos purportedly raiding Aduederman's home days earlier was traced by the Bundespolizei to an internet protocol (IP) address originating in Russia, although the Russian government denied any involvement with the video's release.

It was later assessed that the Russian disinformation campaign did not occur independently. Instead, it was coordinated with other elements of subversive power. A highly classified intelligence assessment produced by Germany's domestic intelligence agency, the Federal Office for the Protection of the Constitution, concluded that agents from the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, commonly known as the GRU, had been covertly deployed and embedded within both German far-right and far-left political groups. Their advice and assistance on the ground was invaluable to the organizers of far-right movements that demonstrated during Aduederman's purported detainment—as well as to the far-left groups who counter-protested.[4] It remains unknown at this time who leaked the report.

Elsewhere, during the 2022 French elections, Russian intelligence agencies began a targeted social media campaign to turn out the vote among far-right voters. Much like the 2017 elections, the 2022 election saw poor voter turnout with slightly less than 50 percent of the eligible voting population going to the polls. However, among far-right voters, the turnout was 55.3 percent, leading to additional seats for the National Front.

> "Though democracy hasn't died yet since then, it has nonetheless become extremely dysfunctional due primarily to the unmitigated chaos of the information environment."

Notably, the Russian campaign had focused almost entirely on social media engagement, which it apparently concluded was the tool-of-choice to mobilize voters and sow discord.[5] This strategy emphasized a geo-cyber approach. Advertisements funded by Russian state-owned corporations through shell companies focused on far-right voters in districts with the best odds of success for far-right parties, while Facebook pages and Twitter accounts run by intelligence agencies generated sensational news accounts that focused on how key issues affected a particular community. Appropriately, there were also a spate of tweets and articles targeted at moderate and left-wing voters that questioned the value of an individual vote, to try to drive down turnout among those groups. Additionally, the emphasis on a bottom-up approach that relayed how a voter's own town or region was impacted by, say, immigration and then connected it to a broader theme of national, secular, or religious identity yielded impressive results.

An important aspect of this operation was coordination. The Russian government was careful to

Spc. Thomas Sarsfield, U.S. Army, is an Apache attack helicopter electrical/avionics/armament systems maintainer in Company D, 1st Attack Reconnaissance Battalion, 1st Combat Aviation Brigade, 1st Infantry Division at Fort Riley, Kansas. This article is a work of speculative fiction meant to encourage critical thinking about the future of information warfare. It does not represent the views of the U. S. Army or the Department of Defense.

FICTION

ensure that local narratives did not conflict with strategic narratives, while at the same time giving the lower echelons responsible for creating local products the space needed to be creative, timely, and relevant.

Though in the West, the psychological (PSYOP) forces of various nations attempted to counter such efforts by performing what the U.S. military calls Military Information Support Operations (MISO), the United States and its allies were not prepared to respond to the Russian effort at the same scope or level of Russian sophistication.

“Indeed, by 2020, the Russian military had substantially reenvisioned the role of armed force in conflict all together, especially its relationship to information warfare.”

Even now, MISO narrowly aims to achieve behavioral change through the use of information in order to support military and political objectives. As such, MISO doctrine remains an inadequate lens to assess the massive scope and reach of the Russian PSYOP capabilities that have emerged since 2016. Indeed, by 2020, the Russian military had substantially reenvisioned the role of armed force in conflict all together, especially its relationship to information warfare. While the United States continued to view MISO merely as a force multiplier of other actions, the Russians viewed other military actions as a force multiplier of psychological warfare. As early as 2014, Janis Berzins noted, “[T]he Russian view of modern warfare is based on the idea that the main battlespace is the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare… .”[6]

So while the United States continued to view PSYOP in a secondary, support capacity, Russia apparently had concluded that the aim of modern war is to fundamentally alter the adversary’s perspective, which means heavy emphasis on PSYOP in all realms of influence. Influence, as Berzins puts it, is “at the very center of [Russian] operational planning.”[7]

As a result, by 2021 the United States and its NATO allies found it difficult to coordinate effective responses in a rapidly evolving information arena that broadly favored their adversaries. For example, whereas Western penetration of adversary firewalls to effectively exploit social media websites like Weibo in China or VK in Russia was, and is, hampered by strong censorship measures by both the platform operators and government, in contrast, Western platforms—which were largely unregulated by firewalls and committed to free speech—enabled extensive foreign exploitation by the mass dissemination of subversive messages.[8]

Post-2022, our adversaries continue to be less susceptible to the strategies they themselves employ by virtue of the restrictive social and government structures that control information dissemination in their societies. Furthermore, despite being a powerful tool for information operations, Western MISO activities remain constrained by ethical concerns about “collateral information damage” from PSYOP information campaigns that potentially influence Western domestic populations in ways that continue to be interpreted as unethical, even illegal. Whereas traditional PSYOP tools such as pamphlets, radio broadcasts, and loudspeaker operations are limited in geographic scope, such limitations do not exist for online information, which cross national borders easily and have global reach. Anyone anywhere can access an open website like Facebook or Twitter and traverse its “digital terrain” with ease. Thus, concerns about how MISO operations affect American civilian perceptions, which are still factored into operational planning, have in a practical sense proven to be a great impediment. As a result, not only are we limited in what we are able to do by how our adversaries regulate their own websites, but also we are restricted by our own ethical commitment to shielding our population from messages intended to shape the behaviors of foreign audiences.

Furthermore, other challenges to the reliability and trustworthiness of information in the news have come to fruition since the last decade as rapid advances in technology have created new disinformation challenges. In 2016, a group of German and American researchers developed software that allowed them to manipulate

people's faces in real time.[9] They demonstrated this concept by altering facial movements of former presidents George W. Bush, Donald Trump, Barack Obama, and also of Russian president Vladimir Putin as they were being interviewed on television in an effort to create false impressions of the body language reputedly depicted. This technology has been subsequently refined since that time and has advanced by voice replication software and Computer Generated Imagery—the same technology used to create spectacular effects in movies. Now fake interviews appearing online are virtually indistinguishable from real interviews. Only seasoned analysts can identify the microirregularities and parse fact from fiction in what is electronically depicted. From the growing difficulty in their ability to determine fact from fiction, by the late 2010s, the public had largely withdrawn their faith in expertise. These tools, which were routinely used within Russia against political dissidents, now are routinely deployed against activists and candidates across the world. The so-called "end of expertise," combined with other global trends such as the rise in identity politics and decline of social capital, has created exceedingly fertile ground for sowing dissent.[10]

Ironically, *The New York Times* subscription base grew considerably in 2017.[11] So too did the subscription numbers of the *Washington Post* and *The Economist* grow as well, both in America and Europe. However, information insurgents found that they didn't need to kill the mainstream media to win and achieve their influence objectives. Rather, information insurgents could attain objectives by disrupting on the fringes, identifying and manipulating the political radicals to vote in higher numbers, cause scenes, and sow social disorder. They even managed to disrupt within parties and movements by dredging up, seizing on, and sensationalizing reputedly unscrupulous past behavior of targeted persons to weaken support for a candidate during election cycles. Such "digital assassinations" were sometimes the work of remarkable investigative work by information insurgents who dug through the old social media accounts of potential targets, finding unseemly or embarrassing behavior and then resurrecting it for the world to see.

Other times a well-developed human intelligence network brought a long-forgotten video provided by an old associate of the target, captured years earlier and sitting on an old cell phone. But, in far too many cases, such reputed information was simply fabricated and subsequently amplified in a digitally constructed echo chamber, as was the case during the 2016 Lisa controversy in Germany.[12]

Interestingly, the online forum known as 4Chan has long been a source of open-source political deception and influence campaigns. Originally founded by a young man named Christopher Poole as an online forum to discuss Japanese culture and anime, 4Chan quickly morphed into a toxic blend of far-right politics, misogyny, and practical jokes. 4Chan users on the /b/ and /pol/ boards were known for their self-described "psyops" campaigns against communities or groups they deemed to be "libtard cucks."[13] Frequent targets included Reddit and Tumblr. A good example is the "O-K" hand sign scandal of 2018. 4Chan users began circulating posts online that alleged that the "W" formed by an "OK" hand sign represented "white power."[14] This provoked outrage across many groups online, who fell for the gag—thus reinforcing the belief that liberals were gullible or reactionary amongst conservatives who understood the prank's origins or otherwise believed the notion of the hand sign being racist to be ridiculous.

However, despite the disinformation campaign being called out by the Anti-Defamation League, the trick had real world consequences.[15] A Coast Guardsman was relieved from Hurricane Florence relief efforts after flashing an "O-K" hand sign on national television, which led many Twitter users and news outlets to allege that the Coast Guard harbored racists among its ranks.[16] This open-source disinformation campaign was so effective in part because the "O-K" sign was also associated with a cultural meme at the time, in which a person would trick another person into looking at their hand, which formed an "O," below the waist and say "Got 'Em!"[17] Thus, many who innocently flashed this sign on social media were unfairly castigated as racists. In one particularly unfortunate example, Alabama police officers were placed under investigation after a group of officers posed in a "Got 'Em!" picture.[18]

Although the laddish pranks of online tricksters were naively seen by some as benign, these sorts of native disinformation campaigns were amplified or taken advantage of by foreign agents. For instance, take the Crowley scandal that rocked the United Kingdom. In 2021, following a no-confidence vote in Her Majesty's Government over its handling of the United Kingdom's relationship with Europe, general parliamentary elections were triggered.

A reputed video of Conservative Party leader Robert Crowley exposing himself to clearly underage girls on the video chat website Omegle was posted on the 4Chan image board /pol/ two weeks before the May parliamentary elections. It quickly spread and was reported widely across several news agencies. The poor handling of the situation by the Conservative party led to sharp losses against the Labour party. However, following a criminal inquiry by Scotland Yard, it was discovered that the video was a "deep-fake" made by a small group of student left-wing Green Party activists. Irrespective, it was too late for Crowley and the Conservatives.

Additionally, despite not originating in Russia, the controversy was a golden opportunity for the Russians to exploit in further undermining Crowley's agenda in Europe. A staunch defense advocate, Crowley had endeavored to strengthen the United Kingdom's position in Europe. He voted to increase military spending, argued to station British service members in Poland, and planned to send British troops to advise and assist the Ukrainian army as prime minister if the Conservative Party won the general election. As the video gained traction, Russian social media accounts began to amplify the story and develop a narrative that casted the Conservative party as protecting pedophiles.

There are two lessons that should be drawn from the Crowley and 4Chan controversies. First, natural fissures in social cohesion can be widened by state actor intervention using disinformation techniques. Second, the challenge in combatting disinformation is not the lack of truthful information but rather the widespread proliferation and volume of disinformation. The Russian way of PSYOP seeks to cause paralysis through information discord. It often involves the use of techniques designed to saturate the target audience with false, often contradictory, information repeatedly. The veracity of the information is less important to a recipient than the number of times it is repeated. Thus, the tragic irony of the internet age is that despite citizens having access to a vast repository of information, the decentralized nature of the web in the West means that a nefarious agent has virtually unlimited ability to post whatever he or she so chooses.

This is now compounded by artificial intelligence, which can directly and indirectly act as disinformation force multipliers. As they have since the past decade, social media and web query platforms continue to have a strong financial incentive to keep users occupied on their sites for as long as possible. The longer a user is engaged, the more they see or click advertisements and thus the more money a company makes. Therefore, astonishingly sophisticated bots have been developed to analyze users and tailor their feeds to suit taste and interests. This can lead users to become trapped in a political echo chamber. Users click on videos or posts they like or agree with, leading the bot to continuously recommend videos that reinforce their beliefs in a bid to keep them engaged longer. As a result, it has become easy for a person to become trapped in a vortex of politically radical content that often spews disinformation. Repeated exposure to disinformation leads to belief in that disinformation, even if it is demonstrably false. There is often a snowball effect, too. A post, video, or article that is particularly sensational or salacious is more likely to be shared by users, leading to more users seeing that fake information and sharing it to their social networks.

Additionally, artificial intelligence is now used to refine disinformation in very threatening ways. As the mass of personal data online has grown, so too did the tools to analyze and make sense of that data. Advanced algorithms can sift through a person's online life, creating a psychological and political profile that is subsequently used in "micro-targeted" propaganda assaults.

Kremlin front organizations now have hundreds of ads, each tailored to a particular profile, that are "launched" at users based on their online behaviors.[19] This precision information assault is particularly dangerous. Disillusioned soldiers and diplomats, identified by their social media activity, are now at personal risk as never before of having their news feeds manipulated to magnify feelings of dissent. This creates a hospitable environment for foreign case officers to recruit spies and saboteurs. Furthermore, armed with data collected from social media platforms, actors can employ armies of "social bots" that aim to push narratives by pretending to be real people. These bots, coupled with human handlers, can "curate" content to mislead a target audience.

Although the U.S. Army routinely conducts military drills in Europe and rotates contingents of combat ready soldiers to potential hotspots like the Baltic States, its ability to engage in warfare stems not only from capability and posture but also domestic resolve. Though the president is authorized to deploy the military for up to ninety days by invoking the War Powers Resolution of 1973, the authority to declare war ultimately resides in

the democratically-elected Congress. Thus, malign actor states have taken to funding organizations that directly follow their instructions and promote their message, such as Chinese-funded cultural institutions that have become ubiquitous, indirectly supporting their information operations goals, such as movements advocating for isolationism or global retreat.

> The responsibility lies first and foremost with the native governments of those nations that are threatened, which is influenced by a variety of cultural, political, and economic factors.

In the eyes of our adversaries, undermining the domestic will to fight is now at least as important as deterring or defeating us militarily. The principle goal of such information operations (IO) strategy is to achieve the kind of practical result of the Vietnam War-era surprise Tet Offensive in 1968 (without actually conducting a Tet Offensive), which historically is seen as a turning point leading to loss of American popular support for that war. If in a similar manner Americans can be persuaded to doubt the importance of international treaty organizations, deterrence, and maintaining the rules-based global order, our country is considerably less likely to take actions that support those goals.

For example, from a Russian standpoint, making Americans doubt the value of sacrificing young eighteen- and nineteen-year-old soldiers to preserve the sovereignty of Lithuania may be almost as effective in achieving Russian goals as having the military capacity to threaten the physical sovereignty of Lithuania. Additionally, establishing satisfactory sociopolitical conditions can greatly reduce the length of or even prevent a conflict during an escalation sequence.

In other words, activity on the digital realm is a way of not only altering the human terrain in preparation for military operations but may be an effective and decisive military operation of itself. Disinformation, controversy manufacturing, inflaming social tensions, and keeping attention focused on divisive issues, are all means to weaken the internal resolve of a state's population or attack the integrity of the nation-state itself.

Since 2022, Russia has seemingly totally adopted the view that war is a total effort that encompasses an array of informational, military, diplomatic, and political strategies to defeat the enemy both before and during conflict. In countries like Latvia or Estonia, where the U.S. Army is most likely to engage not only with Russian conventional forces, but also irregular guerillas recruited from Russian-speaking minority populations, combatting Russian efforts to shape the human terrain is as important, if not more so, than military force that aims to deter, and also defeat military aggression. Yet efforts by the U.S. Army and diplomatic community to shape the human terrain are difficult to achieve at best. The responsibility lies first and foremost with the native governments of those nations that are threatened, which is influenced by a variety of cultural, political, and economic factors. For instance, 250,000 ethnic Russians continue to live in Latvia as "non-citizens." This gives many Latvian-Russians the feeling they are second class citizens, thus playing into victim narratives pushed by the Russian government. The U.S. Army cannot control Latvian citizenship policy, yet those policies inevitably aid Russian efforts to shape the human terrain in Latvia. Ultimately, the U.S. Army has to coordinate with local governments and the State Department to deploy narratives that do not conflict with the host nation's domestic political agenda—while at the same time ensuring that those same narratives are in keeping with the Army values.

If the printing press was the "seventh great power," as Napoleon once called it, and radio was indeed the "eighth great power," as Nazi propaganda minister Joseph Goebbels called it, then the internet today is the "ninth great power." Much like the printing press and radio before it, the internet has introduced a truly revolutionary new means of communicating information while also hastening its spread. And, just as the printing press spread social upheaval in revolutionary France and the radio helped the ascent of Nazism, the internet has already proved itself to be an immensely

powerful tool for agents seeking to change the world for better, and often, for worse. Whether the West and their armies can ever master it for the purpose of protecting democracy in the face of subversive antidemocratic elements that have considerably more leeway in exploiting it for their aggressive political purposes as of this writing remains yet to be seen. ■

This article was previously published by Military Review *as a Future Warfare Writing Program online article in June 2019.*

Notes

1. John Bowden, "Russian Government Funded Eastern European News Sites: Report," The Hill, 29 August 2018, accessed 25 March 2019, https://thehill.com/policy/technology/404137-russian-government-funded-eastern-european-news-sites-report.

2. Hanna Kazlowska, "On Twitter, Fake News Spreads Faster Than Truth, MIT Researchers Say," Quartz, 9 March 2018, accessed 25 March 2019, https://qz.com/1225921/on-twitter-fake-news-spreads-faster-than-truth-an-mit-study-says/.

3. Micah Zenko, "The Problem Isn't Fake News from Russia. It's Us," *Foreign Policy* (website), 3 October 2018, accessed 25 March 2019, https://foreignpolicy.com/2018/10/03/the-problem-isnt-fake-news-from-russia-its-us/.

4. Mike Glenn, "A Houston Protest, Organized by Russian Trolls," *Houston Chronicle* (website), 20 February 2018, accessed 25 March 2019, https://www.houstonchronicle.com/local/gray-matters/article/A-Houston-protest-organized-by-Russian-trolls-12625481.php.

5. University of Texas at Austin, "Facebook More Effective at Mobilizing Voters than Traditional Get-Out-the-Vote Efforts, Study Finds," UT News, 11 October 2016, accessed 25 March 2019, https://news.utexas.edu/2016/10/11/facebook-more-effective-at-mobilizing-voters/.

6. Janis Berzins, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*, Policy Paper No. 2 (Riga, Latvia: National Defence Academy of Latvia, Center for Security and Strategic Research, April 2014), accessed 2 April 2019, http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002- 2014.ashx.

7. Ibid.

8. Zhuang Pinghui, "Weibo Falls Foul of China's Internet Watchdog for Failing to Censor Content," *South China Morning Post* (website), 28 January 2018, accessed 25 March 2019, https://www.scmp.com/news/china/policies-politics/article/2130931/weibo-falls-foul-chinas-internet-watchdog-failing.

9. Adam Freelander, "Nothing is Real: German Scientists Figured Out a Way to Make Putin and Trump Say Anything," Quartz, 5 April 2016, accessed 25 March 2019, https://qz.com/654669/nothing-is-real-germanscientists-figured-out-a-way-to-make-putin-and-trump-say-anything/.

10. Tom Nichols, "How America Lost Faith in Expertise," *Foreign Affairs* (website), 13 February 2017, accessed 25 March 2019, https://www.foreignaffairs.com/articles/united-states/2017-02-13/how-america-lost-faith-expertise.

11. Brian Stelter, "New York Times has Record Subscriber Growth— and Some Bad News Too," CNN Business, 3 May 2017, accessed 25 March 2019, https://money.cnn.com/2017/05/03/media/new-yorktimes-subscriber-growth/index.html.

12. Adam Taylor, "An Alleged Rape Sparked Tensions between Russia and Germany. Now Police Say It Was Fabricated," *Washington Post* (website), 29 January 2016, accessed 25 March 2019, https://www.washingtonpost.com/news/worldviews/wp/2016/01/29/an-allegedrape-sparked-tensions-between-russia-and-germany-now-police-say-itwas-fabricated/.

13. Jessica Roy, "Cuck, 'Snowflake,' 'Masculinist': A Guide to the Language of the 'Alt-Right,'" *Los Angeles Times* (website), 16 November 2016, accessed 25 March 2019, https://www.latimes.com/nation/la-napol-alt-right-terminology-20161115-story.html. 4Chan is an online forum divided into topic-specific image boards. /b/ is the offtopic board dedicated to general discussion, and it is most infamously known as the home of "The Fappening," when users published nude photographs of celebrities stolen from iCloud. /pol/ is the political discussion board where discourse typically revolves around white supremacism, antifeminism, and alt-right ideology.

14. Dylan Matthews, "No, a Former Kavanaugh Clerk Didn't Flash a 'White Power Sign.' Here's What Really Happened," Vox, 5 September 2018, accessed 1 April 2019, https://www.vox.com/2018/9/5/17821946/white-power-hand-signal-brett-kavanaugh-confirmation-hearing-zina-bash-4chan.

15. "How the 'OK' Symbol Became a Popular Trolling Gesture," *ADL Blog*, Anti-Defamation League, updated September 2018, accessed 1 April 2019, https://www.adl.org/blog/how-the-ok-symbol-became-a-popular-trolling-gesture.

16. Dennis Romero and Dystany Muse, "Coast Guard Member Flashes White Power Hand Signal on TV," NBC News, 14 September 2018, accessed 1 April 2019, https://www.nbcnews.com/news/us-news/coast-guard-member-flashes-white-power-hand-signal-tv-n909856.

17. Urban Dictionary, s.v. "Circle Game," by Erekai, 24 June 2011, accessed 1 April 2019, https://www.urbandictionary.com/define.php?term=Circle%20Game.

18. Stephen Quinn, "Alabama Police Officers Suspended for Hand Gesture Linked to 'Circle Game,'" WBMA News, 16 July 2018, accessed 1 April 2019, https://abc3340.com/news/local/jasper-police-officerssuspended-for-hand-gesture-linked-to-circle-game.

19. Sara M. Watson, "Russia's Facebook Ads Show How Internet Microtargeting Can Be Weaponized," *Washington Post* (website), 12 October 2017, accessed 1 April 2019, https://www.washingtonpost.com/news/posteverything/wp/2017/10/12/russias-facebook-ads-show-how-internet-microtargeting-can-be-weaponized.