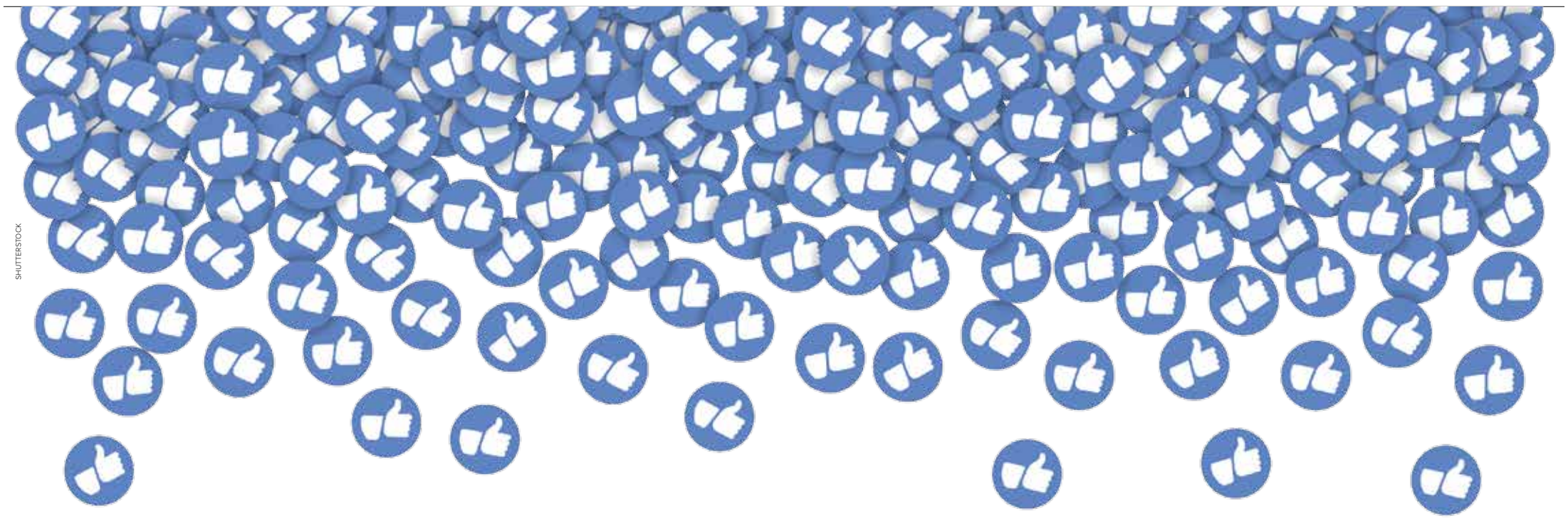

SHUTTERSTOCK

The real cyber threat is your likes

It was the largest data breach in German history. But what made it remarkable is what came after the massive theft of information: its spread

BY P.W. SINGER AND EMERSON BROOKING

All through December 2018, a hacker by the online handle "Orbit" teased and tantalized his followers, releasing a new heap of hacked emails, chatlogs and home addresses each day. At first, German comedians, YouTube stars, rappers and TV stars were the only ones affected, with the media and public commenting and sharing the information that went viral. But then the real target, over 1,000 politicians from the Free Democrats and Greens to the Social Democrats and the Christian Democratic Union, were hit. This led to a wave of wave of finger-pointing and a slew of questions: Why was the far-right AfD the only party spared? Why had the federal government and information security agency, the BSI, originally dismissed the breach in December as a "one-off incident"?

Yet, what so shocked the German political system should not have been a surprise, as it followed a familiar script. Social media's use as a new kind of weapon to spread disarray had previously struck everywhere from the Brexit vote in the UK to elections in the US, France, Brazil, Italy, the Philippines and Mexico. And it has also appeared in conflicts ranging from the Ukraine invasion to the Syrian civil war. This new kind of attack is not about hacking the networks of computers (known as cyber warfare) but, rather, hacking the users of social networks, driving ideas viral through a mix of "likes" and lies – what we call "LikeWar."

Over the last year, revelations of such operations targeting democracies have come out in dribs and drabs, meaning that the sum total is greatly underappreciated. For instance, after initially downplaying the problem, Facebook now estimates 146 million Americans – roughly half the nation's population – saw content on its networks surreptitiously pushed by Russia's information warriors during the 2016 vote. On Twitter, tweets driven by Russian trolls and bots were viewed at least 288 million times in just the closing six weeks of the election. Meanwhile, a study of just 28 Instagram accounts since identified as being covertly operated by the Russian government shows that they alone drew an astounding 145 million "likes," comments and plays of their embedded videos.

Importantly, the reach of these efforts is much wider than even those numbers show, as they rippled out into other media. It has become increasingly common among journalists to use social media to determine what stories to cover, what angle to take and whom to interview, meaning online trends also shape radio, newspapers and TV. For instance, British journalists shared the false Russian accounts, as if they were authentic voices, in stories on at least 80 different topics ranging from Brexit to the London bridge attacks.

While it is up to the historians to debate the impact that such campaigns had in historically close elections, we do know one thing: the attackers think it worked, because they are still at it now. In the US, Russian accounts have since been caught trying to glom onto everything from the NFL anthem controversy to debates over gun rights, while in Europe, they are expected to go after the wave of elections in the spring.

Whatever the topic, the goal is always the same: using online means to alter real-world beliefs and actions. To compound the problem, it is no longer just Russia whom we must keep an eye on; there are also dueling online influence campaigns by Saudi, Qatari and Iranian operatives as well as would-be authoritarians in places like Turkey or the Philippines that are weaponizing social media. According to the Oxford Internet Institute, an estimated 48 nations now engage in some form of social media manipulation. To make matters worse, this can involve a mercenary-for-hire situation – the LikeWar version of private military contractors.

As bad as all this may seem, the battles playing out on every smartphone are set to worsen. Just as the first biplanes introduced into World War I quickly became antiquated, the tactics and technologies used in the first wave of LikeWar will be soon surpassed. A massive increase in data availability will enable propagandists to target smaller and smaller segments of a population, going after not merely a national vote, but single legislative districts or even local elections. In turn, the ongoing revolution in artificial intelligence will enable machine-run accounts – "bots" – to masquerade effortlessly as humans, as well as the creation and then weaponization of fabricated images and video that are indistinguishable from the real thing – known as "deep fakes."

But that future has not arrived yet. NATO has stood strong for 70 years, adapting to ever-changing military technologies and political conditions. There is still time to confront this newest challenge. But our work must begin now.

First, we must acknowledge the stakes and adjust our perception of and preparation for online threats. Since 2006, NATO has codified the importance of cybersecurity in its formal strategy, establishing and expanding new capabilities and doctrines. It must do the same for the LikeWar side, as events have shown online influence operations to be equally or even more threatening to the Alliance. Indeed, by altering political realities in several key member states, NATO itself has been called into a question like never before in its history.

In this endeavor, though, NATO cannot look to the United States for leadership. While the US may have invented the internet, it is now the poster child for how not to face these new online threats.

Instead, the best model for responding aggressively comes from the countries nearest Russia, as they were the first to suffer such attacks. Drawing on a mix of defense strategy, education and lessons from public health, countries like Estonia and Sweden have moved towards "whole-of-nation" efforts intended to inoculate their societies from viral misinformation. Overall, these countries seek to build a layered defense, through efforts like citizen education programs, public tracking and notices of foreign disinformation campaigns, enhanced transparency of political campaign activities, and action to limit the effect of what might be thought of as "superspreaders," the subset of people and accounts who serve as statistically virulent distributors of online disinformation.

It is equally important to recognize that this battleground may shape security and politics, but the terrain itself is managed by a handful of private companies.

In many ways, Silicon Valley's response has been most akin to that of parents progressing through the stages of grief after a dark turn taken by their creations. For instance, Mark Zuckerberg went from denial – claiming it was a "pretty crazy idea" that such threats mattered – to acceptance – discussing recently how his firm is in an "arms race" with information warriors. But while the firms have laudably stepped up measures for disinformation campaigns attacking both their customers and their home nation, there is still a long way to go. Indeed, on Twitter, some 80 percent of the accounts that spread the most misinformation during the 2016 election are still online today, pushing "upward of a million tweets a day," while the Brazilian election saw many of the same online toxic forces prevail, despite a new wave of Facebook reforms.

Governments must endeavor to work more closely with these companies; to work as helpful friends in some cases, providing needed information and tips; and to apply regulatory pressure when they fall short. The needed efforts by the tech firms include stepped-up investment in content moderation; creating a cross-industry information clearing house on disinformation operations akin to the organizations that industry sectors like banking have in cybersecurity threat-sharing (known as ISACs); "deplatforming" proven super-spreaders of harassment and foreign influence operations; wargaming their products before they are deployed into the world, not just to uncover cybersecurity vulnerabilities, but likely misuse by attackers as well; labeling bots and deep fakes to allow humans to know when they are interacting with a machine online (aka the "Blade Runner" rule); and implementing measures to identify and foil the next generation of AI used as sophisticated chatbots and faked imagery.

Yet, one of the best things these firms can perhaps do is to aid their own customers in better understanding how their very business works, which means admitting the inherent dangers that come with it. For instance, 74 percent of Facebook users do not even know the basics of where the information that pops up in their feed comes from, that the firm collects and shares data about them, or even the difference between the online news and advertisements that are deliberately interwoven. Digital literacy is now also a national security issue. But, similar to public health or cybersecurity, it is one that requires both the government and the private sector to play a part. Imagine a world where instead of downplaying Russian information attacks, the firms deployed pop-up tutorials that explained how you had been taken in and then how to prevent this from happening again.

But there is also a larger problem that will stay with us until we acknowledge the elephant in the room in Munich. The challenge for any proper Western government response to new online threats is not merely that the only cabinet meeting the US president has ever held on election security did not discuss the problem of disinformation, or that his administration has not used nearly any of the $100 million dollars allocated to it by Congress to combat Russian influence operations. The challenge is that the commander-in-chief himself is a core part of the problem, with @realdonaldtrump acting as a venue for disinformation on nearly a daily basis.

But Donald Trump is far from the only one. We now have the data to track who provided their personal megaphone to elevate foreign government misinformation and the forces of extremism. It is remarkable how few have apologized for aiding and abetting enemies who seek to harm democracy, or explained what actions they are taking to prevent future votes from being poisoned.

The battles waged on social media are no longer merely about personal branding or political identity. They are about the very future of our democracies. ■

P.W. SINGER AND EMERSON BROOKING are co-authors of the book *LikeWar: The Weaponization of Social Media*. Portions of the above article previously appeared in *The Guardian*.

Showing backbone

We need a genuine European Cybersecurity Agency

BY SIR JULIAN KING

The security threats we face, not only in Europe but around the world, are increasingly cross-border in nature. Those who seek to harm us pay little heed to the niceties of national boundaries or international law.

Successfully tackling these cross-border threats requires a cross-border response. Our work on security in the European Union underscores the added value in enhanced cooperation. Security is first and foremost a national responsibility. But we also work with member-state authorities, providing the tools and support needed to help keep Europeans safe from the threats posed by terrorism as well as organized and cybercrime.

In response to the series of deadly terror attacks on European soil in recent years, we have sought to deny terrorists their means to harm by restricting their movement and access to money, munitions and manpower. Along the way, we have strengthened our capacity to not only prevent attacks but improve our response when they do take place. This includes countering radicalization by working on the ground in our communities and by tackling terrorist content online. We have also made headway in improving how we protect our public spaces and our support for victims of terrorist attacks.

We are working to counter the fast-growing and evolving array of cyber and cyber-enabled threats we face. We are in the process of introducing a new EU Cybersecurity Act aimed at building our resilience, strengthening our deterrence and supporting member states in cyber defense. This includes creating a European Cybersecurity Agency with the authority to develop a new European certification scheme, coordinate the response to major incidents and institute a network of competence centers. Moreover, we must establish credible disincentives for those who may contemplate cyberattacks, including improving law enforcement access to electronic evidence.

We also need to tackle cyber-enabled threats, which include disinformation and the manipulation of data and behavior. This is particularly important in terms of election security and ensuring that our democratic processes are free, fair and open.

We have introduced a series of measures – with member states, the European Parliament and European political parties – to guard against cyberattacks, data abuse and disinformation. We want to reinforce cooperation with fact-checkers to call out disinformation. And we need internet companies to step up and make real progress on their commitments to tackling disinformation.

These commitments on the side of industry include improving how advertisements are placed online, strengthening transparency around sponsored content, rapidly identifying and deleting fake accounts, regulating the use of bots, promoting more effectively genuine narratives that are maliciously obscured and being more clear about the use of algorithms. Last month, we reported on the progress made by internet companies and while we acknowledge their efforts, they must go further and faster if they are the effect required before the European elections in May.

In Europe, we need to discuss whether we want to continue watching our own cutting-edge technologies sold off, one after another. We also need to consider how we might minimize the risk of a dominant supplier within a given sector emerging across the continent. Deepening European coordination would also allow our collective investment in artificial intelligence and other vital technologies, such as quantum computing and cryptography, to yield more than the sum of its parts.

These issues present challenges to national decision-making that will not be easy to resolve. Trying to protect everything will not work. We must determine what really matters in a digital ecosystem and whether greater transparency around suppliers, supply chains and foreign investment is enough to offset the security risks. It may be that certain elements of digital infrastructure are simply too critical to risk.

Wherever that discussion takes us, cooperation is clearly essential to our work on all these security challenges. The only way to tackle them successfully is to work together at several levels, including the European level.

As threats evolve, we must strengthen and deepen our joint efforts to help keep Europe safe. ■

SIR JULIAN KING is European commissioner for the Security Union.