2
Understanding Disinformation Operations in the Twenty-First Century

Steven J. Barela and Jérôme Duberry

Although there is nothing necessarily new about propaganda, the affordances of social networking technologies—algorithms, automation, and big data—change the scale, scope, and precision of how information is transmitted in the digital age.[1]

I. Introduction

The term *dezinformatsiya* is said to have been coined by Joseph Stalin and denotes the political tactic of spreading fragments of falsehoods by design against one's adversaries.[2] One valuable source to begin understanding such actions is through the former three-star general for the secret police of Romania, Lt. Gen. Ion Mihai Pacepa, who in 1978 was one of the highest-ranking officials to defect from the Communist bloc. Our chapter will begin here as his view offers unique insights into the nature of the activity.

Beyond this basic understanding, there is a reason why the global community is witnessing a dramatic rise of state-sponsored disinformation operations carried out across international borders: the remarkable developments in information and communication technologies (ICTs) provide opportunities for spreading *dezinformatsiya* with a volume and accuracy that has never been known before. In the wake of such actions—to be labeled *disinfo-ops* in this chapter—the targeted societies have found themselves destabilized as facts and events become deeply contested among citizens. Indeed, we believe that much of the exacerbated political division we are witnessing today arises from a wide disagreement over the terms of what is actually happening in society.

Political marketing innovations have led to the emergence of a novel news ecosystem where marketeers, political parties, and criminal groups share the same tools, strategies, and expertise to access citizens' data and influence their behavior. The rapid

[1] Samantha Bradshaw & Philip N. Howard, The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation, Project on Computational Propaganda 11 (2019).

[2] Lt. Gen. Ion Mihai Pacepa & Ronald J. Rychlak, Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism 39 (2013).

Steven J. Barela and Jérôme Duberry, *Understanding Disinformation Operations in the Twenty-First Century* In: *Defending Democracies*. Edited by Duncan B. Hollis and Jens David Ohlin, Oxford University Press (2021). © Duncan B. Hollis & Jens David Ohlin. DOI: 10.1093/oso/9780197556979.003.0003

and wide growth of social media platforms and associated marketing instruments has contributed to the emergence of a new set of vulnerabilities—exploited with the greatly enhanced *breadth*, *depth*, and targeting *precision* of digital disinformation campaigns.[3]

In the coming pages we provide a descriptive work to illustrate the essential components of this activity today, to be organized in the following manner. Section II will offer a view on Soviet-era disinformation campaigns through the eyes of Pacepa, the former Romanian intelligence chief. Sections III and IV will respectively outline the elements of information warfare and the role of today's big data and social media platforms. Then, to provide detailed insight into the practice, we will put forward an example in section V of distorted content based on foreign maneuvers being amplified in social media.

There are three important conclusions to draw from this exploration. First, because disinformation aims to twist the truth in subtle ways when key facts remain secret and unavailable, exposing an operation becomes a tedious and difficult task. Second, the new digital world of ICTs has opened the door to omnipresent operations that occur below the threshold of armed conflict and are accelerated exponentially by big data warehousing and algorithms that allow individualized targeting during an election cycle. Each of these developments requires progress in international law to regulate an activity that is different in kind from what has been previously known. Third, when disinformation operations disrupt the flow of information during a political campaign, the candidates involved and the process itself emerge with an eroded legitimacy—a sine qua non for all societies.

In addition to these insights, this study brings us to one overall important finding: breaking and distorting information flows within a foreign society goes largely untracked today. The bulk of these operations are occurring in the difficult to research space of online social media (closed for reasons of privacy and trade secrets). Consequently, section VI will close our chapter by raising a clarion call to allow access for social scientists to study what is happening in this opaque public square where ever more political understanding is being fashioned. More comprehensive empirical study promises to unlock desperately needed details still missing from the analysis of digital *disinfo-ops*.

II. *Dezinformatsiya*

Capturing the nature and essence of disinformation is by no means easy. When an operation is successful, people have been subtly influenced to accept a narrative that has been purposefully bent by external forces to accommodate a political agenda. However, very few people readily admit that they have been duped, manipulated, or even influenced by someone without their knowledge. We all cherish our intellectual

[3] In particular, we believe these three parameters should be used to give measurable and verifiable shape to the term of "coercion" as it pertains to the international law principle of nonintervention. *See* Steven J. Barela, *Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion*, Just Security (Jan. 12, 2017); Steven J. Barela, *Zero Shades of Grey: Russian-Ops Violate International Law*, Just Security (Mar. 29, 2018).

autonomy. When such a campaign is carried out on a massive scale, proving its existence often runs against conventional knowledge of facts and events. So how do we talk about widely shared misunderstandings that have been pushed with tiny nudges from an outside force?

As a starting point it is helpful to note that this practice has been classified under various terms over the last century. One volume on intelligence history has explained that during the Soviet era, "disinformation operations against enemy special services had several [...] designations: 'actions of influence,' 'operational disinformation,' 'active measures,' 'operational games,' 'assistance measures' etc."[4] Today, "information warfare," "information confrontation," and "cyberwarfare" are terms often used to describe such subversion campaigns aiming to weaken and undermine adversary societies using ICTs.[5] Nevertheless, the existence of multiple terms already demonstrates part of the difficulty. Some scholars have pointed out that words themselves are used to obfuscate: " 'Active measures' is a historical, now somewhat imprecise term. Like many Russian terms, this one also is a façade, behind which various methods of influencing the international community are concealed."[6] Duly noting these variations, we will simplify the discussion in this chapter by largely applying "disinformation" and *dezinformatsiya* for the deep-rooted Soviet tactic, and *disinfo-ops* for today's application with new technologies.

To illuminate the discussion for our purposes we turn to Lt. Gen. Ion Mihai Pacepa and look into his 2013 book, co-authored with Ronald J. Rychlak, entitled, *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*.[7] In doing so, even briefly, it is necessary to acknowledge that many of the suggested corrections to contemporary events can produce pause. This is because successful information operations make searching for a truth that runs counter to a dominant belief onerous and time-consuming.[8] To then convince others of the need for correction becomes another daunting task entirely. As

[4] Herbert Romerstein, *Disinformation as a KGB Weapon in the Cold War*, 1 J. INTEL. HIST. 54 (2001) (citing OCHERKI ISTORYA ROSSIISKOY VNESHNY RAZVEDKI, MEZHDUNARODNIYE OTNSHENIYA, VOL. 2, at 13–14 (Y.M. Primakov ed., 1996)).

[5] *See, e.g.*, KEIR GILES, HANDBOOK OF RUSSIAN INFORMATION WARFARE 24 (NATO Defense College, 2016); THOMAS ELKJER NISSEN, #THEWEAPONIZATIONOFSOCIALMEDIA 31 (Royal Danish Defence College, 2015); Andrew Foxall, *Putin's Cyberwar: Russia's Statecraft in the Fifth Domain*, 1 Russia Studies Centre (Policy Paper No. 9, 2016); Dima Adamsky, *Cross-Domain Coercion: The Current Russian Art of Strategy*, Institut français des relations internationals 1–43 (Proliferation Papers No. 54, 2015). For discussion of what has been incorrectly termed the "Gerasimov Doctrine" from the scholar who created it, *see* Mark Galeotti, *The Mythical "Gerasimov Doctrine" and the Language of Threat*, 7 CRIT. STUD. SEC. 157–161 (2019); *see also* Mark Galeotti, *The "Gerasimov Doctrine" and Russian Non-Linear War*, IN MOSCOW'S SHADOWS (2013), *at* https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ (Galeotti's original blog publishing the first translation by Rob Coalson of the speech by Russian Chief of the General Staff Valery Gerasimov in 2013 appearing in VOENNO-PROMYSHLENNYI KUR'ER (Military-Industrial Courier)).

[6] Jolanta Darczewska & Piotr Żochowski, *Active Measures, Russia's Key Export*, 64 POINT OF VIEW 12 (Centre for Eastern Studies, No. 64, 2017).

[7] *See* PACEPA & RYCHLAK, *supra* note 2. For similar firsthand testimony of a Czech defector from the Czech intelligence and security services, *see* LADISLAV BITTMAN, THE KGB AND SOVIET DISINFORMATION: AN INSIDER'S VIEW 50 (1985); *see also* KGB defector Yuri Bezmenov, *Warning to America*, YOUTUBE (Feb. 1, 2013), *available at* <https://www.youtube.com/watch?v=bX3EZCVj2XA>.

[8] *See* GILES, *supra* note 5, at 58 ("countering every single piece of Russian disinformation is labour-intensive out of all proportion to the result").

a result, our intention in this first section of the chapter is simply to elucidate the elusive concept of disinformation, rather than to analyze the veracity of the entire list of historical amendments presented in the Pacepa and Rychlak book.[9]

As one of the top advisers to President Nicolae Ceauşescu of communist Romania and chief of its intelligence service, Pacepa's perspective is unique. He is able to discuss the concept of disinformation from the vantage point of key meetings, access to top-secret documents, and sensitive discussions within the KGB of the Soviet era. Fundamentally, the intelligence services that Pacepa oversaw were spending a great deal of their resources curating narratives, rewriting history, and framing enemies rather than gathering information. In fact, the function of discovering what adversaries were doing was largely subordinated to the efforts of manufacturing and propagating a slightly adjusted reality to suit their government's interests: "During the Cold War, more people in the Soviet bloc worked for the disinformation machinery than for the Soviet army and defense industry put together."[10]

Even if deception has deep roots around the globe in wartime, Pacepa claims that the idea that this tactic should be elevated to the status of a permanent peacetime national policy was born in Russia.[11] As one indication of this, he recounted that the highly classified Russian training manuals on disinformation taught that it was first the fruit of Prince Grigory Potemkin's efforts to charm Catherine the Great. Many know that Prince Grigory constructed empty-façade villages to feign rural prosperity along the route she would take in Crimea in the eighteenth century—hence the term used today of a "Potemkin village."[12] These manuals that regulated and instructed Pacepa's role as an intelligence chief made special note of its Russian roots and proudly termed it a "science."[13] So sophisticated was this science that Joseph Stalin chose to even obscure its origins to the outside world by spreading the rumor that the Russian term actually only came as a translation from the French. Pacepa explains that his intelligence services were instructed to circulate this idea by their Soviet counterparts,

[9] Pacepa and Rychlak contend that the Soviet Union, followed by Russia, launched information operations that range from framing Pope Pius XII as Hitler's Pope, claiming CIA involvement in the assassination of President John F. Kennedy, fanning the flames of conflict in the Middle East, launching defamatory attacks on American soldiers in Vietnam, and advancing a socialist transformation in the United States during the Obama era. *Id*. Perhaps most troublesome for these authors is the charge of a false story put forward in the epilogue: "France and Germany accused the US of torturing the al-Qaeda prisoners held at its military prison in Guantanamo Bay, Cuba" *Id.* at 353. This has now undoubtedly been shown to be true—not *dezinformatsiya*. *See, e.g.*, Interrogation and Torture: Integrating Efficacy, with Law and Morality (S.J. Barela et al. eds., 2020). This last erroneous assertion shows an enormous difficulty caused by disinformation—it can often be dismissed as a matter of political perspective. Nevertheless, amplifying illegal, immoral, and ineffective actions by the CIA in this case can still serve the purposes of the operation to delegitimize the government of an adversary.

[10] Pacepa & Rychlak, *supra* note 2, at 38; *see also* Bezmenov, *supra* note 7 ("The main emphasis of the KGB is not in the area of intelligence at all. According to my opinion, and many opinions of defectors of my caliber, only about 15% of time, money and manpower is spent on espionage as such. The other 85% is a slow process which we call ideological subversion or active measures.").

[11] Pacepa's claim of the initial historic roots starting in Russia is less important here. More importantly, we find that other various sources suggest that for Russia today, there is little difference between wartime and peacetime. *See* Giles, *supra* note 5, at 4; Adamsky, *supra* note 5, at 29.

[12] Pacepa & Rychlak, *supra* note 2, at 36–37.

[13] *Id.* at 36.

and the operating definition is captured in the 1952 edition of the *Great Soviet Encyclopedia* that describes it as a capitalist tool:

> DEZINFORMATSIYA (from *des* and French *information*). Dissemination (in the press, on the radio, etc.) of false reports intended to mislead public opinion.[14]

While the Pacepa and Rychlak book offers general descriptions of disinformation as a means, most intricate and extensive are the dismantlings of successful Soviet operations that have taken root and grown into a narrative all their own. To carry out the task that dominates nearly half of the book—unraveling the transformation of a Christian leader who silently provided aid and saved numerous Jews during the Holocaust into "Hitler's Pope"—Lt. Gen. Pacepa worked with a co-author who is a historian and law professor. Professor Rychlak had extensively researched and written his own book on the subject of Pope Pius XII, uncovering Soviet efforts to discredit the Catholic Church and its leader.[15] The two were well suited to their task: "an in-depth, guided tour of a sophisticated, complicated, long-term, multifaceted campaign of pure lies and smears. That is the nature of disinformation."[16]

Emerging from World War II, Joseph Stalin took to framing those whom he saw as a threat as "Nazi collaborators" and removed them from the scene via arrest, trial, detention, or death. This included high-ranking figures in the Ukrainian Catholic Church. Pius XII issued an encyclical announcing that "all its bishops and many of its priests have been arrested," and assured the faithful in Ukraine that God would "calm this terrible storm and . . . bring it to an end."[17] The authors explain that this was taken as a deep affront by Stalin and an offensive disinformation campaign was launched against Pius XII along with other Catholic leaders.

One of the most dramatic operations described in the book was unleashed upon the archbishop of Hungary, Jószef Mindszenty.[18] It was lauded in the highly classified Soviet manuals of disinformation because it was meant to encapsulate a significant refrain emphasized in all caps on the first page, "IF YOU ARE GOOD AT DISINFORMATION, YOU CAN GET AWAY WITH ANYTHING."[19] That is, the KGB believed that the operation against Cardinal Mindszenty showed that it was possible to "neutralize even a saint" and was one of "our most stupendous, monumental *dezinformatsiya* operations."[20] The Roman Catholic clergyman was arrested and convicted of treason in 1949, and then later sought asylum in the U.S. embassy of Budapest, spending fifteen years in voluntary confinement there. Today the *Encyclopedia Britannica* explicates that he "personified uncompromising opposition

[14] *Id.* at 39. The *Larousse* dictionary carried no mention of the word in either its 1952 or 1978 editions.

[15] Ronald J. Rychlak, Hitler, the War, and the Pope (2010).

[16] Pacepa & Rychlak, *supra* note 2, at 55. As seen later, the accusation of "pure lies and smears" is an exaggeration.

[17] Encyclical of Pope Pius XII to the Venerable Brethren, the Patriarchs, Primates, Archbishops, Bishops, and other Ordinaries in Peace and Communion with the Apostolic See (Dec. 23, 1945), *available at* <http://www.vatican.va/content/pius-xii/en/encyclicals/documents/hf_p-xii_enc_23121945_orientales-omnes-ecclesias.html>.

[18] Alex Last, *Fifteen Years Holed Up in an Embassy*, BBC News (Sept. 6, 2012).

[19] Pacepa & Rychlak, *supra* note 2, at 80.

[20] *Id.*

to fascism and communism in Hungary for more than five decades of the 20th century."[21] Nonetheless, this opponent was forced into isolation.

While the Mindszenty case would appear to be more straightforward, the same cannot be said for Pope Pius XII. Indeed, successful operations are built on two pillars:[22] first, they must contain a "kernel of truth";[23] and, second, they should be planted in local sources to lend credibility to the narrative far beyond what the Soviets could achieve with their own statements.[24] When these two elements are the foundation, disentangling and proving the existence of a foreign operation are extremely difficult.

In this case, the solid grain of fact that would serve as the foundation of the campaign against Pius XII was that he never publicly denounced the persecution of Jews and anti-Semitic laws by Nazis—neither during nor after the war.[25] Of course, Pacepa and Rychlak go out of their way to document the moments when Pius XII spoke up and defended the Jews during the Holocaust.[26] However, at the same time, one moment that has been commemorated in a plaque in the historic Jewish ghetto outside the windows of the Vatican is the night of October 16, 1943, when over one thousand Jews were rounded up and deported out of Rome to Auschwitz.[27] This tragic event is a hard truth.

As for sources from the West that framed Pius XII, three are deeply analyzed by Pacepa and Rychlak to unknot an extensive campaign. One is the book *The Silence of Pius XII*, which uses "heavy-handed documentation" from a communist Croatian trial[28] that was later annulled.[29] These discredited records from Soviet secret police forces found their way into the prominent work on the subject by John Cronwell's *Hitler's Pope*;[30] Rychlak systematically dismantles his "exclusive" archival research and

[21] ENCYCLOPEDIA BRITANNICA, *József Mindszenty, Hungarian Bishop*, *available at* <https://www.britannica.com/biography/Jozsef-Mindszenty>.

[22] PACEPA & RYCHLAK, *supra* note 2, at 96 ("To ensure credibility of the lies, two things were required. First the fabrications had to appear in Western sources; and second, there had to be what Sakharosky called "a kernel of truth" behind the allegations, so that at least some part of the story could be definitely verified—and to ensure that the calumny would never be put to rest").

[23] *Id.*at 38.

[24] *Id.* at 35–36.

[25] Interview with historian and Rabbi David Dalin, *Pius XII Saved More Jews Than Schindler, Rabbi Says*, ZENIT.ORG (Aug. 28, 2001) ("His silence was an effective strategy directed to protecting the greatest possible number of Jews from deportation. An explicit and severe denunciation of the Nazis by the Pope would have been an invitation to reprisals, and would have worsened attitudes toward Jews throughout Europe.").

[26] Pinchas E. Lapide (after months of research at the Israeli consul in Italy) wrote: "The Catholic Church saved more Jewish lives during the war than all other churches, religious institutions and rescue organizations put together. Its record stands in startling contrast to the achievements of the International Red Cross and the Western Democracies … The Holy See, the nuncios, and the entire Catholic Church saved some 400,000 Jews from certain death [the estimate was eventually increased to 860,000]." PACEPA & RYCHLAK, *supra* note 2, at 68.

[27] Lisa Palmieri-Billig, *Italy's First Holocaust Museum to Be Built in Rome*, JERUSALEM POST (Feb. 22, 2011) ("The section on Italy promises to draw extreme interest, with documentation on the country's most famous controversial wartime issues. It will explore both the positive and negative roles of the Vatican—its proverbial silence during the 1943 deportations, contrasted with the opening of its institutions to thousands of Jewish refugees; and its helping Jews by providing false documents, but also helping Nazis flee to South America after the war.").

[28] Whitall N. Perry, *Book Review: The Silence of Pius XI by Carlos Falconi*, 4 ST. IN COMP. REL. (Winter 1971).

[29] *Croatia overturns conviction of WW2 "collaborator" Cardinal Stepinac*, BBC NEWS (July 22, 2016).

[30] Jure Krišto, *Book Review Accentuation of the Known and Repetion of Untruths: About the Book John Cornwell, Hitler's Pope. The Secret History of Pius XII (1999)*, 32(1) ČASOPIS ZA SUVREMENU POVIJEST (2000)

cherry-picked citations that even suggest Pius XII was partly responsible for Hitler's rise to power and the Holocaust itself.[31] The authors additionally trace the writing and production of a play that denigrates Pius XII as a Nazi collaborator: *The Deputy. A Christian Tragedy*. They discuss its premier in Berlin and follow it to Paris, London, and New York, where it won a Tony award on Broadway (and finally made it to film).[32] And to show nefarious intent, they track the anti-Semitism and Holocaust denials, along with the promotion, reviews, and printings of the theatrical piece financed and pushed with communist and KGB connections.[33] All of this makes for tedious work to add nuance to a complicated story.

One final piece of a successful disinformation campaign should also be noted: incomplete knowledge gives life to a false storyline. As can be noted in the previous analysis, a great deal of (further) research and verification of sources is necessary to definitively prove or disprove a narrative. Disinformation thrives on conflicting stories that demand unavailable verification. Thus, effective *dezinformatsiya* aims to push a description of events, while opacity rules the day.[34]

For this reason it is important to point out that this discussion over Pope Pius XII has become polarized over the past decades—during the time when a full accounting has remained obscured.[35] The archives at the Vatican (no longer designated as "Secret" by order of Pope Francis[36]) will only now be opened to scholars in March 2020 to shed a fuller light on the matter with reports, letters, notes, and telegrams from the Vatican on decisions surrounding the highly sensitive days of Pius XII.[37] Hence, even more work is in store to present a full picture to avoid exploitation.

We now pivot to discuss weaponized information in the twenty-first century and the greatly expanded opportunities for spreading falsehoods in the cyberworld. To set the stage it is fitting to transition with two final descriptions of *dezinformatsiya*. The first comes from a volume on Russian intelligence history edited by Yevgeni Primakov, former prime minister of Russia and a prior chief of Soviet intelligence

("Cornwell's treatment of Catholic Church in the Independent State of Croatia ... is a travesty of research and objective writing. Cornwell perhaps did not know, but he could have and must have been informed, that Falconi wrote his piece on the basis of the propagandistic material given to him by the Yugoslav secret service and propagandists").

[31] Pacepa & Rychlak, *supra* note 2, at 188–195.

[32] *Id.* at 120–140.

[33] *Id.* at 141–182.

[34] We explain in the following section how the recent conflict in Ukraine, and in particular the annexation of Crimea, illustrates this point. Contradictory narratives communicated through official and nonofficial channels by Russian authorities contributed to create a veil of opacity over what was really happening in the field, and consequently bought time for Russian military troop to launch the kinetic military operation.

[35] Harriet Sherwood, *Unsealing of Vatican Archives Will Finally Reveal Truth about "Hitler's Pope,"* The Observer (London) (Mar. 1, 2020) ("Mary Vincent, professor of modern European history at Sheffield University, said that much of the criticism of Pius Xll lacked nuance. 'He was a careful, austere and quite unlikable man, trying to steer a path through almost impossible circumstances. He had clear views about what he saw as the threat of Soviet communism, and his view of Italian fascism was quite a bit softer. But categorising him as good or bad is not helpful—it's about the decisions he took, and the space he had to make those decisions.'").

[36] Nicolas Senèze, *Vatican Archives Will No Longer Be "Secret,"* La Croix International (Oct. 30, 2019).

[37] Lisa Palmieri-Billig, *Opening of Pius XII Archives: To Speak or Not to Speak: That Was the Question*, La Stampa: Vatican Insider (Feb. 27, 2020); Sylvia Poggioli, *Vatican Opens Archives of World War II–Era Pope Pius XII*, National Public Radio News (Mar. 2, 2020).

services. Regardless of the many various terms that have been applied to these types of operations, it was explained: "they all were and are specific targeted actions to confuse an actual or potential adversary as regards our true intentions or capabilities, and to obtain an advantageous reaction from the 'action target' that would be practically unattainable by open means."[38] Fully capturing the design of such deception and disorder is a challenge.

Secondly, Pacepa offered useful imagery for understanding the importance of the quantitative element of these actions. He referenced a document from the head of the Soviet bloc espionage community which vividly expressed a valuable insight about *dezinformatsiya*: "a drop makes a hole in a stone not by force, but by constant dripping."[39] What we will find in the subsequent sections is that ICTs and social media platforms now afford an incessant delivery of drops that are individually crafted to leave a mark more quickly.

III. Information Warfare: A New Breadth for *Disinfo-Ops*

Information has long been considered by political decision makers as a powerful weapon to advance the interests of the state, complementary to traditional warfare approaches. This strategy is not new. Homer already described the crucial influence of poets on the mobilization of the Greeks in the war against Troy.[40] As seen previously, Russia has traditionally held this expansive view as well. More recently in 2012, President Putin and Maj. Gen. Sergei Kuralenko—then Chief of Military Art at the Academy of the General Staff—interpreted information technology as a new means for the military.[41] They argued that "the development of information technologies has caused significant changes in the ways wars are fought and led to a build-up of cyber-troops."[42]

Cyber power involves a wide range of instruments, strategies, and capacities; it is "the ability, in peace, crisis, and war to exert prompt and sustained influence in and from cyberspace."[43] It encompasses the potential impacts of strategies in cyberspace, but also in the kinetic world.[44] In other words, cyberspace is at the same time a place where states compete and defend their interests and a toolbox to achieve specific objectives.

[38] Cited in Romerstein, *supra* note 4, at 54. This description echoes the words of U.S. ambassador to Ukraine Geoffrey Pyatt in 2015: "Everyone knows the Kremlin seeks to use information to deny, deceive, and confuse," GILES, *supra* note 5, at 59 (citing Pyatt).

[39] PACEPA & RYCHLAK, *supra* note 2, at 350.

[40] Andrei Aliaksandrau, *Brave New War: The Information War between Russia and Ukraine*, 43 INDEX ON CENSORSHIP 55, 56 (2014).

[41] OSCAR JONSSON, THE RUSSIAN UNDERSTANDING OF WAR: BLURRING THE LINES BETWEEN WAR AND PEACE (2019).

[42] Sergey V. Kuralenko, *Changing Trends in Armed Struggle in the Early 21st Century*, 21 MIL. THOUGHT 29, 29–35 (2012).

[43] John B. Sheldon, *The Rise of Cyberpower*, in STRATEGY IN THE CONTEMPORARY WORLD 306 (John Baylis, James Wirtz, & Colin Gray eds., 2018).

[44] DAMIEN VAN PUYVELDE & AARON F. BRANTLY, CYBERSECURITY: POLITICS, GOVERNANCE AND CONFLICT IN CYBERSPACE (2019).

Moreover, cyber power is often considered a weapon of the weak due to the limited investment it requires to achieve substantial and tangible impact on other states.[45] Analogous to the concept of smart-power strategies developed by Joseph Nye,[46] the intended impacts can serve as a useful analytical division between information-technology and information-persuasion.[47] On the one hand, digital instruments aim to disable information technology systems and critical infrastructure, and provide new means for on-the-ground military operations. On the other hand, persuasion techniques use social media platforms and data-driven marketing tools to influence opinions abroad. This chapter focuses on the latter.

Interstate and intrastate hybrid conflicts place information at the center of defensive and offensive strategies.[48] This change is reflected by the Russian military's understanding of the emergence of a "new generation of warfare" (*voina novogo pokoleniya*), and is well illustrated by the use of information during the Russian military annexation of Crimea.[49] Persuasion techniques allow the operator to send "specially prepared information to incline [a partner or opponent] to voluntarily make the predetermined decision desired by the initiator of the action."[50] To be effective, persuasion first requires a reconnaissance phase to collect data about the targets, whether they are individuals or organizations. Thanks to this first phase of information gathering, the disinformation operators can fully exploit the vulnerabilities of the targeted populations. Data collection allows persuasion techniques not only to identify the best strategy to make their messages heard (i.e., choice of channel and format of communication, time, language, tone of the voice, name of sender) but also to craft their content according to the psychological profiling of targeted individuals or groups of individuals. Whether it is to push for a specific narrative or sow chaos, successful persuasion techniques spread content on multiple platforms and channels of communication simultaneously.

Information is used in situations of conflict today to support traditional kinetic military operations. Some examples include confrontational and contradictory statements by President Putin to give the impression of a dangerously unpredictable leadership, amplifying the narrative of war preparedness and at the same time refuting any troop movement nearby Ukraine right before the conflict.[51] For instance, contradictory information about movements of Russian troops near the eastern border of Ukraine was published before and during the conflict. This effort resulted in buying

[45] Simone Dossi, *Confronting China's Cyberwarfare Capabilities: A "Weapon of the Weak" or a Force Multiplier?*, in U.S. Foreign Policy in a Challenging World 357–377 (Marco Clementi, Matteo Dian, & Barbara Pisciotta, eds., 2018).

[46] Joseph S. Nye Jr., *Get Smart: Combining Hard and Soft Power,* Foreign Aff. 160–163 (July/Aug. 2009).

[47] Emilio J. Iasiello, *Russia's Improved Information Operations: From Georgia to Crimea*, 47 Parameters 51–63 (2017).

[48] Dave Johnson, *Russia's Approach to Conflict: Implications for NATO's Deterrence and Defense*, 111 Research Division NATO 1–12 (2015).

[49] Rod Thornton, *The Changing Nature of Modern Warfare: Responding to Russian Information Warfare*, 160 Rusi J. 40–48 (2015); *see also* Nye, *supra* note 46.

[50] Timothy Thomas, *Russia's Reflexive Control Theory and the Military*, 17 J. Slavic Mil. Stud. 237–256 (2004); *see also* Ido Kilovaty, *Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information*, 9 Harv. Nat. Sec. J. 146–179 (2018).

[51] Mason Richey, *Contemporary Russian Revisionism: Understanding the Kremlin's Hybrid Warfare and the Strategic and Tactical Deployment of Disinformation*, 16 Asia Eur. J. 101–113 (2018).

time in the initial stages of the conflict by thickening the fog of war.[52] This led former NATO Supreme Allied Commander Europe, General Philip Breedlove, to describe Russian's information warfare in Ukraine as "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[53] Russia's specialized tactic further benefits from the relationship between government and broader criminal networks,[54] such as the Russian Business Network[55] and the degree of immunity they enjoy.[56]

The Russian government also supported bloggers and individuals who broadcast pro-Russian narratives on social media networks[57] and sometimes simulate anti-Russian news sources to disseminate false information about the ongoing conflict. Both refuted the presence of the Russian military behind the Ukrainian border and condemned Western media outlets for running broad informational warfare against Russia.[58] The Kremlin thus tried to inflate its military power and legitimize false facts on the ground (e.g., peace or a truce).[59]

The Russian narrative of unpredictable leadership is a key element of Russian's disinformation campaigns, as it feeds the other three objectives: (1) to trigger uncertainty about the real situation on the ground and Russia's intentions; (2) to support dissension within and among other states; and (3) to contribute to the perception of a strong Russia. It does not draw a clear line between war and peace; it conducts information warfare continuously in peacetime and wartime alike.[60] In times of peace (and, more precisely, in the West), Russia's information warfare intends to manipulate the information circulated in Western mass media, alter democratic decision-making processes, influence elites and citizens' consciousness, and foment societal tensions to strengthen its position on the international stage.[61] We saw this expressed previously by Pacepa when describing the Soviet era, and it continues to be the case. For example, one scholar explains, "the informational campaign is an uninterrupted (*bezpriryvnost*) strategic effort. It is waged during 'peacetime' and wartime."[62]

[52] James J. Wirtz, *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy*, in Cyber War In Perspective: Russian Aggression Against Ukraine 29–38 (Kenneth Geers ed., 2015).

[53] John Vandiver, *SACEUR: Allies Must Prepare for Russia "Hybrid War*," Stars & Stripes (2014).

[54] Julie Anderson, *The Chekist Takeover of the Russian State*, 19 Int. J. Intelligence & Counterintelligence 237–288 (2006).

[55] An internet business, based in St. Petersburg, the Network operates as a world hub for sheltering illegal activities, including child pornography, online scams, piracy, and other illicit operations. *See* Brian Krebs, *Shadowy Russian Firm Seen as Conduit for Cybercrime*, Washington Post (Oct. 13, 2007).

[56] Jack A. Jarmon & Pano Yannakogeorgos, The Cyber Threat and Globalization: The Impact on U.S. National and International Security (2018).

[57] Jill Dougherty, *Everyone Lies: The Ukraine Conflict and Russia's Media Transformation*, 88 Harv. Center on Media 1–29 (Discussion Paper Series, 2014).

[58] Sascha Dominik, Dov Bachmann, & Hakan Gunneriusson, *Russia's Hybrid Warfare in the East: The Integral Nature of the Information Sphere*, 16 Geo. J. Int'l Aff. 198 (2015).

[59] Richey, *supra* note 51.

[60] Ulrik Franke, War by Non-Military Means: Understanding Russian Information Warfare (2015).

[61] Puyvelde & Brantly, *supra* note 44.

[62] Adamsky, *supra* note 5, at 29. *See also* Giles, *supra* note 5, at 4 ("it is an ongoing activity regardless of the state of relations with the opponent").

The fact that this activity is continuous regardless of a state of conflict is particularly important from the point of view of international law. Not only does the activity occur below the threshold of armed conflict, it is omnipresent across long spans of time. In this sense, humanitarian law tools used for regulating armed conflict are ill-fitting. It is necessary to look to other legal paradigms to understand the type of damage that can be wrought, along with what sort of regulation could be effective for harnessing the activity.[63]

The concept of "reflexive control" adopted by Russia consists of influencing the opponents' perceptions to make them adopt positions advantageous to Russian objectives.[64] It is not a new concept and was applied in the past against both civilians and military targets. In fact, reflexive control is an information weapon that has "been studied in the Soviet Union and Russia for over 40 years" to persuade the targeted individual or group of individuals to make choices and carry out actions in the interest of the initiator.[65] Reflexive control encompasses a large range of instruments and strategies that are based on the knowledge of how the targeted individuals make their decisions. What differs today is the greater capacity to collect data about the opponent, which allows the initiator of the action to know their target extremely well and consequently make their persuasion more effective.

Thus, while most Western governments focused their attention on Russia's official diplomacy, the country was developing government-to-people diplomacy and its influencing capacity.[66] In Europe, Russia supported far right movements with financial backing and propaganda techniques: France's Rassemblement National, Hungary's Jobbik, Great Britain's UKIP, and the Austrian FPÖ benefited from the Russian helping hand.[67] These parties were quite instrumental for Russia to support efforts to dismantle some of the European Union's agreements and institutions, including the euro area and the Schengen Area.[68] In addition to providing Euroskeptic content, Russia produced and distributed narratives to legitimize its actions, including Crimea's secession referendum and its assistance to Syria's Bashar al-Assad regime to contain rebel groups, which led to widespread criticism for crimes against humanity.[69]

However, the Kremlin also aimed to create political discord. To do so, it generated messages with opposite views. For instance, in Germany, while Angela Merkel was under pressure to step down due to her immigration policy, the Kremlin supported

[63] *See, e.g.*, Barela, *Cross-Border Cyber Ops* and *Zero Shades of Grey*, *supra* note 3; Jens D. Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579 (2017); Sean Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, in CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS (Jens D. Ohlin, Kevin Govern, & Claire Finkelstein eds., 2015); along with the chapters in Parts II and III of this volume exploring various creative options for dealing with a threat that has morphed beyond previously known operations.

[64] Maria Snegovaya, *Putin's information warfare in Ukraine: Soviet Origins of Russia's Hybrid's Warfare*, 1 RUSSIA REPORT 7 (2015).

[65] Thomas Timothy, *Russia's Reflexive Control Theory and the Military*, 17 J. SLAVIC MIL. STUD. 237–256 (2004).

[66] Richey, *supra* note 51.

[67] Frederik Wesslau, *Putin's Friends in Europe*, 19 EUR. COU. FOREIGN REL. (2016).

[68] *Id.*

[69] Andrew Dawson & Martin Innes, *How Russia's Internet Research Agency Built Its Disinformation Campaign*, 90 POL. Q. 245–256 (2019).

both her and far-right movements with hashtags such as "#MerkelMustStay" and "#AfDisshit."[70] Social bots and online disinformation were also found during the 2016 Referendum in the United Kingdom,[71] the 2017 French presidential elections,[72] and the 2017 Catalan referendum.[73] The 2019 European Parliament elections also saw the presence of disinformation efforts in multiple member states, including in Italy[74] and Sweden,[75] where operators ran automated bots to distribute known junk news on Twitter.[76]

The European Union has taken disinformation campaigns seriously and set up an action plan to develop its capabilities and enforce cooperation between EU member states. In the run-up to the 2019 EU elections, it built a fact-checking portal and a database to denounce "partial, distorted, or false depiction of reality and spread of key pro-Kremlin messages."[77] Studies of media reporting and analysis by the East Stratcom Task Force[78] have found that of the 7,572 results of key pro-Kremlin messages, 1,897 involved at least one of the 27 EU member states since the creation of the database;[79] 246 directly targeted the European Union, out of which only 20 mentioned explicitly the EU elections in 2019. Other messages mainly target the United States (1,867) as well as Russia and former USSR countries: Moldova (123), Estonia (138), Latvia (122), Lithuania (173), Kazakhstan (10), Kyrgyzstan, Tajikistan (5), Turkmenistan (1), Uzbekistan (3), Armenia (71), Azerbaijan (29), Georgia (331), and Ukraine (3,063). These numbers illustrate that the current geopolitical struggles with Ukraine sit atop Russia's agenda—it is its main disinformation target. Baltic countries are also of strategic concern for Russia,[80] in particular due to the presence of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.[81]

Disinformation is a challenge the European Union is determined to address. EU Commission Vice President Věra Jourová, in her speech at the Opening of EU vs

[70] *Id.*

[71] Marco T. Bastos & Dan Mercea, *The Brexit Botnet and User-Generated Hyperpartisan News*, 37 Soc. Sci. Com. Rev. 38–54 (2019).

[72] Emilio Ferrara, *Disinformation and Social Bot Operations in the Run Up to the 2017 French Presidential Election*, 22 First Monday (2017).

[73] Massimo Stella, Emilio Ferrara, & Manlio De Domenico, *Bots Increase Exposure to Negative and Inflammatory Content in Online Social Systems*, 115 PNAS 12435–12440 (2018); Javier Lesaca, *Los Zombis De La Desinformación*, El País (Nov. 11, 2017); Javier Lesaca, *Why Did Russian Social Media Swarm the Digital Conversation about Catalan Independence?*, Washington Post (Nov. 22, 2017).

[74] Francesco Pierri, Alessandro Artoni, & Stefano Ceri, *Investigating Italian Disinformation Spreading on Twitter in the Context of 2019 European Elections*, 15 PLoS One 1–23 (2020).

[75] Freja Hedman et al., *News and Political Information Consumption in Sweden: Mapping the 2018 Swedish General Election on Twitter* (Oxford University, Project on Computational Propaganda, Sept. 6, 2018).

[76] Johan Fernquist, Liza Kaati, & Ralph Schroeder, *Political Bots and the Swedish General Election*, IEEE ISI 124–129 (2018).

[77] *See* EU vs Disinfo Database, *available at* <https://euvsdisinfo.eu>.

[78] *Id.*

[79] Specifically, these are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Croatia, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Poland, Portugal, Romania, Spain, Sweden, and The Netherlands.

[80] Mark Galeotti, *The Baltic States as Targets and Levers: The Role of the Region in Russian Strategy*, 28 Sec. Ins. (2019); *see also* Greg Simons, *Perception of Russia's soft power and influence in the Baltic States*, 41 Pub. Rel. Rev. 1–13 (2014).

[81] The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defense expertise. *See* <https://ccdcoe.org>.

Disinfo Conference, underscored disinformation's threat to democracy: "There are specific external actors—namely Russia, and increasingly China—that are actively using disinformation and related interference tactics to undermine European democracy, and will continue doing so until we demonstrate that we will not tolerate this aggression and interference."[82]

As discussed, persuasion and deception strategies are not new. What makes disinformation campaigns today more effective is the new man-made environment in which they evolve. *Disinfo-ops* are part of an information warfare that is simultaneously broader and more pervasive than before, and yet more individualized and hidden underneath a continuous flow of communications and an opaque curtain of anonymity. It is a challenge for Western liberal democracies to develop effective measures to counter such actions and to protect democratic processes.

IV. Computational Politics: A New Depth and Precision of *Disinfo-Ops* during Elections

Data is at the heart of today's political campaign strategies. The analysis of big data allows political strategists to make their argument more convincing and visible to specific groups of the population. The data sets and the techniques to collect data, track individuals, and target these persons can be employed by various domestic and foreign actors to pursue legitimate and nonlegitimate objectives—including electoral interference, as illustrated by the recent Cambridge Analytica scandal.[83] In other words, big data provides both new tools and new targets for *disinfo-ops*.

This data-centered approach to political communication stems from the marketing and advertising industries, where data has become a treasurable commodity to target potential buyers more efficiently and effectively. Thanks to data, combining credit card information, personal interests, consumption patterns, and TV-viewing patterns (among other sources), ad buyers identify and reach the people most likely to react to their messages—as narrow a target as 20 of the 1.5 billion daily users of a social network.[84]

Since users are asked to sign in with their real name and identity, social media platforms allow tech companies to permanently identify users. This identity-based targeting paradigm takes even more prominence when coupled with cross-device recognition capacity, including TV, websites, social media platforms, and mobile phones.[85] In turn, large data sets allow political communication strategists to gain unprecedented access to the mind and soul of potential voters and consequently base their contact decisions on individually microtargeted propensity scores.[86] Political

[82] Věra Jourová, *Disinfo Horizon: Responding to Future Threats* (Conference Opening Speech, Jan. 30, 2020), *available at* <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_160>.

[83] Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, The Guardian (London) (Mar. 17, 2018).

[84] Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, 2014 Wis. L. Rev. 861 (2014).

[85] Jeff Chester & Kathryn Montgomery, *The Role of Digital Marketing in Political Campaigns*, 6 Int. Pol. Rev. 1 (2017).

[86] The term "microtargeting" is sometimes used to refer any individual-level contact performed by campaigns and sometimes refers to the data-generated propensity scores used to guide individual-level contact

parties apply computational methods to large data sets, not only to persuade and mobilize potential voters[87] but also to score, rate, and categorize citizens according to behavioral, demographic, and psychographic data.[88] In this context, psychographics means qualifying consumers according to psychological attributes such as personality, values, opinions, and attitude.[89]

Behavioral tracking is mainly based on cookies (small computational identifiers) to explore the digital trail users leave while visiting websites and social media platforms. It then associates them with data collected from other sources, including those offline.[90] That is, data onboarding describes the techniques to transfer offline data to an online environment for marketing needs.[91] They allow connection of offline customer records with online users by matching identifying information to retrieve the same customers.[92]

This unquenchable thirst for data results in a disaggregation of personal data into a myriad of publicly and privately owned databases scattered throughout the world. The data is collected from internet and mobile service providers, social media and web platforms, governmental and intelligence agencies, advertising companies, and data brokers. It is made possible by the widespread adoption of connected devices, such as smartphones and more recently the internet of things,[93] growing high-speed internet access, and the vast deployment of data centers, which allow affordable and reliable cloud-based services.[94]

This disaggregation of personal data and the large variety of sources for it makes data not only treasurable but also highly vulnerable to cyberattacks and cybercrimes—which have also become a part of hybrid war strategies.[95] Data scattered throughout the planet provides an unprecedented level of transparency into the lives, interests, and emotions of billions of citizens. The large data leaks that regularly make the news headlines illustrate how vibrant the illegal data trade has become.

decisions. In this chapter, we refer to the latter. *See* Kyle Endres & Kristin J. Kelly, *Does Microtargeting Matter? Campaign Contact Strategies and Young Voters*, 28 J. Elec. Pub. Opin. & Part. 1–18 (2018).

[87] Zeynep Tufekci, *Engineering the Public: Big Data, Surveillance and Computational Politics*, 19 First Monday (2014).

[88] Chester & Montgomery, *supra* note 85.

[89] Tufekci, *supra* note 87.

[90] Avi Goldfarb & Catherine E. Tucker, *Online Advertising, Behavioral Targeting, and Privacy*, 54 Communications of ACM 25–27 (2011).

[91] Gil Vernik et al., *Data on-Boarding in Federated Storage Clouds*, 6 Int. Conf. IEEE (2013).

[92] Santiago Gallino & Antonio Moreno, *Integration of Online and Offline Channels in Retail: The Impact of Sharing Reliable Inventory Availability Information*, 60 Mgmt. Sci. 1434–1451 (2014).

[93] The "internet of things" describes the increasing number of objects of everyday life with the capacity to communicate with one another and with their users, becoming an integral part of the internet. *See* Luigi Atzori, Antonio Iera, & Giacomo Morabito, *The Internet of Things: A Survey*, 54 Comp. Networks 2787–2805 (2010).

[94] Jiyi Wu et al., *Cloud Storage as the Infrastructure of Cloud Computing*, Int. Conf. Intel. Comp. and Cog. 380–383 (2010).

[95] Bettina Renz, *Russia and "Hybrid Warfare*," 22 Cont. Pol. 283–300 (2016); *see also* Aurel Sari, *Legal Resilience in an Era of Gray Zone Conflicts and Hybrid Threats* (Exeter Centre for International Law, Working Paper Series 2019/1); Hybrid Threats in the Grey Zone: Mapping the Terrain (Milton Regan & Aurel Sari eds., forthcoming 2021).

Thanks to the vast troves of data collected, marketers and disinformation campaign operators can follow an individual through their media and online usage and adapt the content of dynamic ads according to contextual factors such as time, location, and environment. This easily accessible personal data is the foundation of twenty-first-century persuasion techniques as it allows for more efficient and effective advertising placement and targeting. To make ads more accurate in real time, a recent marketing instrument provides an algorithm with the capacity to constantly buy and place ads with what are known as programmatic advertising platforms.[96] These are based on the analysis of big data in real time[97] and ensure that each ad precisely reflects the specific interests of a citizen anytime they are connected.[98] But their use is not neutral. This marketing innovation has had a significant impact on the media ecosystem and the incentives to produce news, content, and ads,[99] including the production of false information.[100]

Disinformation campaigns benefit from the most recent technological and marketing innovations developed by Western companies. They offer a platform for domestic, but also foreign, actors to widely and precisely micro-target citizens without much accountability. Facebook allows the creation and publication of micro-targeting ads, based on demographics and lifestyle interests, but also nonpublic "dark posts," which only show to the potential voter they are trying to influence—and then disappear.[101] This functionality makes disinformation campaigns almost impossible to track.[102]

Facebook and Google offer tailor-made products and services to political campaign leaders: they have political marketing teams aligned with each major political party to provide assistance and advice on targeting strategies.[103] By making the purchase of advertising automatic, advertisers and large web and social media platforms have enabled nefarious actors—adversarial foreign governments and criminal organizations—to distribute an unprecedented amount of false information. These marketing tools and advertising services have indeed granted visibility to the Kremlin's disinformation campaigns. Yet the same dynamic ads can be funded by a large array of actors without public scrutiny or any sort of accountability.

The distribution of such a large amount of false news is possible thanks to the generalized use of social media platforms in the world today. These platforms allow not only individual users and organizations to interact with each and publish new content, but they also enable *disinfo-ops* to spread rapidly. Thanks to the large data sets

[96] Joshua A. Braun & Jessica L. Eklund, *Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes, and the Business of Journalism*, 7 Dig. Jour. 1–21 (2019).

[97] Pedro Palos-Sanchez, Jose Ramon Saura, & Felix Martin-Velicia, *A Study of the Effects of Programmatic Advertising on Users' Concerns about Privacy over Time*, 96 J. Bus. Res. 61–72 (2019).

[98] Yi-Ting Huang, *The Female Gaze: Content Composition and Slot Position in Personalized Banner Ads, and How They Influence Visual Attention in Online Shoppers*, 82 Comp. Hum. Behav. 1–15 (2018).

[99] Lucia Moses, *The Underbelly of the Internet*, Digiday (2016).

[100] Julian Thomas, *Programming, Filtering, Adblocking: Advertising and Media Automation*, 166 Media. Intl. Aus. 34–43 (2018).

[101] Jessica Baldwin-Philippi, *The Myths of Data-Driven Campaigning*, 34 Pol. Com. 627–633 (2017).

[102] Cadwalladr & Graham-Harrison, *supra* note 83.

[103] Jason J. Jones et al., *Social Influence and Political Mobilization: Further Evidence from a Randomized Experiment in the 2012 US Presidential Election*, 12 PLoS One (2017). For a systematic literature review of computational politics, *see also* Ehsan ul Haq et al., *A Survey on Computational Politics*, IEEE ACC (2019).

collected through these platforms, and the precise tracking and targeting they afford, social media platforms are instrumental to disinformation operators. Disinformation campaigns on social media platforms use three main instruments: (1) spreading false news through a large number of bots—handles or accounts that automate content distribution;[104] (2) paid, organized, and supervised trolls—individuals who falsify their true identities to promote discord;[105] and (3) the use of cyborgs—accounts managed by individuals but sometimes taken over by bots or that present bot-like or malicious behavior.[106]

Combined, these techniques aim to deceive populations and decision makers by artificially supporting what seems like a trend, a consensus, a hashtag, a public figure, a piece of news, or a view of the truth. In the area of public health, for instance, Russian trolls and bots promote simultaneously pro- and anti-vaccination content to contribute to political discord.[107]

Citizens are quite vulnerable on social media platforms when it comes to detecting and fighting against false information. They rarely have the skills or time to verify the source of dubious information. Moreover, the design of social media platforms and applications make this verification harder, flooding users with a constant feed of new information, triggering what has been called a fantasy of abundance.[108] Geolocalization targeting allows an advertiser to follow citizens not only anytime but also anywhere, whether they are driving a car, shopping at a store, or relaxing at home.[109] Yet if false content travels faster than true stories, it is not only because of bots but because of humans,[110] who are more attracted by sensational content, even when untrue.[111]

Russia's former Internet Research Agency (IRA) is now recognized for its attempts to influence the outcome of numerous recent political elections in Western countries through Facebook, Twitter, Instagram, YouTube, and stand-alone websites.[112] Their use of bots to influence discourse and sentiment online is also well documented.[113] The efforts of the IRA to set the political agenda abroad were done systematically and through the use of instruments to influence mass audiences. For instance, when examining the IRA's use of Twitter, researchers have identified five categories of

[104] Zi Chu et al., *Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg?*, 9 IEEE Transc. Depen. Secure Comp. 811–824 (2012).

[105] *Troll*, Collins English Dictionary, *available at* <https://www.collinsdictionary.com/dictionary/english/troll>.

[106] Chu et al., *supra* note 104.

[107] David A. Broniatowski et al., *Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate*, 108 Am. J. Pub. Health 1378–1384 (2018).

[108] Jodi Dean, Publicity's Secret: How Technoculture Capitalizes on Democracy (2002).

[109] Son Sooel, Daehyeok Kim, & Shmatikov Vitaly, *What Mobile Ads Know About Mobile Users*, Conf. NDSS (2016).

[110] Soroush Vosoughi, Deb Roy, & Sinan Aral, *The Spread of True and False News Online*, 359 Science 1146–1151 (2018).

[111] Vincent F. Hendricks & Mads Vestergaard, Reality Lost: Markets of Attention, Misinformation and Manipulation (2018).

[112] This new context may lead to a postfactual democracy, where facts have lost their value and truth is relative: "A democracy is in a post-factual state when politically opportune but factually misleading narratives form the basis for political debate, decision, and legislation." Yavor Raychev, *Cyberwar in Russian and US Military-Political Thought: A Comparative View*, 43 ISIJ 349–361 (2019).

[113] Dawson & Innes, *supra* note 69.

trolls: Right Troll, Left Troll, News Feed, Hashtag Gamer, and Fearmonger.[114] (These five categories are not unique to the IRA and correspond to the strategies described previously to sow chaos and generate an environment of opacity.) The first category of messages did not address traditionally right-leaning topics, such as taxes and abortion, but rather distributed contentious content about moderate Republicans. The second category mainly sent out messages about cultural identities, including gender, sexual, religious, and racial identity. The third category presented itself as coming from local news agencies, while the fourth focused on playing hashtag games. The last category sent out pure fake news, fabricating crises such as nonexistent outbreaks of Ebola in Atlanta, nuclear plant accidents, and war crimes perpetrated in Ukraine.[115]

This last category of trolls specifically, in addition to the other content generated, contributes to a constant flow of information, which challenges users and fact-checkers to pinpoint a specific fact or argument, find the source of a piece of news, or simply reread a publication. The existence of this constant flow of information produces a permanent "noise" that makes it impossible to distinguish a specific voice. As some scholars have recently pointed out, "[d]isinformation campaigns thereby overwhelms the 'signal' of actual news with 'noise, eroding the trust in news necessary for democracy to work."[116] This method of bombarding voters with information has also been adopted by domestic campaigns. Journalists immersing themselves in election cyber activities have found the very same tactic present (in this case for the Trump campaign):

> What I was seeing was a strategy that has been deployed by illiberal political leaders around the world. Rather than shutting down dissenting voices, these leaders have learned to harness the democratizing power of social media for their own purposes—jamming the signals, sowing confusion. They no longer need to silence the dissident shouting in the streets; they can use a megaphone to drown him out. Scholars have a name for this: censorship through noise.[117]

The IRA was a highly professional news agency with staff dedicated to specific regions and countries and specialized for each social media platform.[118] They were in charge of producing memes, posting about fifty comments on news articles daily, running several fake accounts, maintaining six Facebook pages, and tweeting at least fifty times daily[119] and were tasked to include five specific keywords in all posts to encourage search engine pickup.[120] Staff would play opposing roles: on the one hand

[114] Darren L. Linvill & Patrick L. Warren, *Troll Factories: Manufacturing Specialized Disinformation on Twitter*, POL. COM. 1–21 (2020).

[115] *Id.*

[116] Karen Kornbluh & Ellen P. Goodman, *Safeguarding Digital Democracy. Digital Innovation and Democracy Initiative Roadmap*, DIDI ROAD 4 (2020).

[117] C. McKay, *The Billion-Dollar Disinformation Campaign to Reelect the President*, THE ATLANTIC (Mar. 2020).

[118] *One Professional Russian Troll Tells All* (Radio Free Europe broadcast, Mar. 25, 2015), *available at* <https://www.rferl.org/a/how-to-guide-russian-trolling-trolls/26919999.html>.

[119] *Russia Has a Troll Army That Is Trying to Mold Public Opinion on Internet News Sites*, HIGHER LEARNING (June 4, 2014), *at* <http://thehigherlearning.com/2014/06/04/russia-has-a-troll-army-that-is-trying-to-mold-public-opinion-on-internet-news-sites>.

[120] *Russian Troll Tells All*, *supra* note 118.

condemning the authorities, and on the other supporting them. They might post an image or a meme to defend one view, and another adding a link to contradict and fuel political discord.[121] Sometimes, to increase the visibility of a newly created Twitter handle, the IRA bought false followers, which provided more traction to the content they then published.[122] Another technique used by the IRA was to engage in follower phishing. This consists of following hundreds or thousands of new accounts, expecting them to reciprocate, and then unfollowing them in order to increase the "followers per followed" ratio and augment the account's "authority" for platform algorithms.[123] Lastly, the IRA engaged in switching narratives, meaning that a false account would change its narrative after some time, either to create confusion or to identify potential individuals for a later disinformation campaign.[124]

When we consider the size of the "disinformation machinery" during the Cold War described previously, the exponentially amplified breadth, depth, and precision of such operations take on a whole new meaning in today's online world. The use of such interference in the last U.S. presidential election was a game changer.

V. The 2016 U.S. Election and Beyond

To get a handle on how such activities unfold, it is extremely useful to provide a more recent example. We know that in 2016, hackers working for units within the Russian military intelligence (GRU) attempted to hack into email accounts, sometimes with success, belonging to the Democratic National Committee (DNC), the Democratic Congressional Campaign Committee, Hillary Clinton Campaign Chair John Podesta, other staff members, and Hillary Clinton's private email server.[125] This first part of the military operation exfiltrated massive amounts of data. But why?

This was not a traditional act of espionage aiming to learn about the enemy. As Pacepa explained, the first part of a durable disinformation campaign is to "collect as much information as possible on the target."[126] For an operation to contain the essential "kernel of truth," the most stable *disinfo-op* is built on incontestable internal documents. Hence, we subsequently saw a steady release of this cache at strategic moments during the campaign; it was timed to be most damaging to Hillary Clinton's candidacy and in turn aid Donald Trump.[127]

Intelligence reports have been publicly released to verify the foreign actions and warn the general population,[128] indictments have been filed against Russian persons

[121] *Trolling for Putin: Russia's Information War Explained*, YAHOO! (Apr. 5, 2015).

[122] *Russian Troll Tells All*, *supra* note 118.

[123] *Id.*

[124] *Id.*

[125] ROBERT S. MUELLER III, U.S. DEP'T OF JUSTICE, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION, VOL. 1, at 36–40 (2019).

[126] PACEPA & RYCHLAK, *supra* note 2, at 84.

[127] MUELLER, *supra* note 125, at 41–48. For the first public identification of this operation, *see* MALCOLM NANCE, THE PLOT TO HACK AMERICA: HOW PUTIN'S CYBERSPIES AND WIKILEAKS TRIED TO STEAL THE 2016 ELECTION (2016).

[128] OFFICE OF DIR. OF NAT'L INTELLIGENCE, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT U.S. ELECTIONS (Jan. 6, 2017).

and organizations,[129] the U.S. Senate Intelligence Committee has commissioned[130] and issued reports,[131] and Special Counsel Robert Mueller has filed an extensive report of his own detailing the activities.[132] Our intention is to build on this broader work and offer some detail and nuance by presenting one small piece of disinformation caught making its way through the information ecosystem after the election. In doing so the objective is to give further shape and form to twenty-first-century disinformation to better understand its nature.

It should not be a surprise that the information exfiltrated from the DNC continued to make its way through the U.S. courts and media landscape even after the election, and has at times been amplified, targeted, and distorted to sow discord within the population. It has been reported that the United States used its military to interrupt outside interference on the day of the 2018 midterm elections,[133] and the head of the Federal Bureau of Investigation (FBI) has warned that malign foreign influence campaigns on social media platforms have "continued virtually unabated and just intensifies during the election cycles."[134]

Of particular importance to this volume, our example is an article that strikes at the legitimacy of the election process—in this case the Democratic primaries to select the party's candidate. It must not be overlooked that free and fair elections serve the essential role of conferring legitimacy upon an authority in a democracy; targeting the process that elevates the leader of a government can inflict genuine damage, even if it is more abstract in nature.[135] These concerns were clearly outlined by the Obama administration before leaving office: "Russia's cyber activities were intended to influence the election, *erode faith* in U.S. democratic institutions, *sow doubt* about the integrity of our electoral process, and *undermine confidence* in the institutions of the U.S. government."[136] As three of these goals are of this exact character, the fact that Russian

[129] (Mueller) Indictment, United States v. Internet Research Agency et al., No. 1:18-cr-32-DLF, 2018 WL 914777 (D.D.C. Feb. 16, 2018); U.S. v. Viktor Borisovich Netyksho, et al., No. 1:18-cr-215-ABJ (D.D.C. July 13, 2018); U.S. v. Elena Alekseevna Khusyaynova, No. 1:18-MJ-464 (East. Dist. VA Sept. 28, 2018).

[130] R. DiResta et al., *The Tactics and Tropes of the Internet Research Agency* (New Knowledge, Columbia University, Tow Center for Digital Journalism, and Canfield Research LLC, 2018); P. Howard et al., *The IRA, Social Media and Political Polarization in the United States, 2012–2018* (Oxford University, Computational Propaganda Research and Graphika, 2018).

[131] 1 United States Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Russian Efforts Against Election Infrastructure, 116th Congress, 1st Sess., Report 116-XX; 2 United States Select Committee on Intelligence, United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Russia's Use of Social Media with Additional Views, 116th Congress, 1st Sess., Report 116-XX.

[132] Mueller, *supra* note 125.

[133] Ellen Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, Washington Post (Feb. 26, 2019).

[134] U.S. Federal Bureau of Investigation (FBI) Director Christopher Wray Interview with Susan Hennessey, *FBI Director Wray on Combating Cyberthreats*, RSA Conference Lawfare Podcasts (Mar. 6, 2019), *at* <https://www.lawfareblog.com/lawfare-podcast-shorts-fbi-director-wray-combating-cyberthreats>.

[135] For a conceptualization of "legitimacy as a target," *see* S.J. Barela, International Law, New Diplomacy and Counterterrorism: An Interdisciplinary Study of Legitimacy (2014); for identification of the Russian operation in the U.S. 2016 presidential election as targeting legitimacy, *see* Barela, *Cross-Border Cyber Ops*, *supra* note 3.

[136] The White House, Office of the Press Secretary, Fact Sheet: *Actions in Response to Russian Malicious Cyber Activity and Harassment* (Dec. 29, 2016) (emphasis added).

bots and trolls were seen amplifying distorted stories about the validity of the election process can be understood as a continued effort to erode faith in the democratic process and the legitimacy of the leaders who emerge from it.

A. Spreading Confusion at the 2016 DNC Convention

The first discernable victim of the Russian campaign in 2016 came when the former DNC chairperson, Debbie Wasserman Schultz, was forced to announce her intention to step down after the national convention. In the days just before the event, WikiLeaks had posted material online that was pilfered from the DNC by the Russians: emails, spreadsheets, donor information, possible vulnerabilities, rebuttals, opposition research, and other documents.[137] Most pertinent at that moment was the fact that these documents revealed some bias by Wasserman Shultz and others in the DNC during the primary elections in favor of presidential candidate Hillary Clinton over Bernie Sanders.[138]

Regardless of the veracity or inaccuracy of the claim that the DNC was biased, Robert Mueller confirmed the release of the material was purposefully timed to impede the intentions behind a party convention—to consolidate support for the nominee and build momentum toward the general election.[139] Additional evidence of how this Russian operation was pushed into the mainstream media conversations is found by looking at candidate Donald Trump's Twitter handle. On the day after the release he tweeted:

> Leaked emails of DNC show plans to destroy Bernie Sanders. Mock his heritage and much more. On-line from Wikileakes [*sic*] really vicious. RIGGED![140]

Of course, the final word in all caps echoes the intention to erode the legitimacy of a leader by raising doubts about the system that brought this person to their position. Yet this cyberattack using the weaponization of exfiltrated information did not end with the election. For our purposes, the same stolen material from the DNC, and the very same wedge within the Democratic electorate, continued to be exploited in the time that followed.

[137] Thomas Rid, *How Russia Pulled Off the Biggest Election Hack in U.S. History*, Esquire (Oct 20, 2016).

[138] It is not within the scope of this chapter to deeply analyze the disseminated stolen material and the validity of claiming such a predisposition by the DNC. What is relevant here is the fact that the stolen material was organized by the hackers to draw specific attention to any and all inappropriate communication within the DNC—stolen for this precise purpose. Nonetheless, it is worth noting here that some have contended that the contest was never close. One well-respected statistician on the left, Nate Silver, concluded after looking at the numbers and giving due regard to all that Bernie Sanders had achieved: "My view is that the race wasn't really all that close and that Sanders never really had that much of a chance at winning." Nate Silver, *Was The Democratic Primary a Close Call or a Landslide?*, FiveThirtyEight (July 27, 2016).

[139] Mueller, *supra* note 125, at 36 ("The release of the documents was designed and timed to interfere with the 2016 U.S. presidential election and undermine the Clinton Campaign").

[140] Kathleen Hall Jamieson, Cyber-War: How Russian Hackers and Trolls Helped Elect a President 111 (2018).

B. Disinfo Dismissed in Court

A class action lawsuit was filed in federal district court in southern Florida, and announced via YouTube,[141] just two weeks after the first disclosure of documents from Guccifer 2.0 in June 2016 (even before they became widely reported on by the press with the WikiLeaks release in July). The case was brought on behalf of all people who had donated to the DNC, those who contributed to the Sanders campaign, and all registered members of the Democratic Party, claiming that Debbie Wasserman Shultz and the party establishment were "in cahoots with the Clinton campaign and sought to tip the scales in her favor in the Democratic primaries."[142]

While there is certainly reason to believe that this was a genuine grassroots effort, it was entirely built on the cyber-poached documents from a Russian operation. As one expert explained in testimony before the U.S. Congress: "Cold War disinformation was artisanal; today it is outsourced, at least in part—outsourced to the victim itself."[143] Of course, there are many genuine and committed supporters of Bernie Sanders and it is unfair to suggest they are acting in concert with Russia here. However, it has also been pointed out that in the disinformation game, there is not only the operator and the adversary, but also the "*unwitting agent* … who is unaware of his true role and is exploited by the operator as a means of attacking the adversary."[144] It is also worth noting that much more pejorative language has been employed to describe those who assist in a disinformation operation without being aware of their role: "useful idiots," a terminology that plays right into the aim of sowing division.[145] Yet considering the swift dismissal of the court case, it might very well be the case here.

A summary judgment for a final order of dismissal of the case was handed down on August 25, 2017. The presiding judge decided that a trial was unnecessary because the court lacked jurisdiction and the plaintiffs did not have standing to assert each of the causes of action. Reasonable reporting, or even sharp critique, would focus on these two questions since they are the crux of the legal issues at stake.

1. A Shard of *Dezinformatsiya*

Only hours after the dismissal was handed down in Florida, an article was posted at the *Observer* entitled, "Court Admits DNC and Debbie Wasserman Schulz [*sic*] Rigged Primaries Against Sanders."[146] This particular media outlet covered the case

[141] Jared H. Beck, Esq., *We Fight Back: Nationwide Class-Action filed Against Democratic Party and Debbie Wasserman Schultz*, YouTube (June 28, 2016), *available at* <https://www.youtube.com/watch?v=hU4I6C-9JZw>.

[142] Wildling, et al., v. DNC Services Corp., DNC and D. Wasserman Schultz, No. 16-61511-CIV-ZLOCH (Aug. 25, 2017) 1 (U.S. D.C. of S. Dist. Fla.).

[143] *Disinformation: A Primer in Russian Active Measures and Influence Campaigns*, Hearing before the Select Committee on Intelligence, U.S. Senate, 115th Congress, S. Hrg. 115–40, Pt. 1 (Mar. 30, 2017) (Statement of Thomas Rid).

[144] Bittman, *supra* note 7, at 50.

[145] Darczewska & Żochowski, *supra* note 6, at 15; Renée DiResta & Shelby Grossman, Potemkin Pages & Personas: Assessing GRU Online Operations, 2014–2019, at 6 (Stanford Internet Observatory, Cyber Policy Center, 2019); Alina Polyakova, *Why Europe Is Right to Fear Putin's Useful Idiots*, Foreign Pol'y (Feb. 23, 2016); Dalibor Rohac, *Cranks, Trolls, and Useful Idiots*, Foreign Pol'y (Mar. 12, 2015).

[146] Michael Sainato, *Court Admits DNC and Debbie Wasserman Schulz [sic] Rigged Primaries Against Sanders*, Observer (Aug. 26, 2017).

at its filing[147] and stayed on top of the story as it progressed through the court.[148] In fact, the small media outlet released a piece only two days after the disorderly cache of material was first dumped on June 15, 2016.[149] That article claimed in its headline, "Guccifer 2.0 Leak Reveals How DNC Rigged Primaries for Clinton: Hillary Clinton didn't win the Democratic primaries through democratic means."[150] As noted previously, the large national uproar and attention only took place after the more user-friendly WikiLeaks release in July. Yet we can clearly see that each of these articles was pushing the story that the primary was "rigged" from the moment the stolen DNC information was made public.

This early, focused, and sustained attention by the *Observer* newspaper—on what would normally be a small courthouse story on a case that never panned out—makes it worth illuminating the fact that Jared Kushner had owned this outlet up until January 2017.[151] In preparation for Kushner to accept a position to work in the White House as a senior adviser to President Donald Trump, his brother-in-law took over as publisher, and interest in the paper was transferred into a family trust.[152]

Another point worth highlighting is the fact that the title of this article changed over the days that followed its first posting. But even if the headline was shifting, it was always misleading, and any of the versions could be easily shared through social media (Figure 2.1). Each of the topline descriptions of the story insisted that the court had ruled that there was a "rigging" of the primary election:

1. "Court Admits DNC and Debbie Wasserman Schulz [*sic*] *Rigged Primaries* Against Sanders";
2. "Court Concedes DNC and Debbie Wasserman Schulz [*sic*] and DNC *Rigged Primaries* Against Sanders";
3. "Court Concedes DNC Had the Right to *Rig Primaries* Against Sanders".[153]

However, at this stage of the proceedings the judge was obliged to assume as true all of the claims put forward by the plaintiff. The judge could only consider the technical matters of pleading and subject matter jurisdiction—requisite hurdles for a full trial. Consequently, the most relevant judicial findings were that "[i]t is readily apparent

[147] Michael Sainato, *Debbie Wasserman Schultz Served Class Action Lawsuit for Rigging Primaries*, Observer (June 30, 2016).

[148] *See* Michael Sainato, *Hearing Set for Class Action Lawsuit Against DNC*, Observer (Apr. 24, 2017); Michael Sainato, *DNC Lawyers Argue DNC Has Right to Pick Candidates in Back Rooms*, Observer (May 1, 2017).

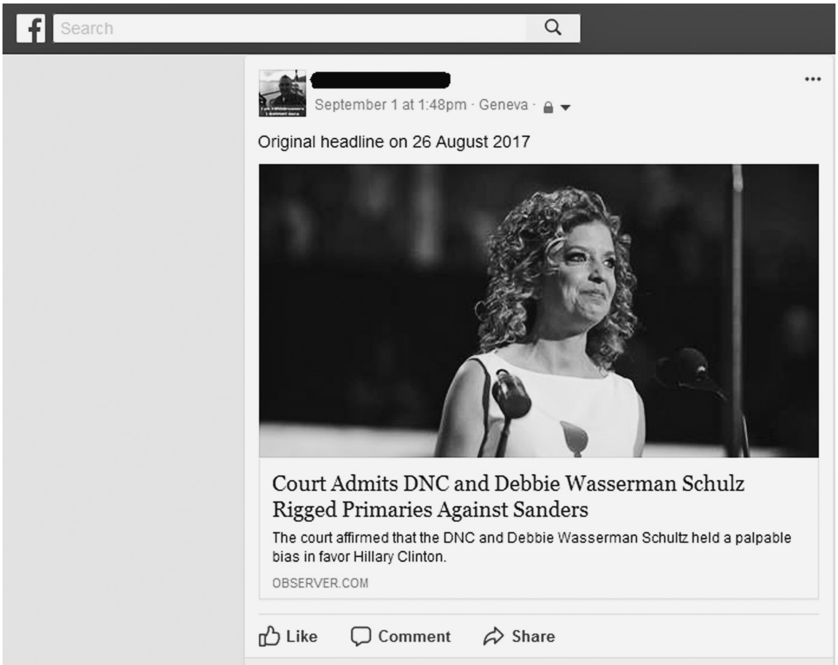
[149] Guccifer 2.0, *Guccifer 2.0 DNC's servers hacked by a lone hacker* (June 15, 2016), *at* <https://guccifer2.wordpress.com/2016/06/15/dnc/>. It is worth noting that the national uproar only took place in July after the more user-friendly WikiLeaks release.

[150] Michael Sainato, *Guccifer 2.0 Leak Reveals How DNC Rigged Primaries for Clinton*, Observer (June 17, 2016).

[151] Dylan Beyers, *Jared Kushner to Transfer Observer Interest to Family Trust*, CNN.com (Jan. 9, 2017).

[152] Nathan McAlone, *Trump Son-In-Law Jared Kushner Will Step Down as Publisher of the Observer, and Have No "Ownership Stake*," Business Insider France (Jan. 10, 2017).

[153] Emphasis added. The first two headlines were captured with a screenshot (the first is pictured in the text *supra*), and the third and final headline is still *available at* <https://observer.com/2017/08/court-admits-dnc-and-debbie-wasserman-schulz-rigged-primaries-against-sanders/>.



[redacted]

September 1 at 1:48pm · Geneva ·

Original headline on 26 August 2017

Court Admits DNC and Debbie Wasserman Schulz Rigged Primaries Against Sanders

The court affirmed that the DNC and Debbie Wasserman Schultz held a palpable bias in favor Hillary Clinton.

OBSERVER.COM

Figure 2.1 Original false and misleading headline moving through social media

that this Court lacks jurisdiction" and that "it is also apparent that Plaintiffs lack standing to assert each of the causes of action raised in this putative class action."[154]

Moreover, the text of the article went through changes as well. The author suggests in the second paragraph of the original version that the summary judgment "reflects a dire state of democracy in this country . . . proving the DNC attorney's claims that the DNC is within their right to rig primaries." Nevertheless, this stark and grim assessment of what the judgment means disappeared in future versions of the article and no longer exists online. The article does later note that at this stage there is an assumption that "a plaintiff's allegation is inherently taken to be true."[155] Yet this point is buried in the article.

We would suggest that an extremely limited number of people would be inclined to do so, but if you follow the link in the article and read the actual judgment from the Florida court, the requirements of the proceedings are made explicitly clear by the judge:

> This Order does not concern who should have been the Democratic Party's candidate for the 2016 presidential election; it does not concern whether the DNC or Wasserman Schultz generally acted unfairly towards Senator Sanders or his

[154] Wildling, et al., v. DNC Services Corp., *supra* note 142, at 11, 12.
[155] Original version on file with authors.

> supporters; indeed, it does not even concern whether the DNC was in fact biased in favor of Hillary Clinton in the Democratic primaries. At this stage, the Court is required to construe the First Amended Complaint in the light most favorable to Plaintiffs and accept its well-pled allegations as true.
>
> [. . .]
>
> This Order therefore concerns only technical matters of pleading and subject-matter jurisdiction. To the extent Plaintiffs wish to air their general grievances with the DNC or its candidate selection process, their redress is through the ballot box, the DNC's internal workings, or their right of free speech—not through the judiciary.[156]

Much of the information in the article is true, so why does this qualify as *dezinformatsiya*? For one, the lawsuit itself was based entirely on the DNC material pinched by Russia.[157] Next, the changing title and content of the article leave the analyst and returning readers grasping for a moving substance that is difficult to fully understand or discuss. (Even if changed over time, the URL still reveals the original title: <https://observer.com/2017/08/court-admits-dnc-and-debbie-wasserman-schulz-rigged-primaries-against-sanders/>.) What is more, as will be discussed further later, it is currently difficult to track and know how far the original headline traveled within targeted communities who would be particularly sensitive to the "proven" accusations—that is, Bernie Sanders supporters who felt disenfranchised.

Perhaps most importantly, we can see that the term "rigged" is consistently tied to the court's judgment in the *Observer* article—along with previous articles on the case. Though this connection is demonstrably false, it is central to the narrative being propagated to erode trust in democracy itself. As for the required "kernel of truth," one expert helpfully tweeted in May 2017: "Historic note: Soviet bloc disinformation operators considered the best fact/forgery mix to be ~90% fact, ~10% fake."[158] The small percentage of falsehood here is the inflammatory allegation that a "rigging" had been proven in court—an accusation that undermines the legitimacy of the electoral system itself.

2. Russian Bots and Trolls

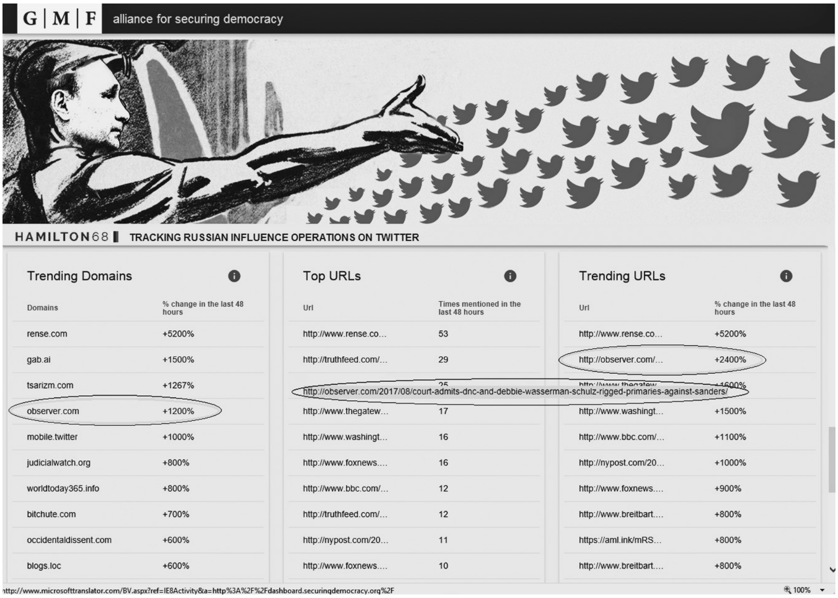
Finally, we can uncover further Russian involvement in this operation. To do so, a useful tool was unveiled in August 2017: the *Hamilton 68 Dashboard*.[159] This website aims to track in real time Russian-aligned propaganda on Twitter. The project was launched by the Alliance for Securing Democracy (ASD) and has involved a

[156] Wildling, et al., v. DNC Services Corp., *supra* note 142, at 8–9.

[157] *Id.* at 4–6 ("The DNC's bias, according to Plaintiffs, came to light after computer hackers penetrated the DNC's computer network. An individual identified as 'Guccifer 2.0' took credit for the hack and posted several documents purportedly taken from the DNC's servers on a publically accessible website. [. . .] As a result of the information 'Guccifer 2.0' released, Plaintiffs conclude that 'the DNC was anything but 'impartial,' 'evenhanded,' or 'neutral' with respect to the Democratic nominating process' ").

[158] Thomas Rid (@RidT), Twitter (May 6, 2017, 4:13 AM), *at* https://twitter.com/ridt/status/860769446083911681?lang=en.

[159] <http://dashboard.securingdemocracy.org/>. The website has now been upgraded to track "the narratives and topics promoted by Russian and Chinese government officials and state-funded media on Twitter, YouTube, state-sponsored news websites, and via official diplomatic statements at the United Nations."



HAMILTON68 TRACKING RUSSIAN INFLUENCE OPERATIONS ON TWITTER

Trending Domains

Domains	% change in the last 48 hours
rense.com	+5200%
gab.ai	+1500%
tsarizm.com	+1267%
observer.com	+1200%
mobile.twitter	+1000%
judicialwatch.org	+800%
worldtoday365.info	+800%
bitchute.com	+700%
occidentaldissent.com	+600%
blogs.loc	+600%

Top URLs

Url	Times mentioned in the last 48 hours
http://www.rense.co...	53
http://truthfeed.com/...	29
[illegible]	25
http://www.thegatew...	17
http://www.washingt...	16
http://www.foxnews....	16
http://www.bbc.com/...	12
http://truthfeed.com/...	12
http://nypost.com/20...	11
http://www.foxnews....	10

http://observer.com/2017/08/court-admits-dnc-and-debbie-wasserman-schulz-rigged-primaries-against-sanders/

Trending URLs

Url	% change in the last 48 hours
http://www.rense.co...	+5200%
http://observer.com/...	+2400%
http://www.thegatew...	+1600%
http://www.washingt...	+1500%
http://www.bbc.com/...	+1100%
http://nypost.com/20...	+1000%
http://www.foxnews....	+900%
http://www.breitbart....	+800%
https://aml.ink/mRS...	+800%
http://www.breitbart....	+800%

http://www.microsofttranslator.com/BV.aspx?ref=IE8Activity&a=http%3A%2F%2Fdashboard.securingdemocracy.org%2F

Figure 2.2 Amplification of the false and misleading material

former FBI special agent, Clint Watts, who is now Distinguished Research Fellow at the Foreign Policy Research Institute and Non-Resident Fellow at the ASD.[160] While the website has received criticism,[161] the preceding analysis indicates why this particular article is worth tracking with this tool to gather whether it was picked up by the accounts being monitored. As the dashboard moves in real time, consulting it now will only display what the bots and trolls are currently doing or have done over the previous forty-eight hours. Therefore, a screenshot taken at 20:00 GMT on August 27, 2016, establishes the amplification of this story by the *Observer* as one of its top URLs mentioned (Figure 2.2).

As can be seen, the specific URL was profiting from a boost supplied by the Russian-aligned bots and trolls the day after it had been published online. In other words, the *Hamilton 68 Dashboard* would suggest that this story was promoted because it includes "news content that supports the story Vladimir Putin wants to tell—a depiction of the West as corrupt, chaotic and collapsing."[162]

[160] *See* Clint Watts, Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News (2018).

[161] Criticism has come for the backgrounds of some of its founders (e.g., Bill Kristol, a neoconservative who hyped the invasion of Iraq in 2003), and for not revealing the accounts it follows (justified at the site out of fear of spooking the account operators and changing behavior: *How to Interpret the Hamilton 68 Dashboard: Key Points and Clarifications*, *at* https://securingdemocracy.gmfus.org/toolbox/how-to-interpret-the-hamilton-68-dashboard-key-points-and-clarifications/). *See* Glenn Greenwald, *With New D.C. Policy Group, Dems Continue to Rehabilitate and Unify with Bush-Era Neocons*, The Intercept (July 17, 2017); M.C. McGrath & Glenn Greenwald, *How Shoddy Reporting and Anti-Russian Propaganda Coerced Ecuador to Silence Julian Assange*, The Intercept (Apr. 20, 2018).

[162] Watts, *supra* note 160.

This appeared to be the peak of activity (relatively high on the site at that time) by these foreign meddlers in the first days of its appearance online. Yet we don't know how far and wide the post was shared and seen beyond this. Nor do we know what increase was gained by this part of the Russian operation as this does not represent the entirety of their social media campaign. Nor do we know how targeted it was to receptive communities. For example, this article was found moving through the newsfeed of one of the authors here who has friends who are Bernie Sanders supporters. What can be said is that the post stimulated comments agreeing with the sentiment of a broken system, and it was shared by others giving the original headline further life.

There are also indications that this story has had influence. When Bernie Sanders suspended his run for president in April 2020 and endorsed Joseph R. Biden Jr. as the Democratic nominee for president, he suggested that it would be "irresponsible" for his loyalists not to support Biden.[163] Days later some enthusiasts were posting virulent objections to Biden as a candidate, voicing the injustice of the primary system, explaining that this was "a world where the DNC argued in court they have the right to cheat"—posting one of the articles from the *Observer* as evidence.[164] Others joined in the exchange also referencing the court decision in Florida. Though this is an anecdote that requires further exploration, it shows that the articles had gained life within the targeted community.

This shard of disinformation reveals several important points. First, we can see how exfiltrated information injected into the media mainstream can spur genuine activists into acting in the interests of Russia as unwitting agents. Second, the subtle manipulation of truth becomes more obvious as we see the real presence of some bias within the DNC becoming a damaging exaggeration of a "rigged" contest—pushing societal divisions and public understandings in ways that benefit Russia. Third, we see how this election interference targets the legitimacy of government and erodes faith in the institutions that are meant to establish governors of society. Finally, it is also a call for greater access to social media data and broader analysis of digital disinformation strategies.

Building off this last point, it should not be missed that we do not have tools for gauging the impact of this story moving through the information ecosystem. That is, not just how many people saw this headline in their newsfeed, but how many commented and helped it travel further by sharing it? And what did readers make of it? Did it influence them? If so, how much? We are certainly not the first to point out this problem:

> In the operations where they are used, it is sometimes difficult to define and determine their effect on the end result of these operations. There is a lack not only of research and tools to measure their effectiveness: in addition, the main limiting factor in the analytical process is the secret nature of the operations.[165]

[163] Joanna Walters & Laura Gambino, *Sanders Warns His Loyalists It Would Be "Irresponsible" Not to Support Biden*, The Guardian (Apr. 15, 2020).

[164] Screenshots of the posts on April 25, 2020, are filed with the authors.

[165] Darczewska & Żochowski, *supra* note 6, at 7. For a veritable effort to make such an assessment with the available social science tools, *see* generally Jamieson, *supra* note 140.

As a consequence, our final section will illuminate the need for fuller access to the empirical data that is now available on social platforms in order to obtain needed answers.

VI. A Clarion Call for Opening Fuller Data Access to Social Scientists

Three essential questions demand full investigation in order to wholly understand disinformation today:

- *Breadth*: How large are these operations?
- *Depth*: How deeply do they penetrate into a foreign society?
- *Precision*: How accurate (individualized) is the targeting for these operations?

Each of these queries should be answerable, in theory. However, social media companies have not allowed unfettered research on their platforms to protect their own trade secrets and the privacy of their users. This means that researchers, journalists, and regulators have not had the required access to provide sufficient answers to these vital questions.

There have been real efforts to study these quantitative research questions. In fact, the studies that have been executed thus far have created pressure on the tech companies to open up their vast troves of data. Initial literature reviews shed a great deal of light on the connection between social media, political polarization, and disinformation.[166] In other words, we are only starting to delineate what is known—and unknown—about this new phenomenon.

Some of the most trailblazing research into the Russian social media operation into the 2016 U.S. presidential election was arguably conducted by Johnathan Albright.[167] He is now the Director of the Digital Forensics Initiative at the Tow Center for Digital Journalism at Columbia University and keen attention on Albright's research into a topic of sudden political importance helped bring about his success in academia.[168] Due to the timeliness of his investigations, a great deal of it has been published online to offer immediate access.[169]

Most pertinent here, Albright's work quickly shattered the myth that Facebook attempted to promulgate when claiming that the Russian Internet Research Agency campaign had reached only 10 million people with 3,000 ads bought on the platform.

[166] Joshua Tucker et al., *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, Hewlett Foundation (2018). This text provides a breakdown of current publications into six categories: (1) online political conversations; (2) the effects of exposure to online disinformation; (3) producers of disinformation; (4) tactics and strategies of dispersing disinformation; (5) political polarization and online content; and (6) polarization, misinformation, and democracy.

[167] Craig Timberg, *Russian Propaganda May Have Been Shared Hundreds of Millions of Times, New Research Says*, WASHINGTON POST (Oct. 5, 2017).

[168] Issie Lapowsky, *Shadow Politics: Meet the Digital Sleuth Exposing Fake News*, WIRED (July 18, 2018).

[169] *See* Albright's online portfolio at MEDIUM.COM, <https://medium.com/@d1gi>, and the research data published to back up these claims at <https://public.tableau.com/profile/d1gi#!/vizhome/FB4/TotalReachbyPage>. His Medium.com page was shortlisted for a Data Journalism Award.

Due to his previous work studying public discourse online, this figure struck him as a vast underestimate. Albright thus set out to extract data and archived content using "CrowdTangle" (Facebook's tool for social analytics) from six of the known IRA pages—Blacktivists, United Muslims of America, Being Patriotic, Heart of Texas, Secured Borders, and LGBT United. Since there were some 470 known Russian accounts, this would represent only a tiny fraction of their overall online content. Yet in analyzing 500 posts for each of these six accounts, Albright found that they had been shared a total of 340 million times and had garnered over 20 million "likes," "shares," and other reactions. When the numbers are extrapolated, this would put the potential number of views for what is currently known about the Russian operation well into the billions.

Disturbingly, the large amounts of data that Albright had scraped during this notable research were quickly removed from the platform just days after his research was published.[170] Which brings us to our final point for this chapter. Namely, there is a large hole in our full understanding of these foreign influence operations today. This gap was aptly summarized for the biggest platform as such in 2017:

> Simply put, without access to Facebook data, understanding of the spread of disinformation through social media will be incomplete. […] a great deal more could be learned about many of the topics contained in this report if a system for sharing Facebook data with scientific researchers could be developed and implemented.[171]

With this in mind, we close our chapter with a call for extensive academic research into social media platforms so that we can wholly comprehend the scale, scope, and accuracy of foreign operations.

In fact, such a program has been launched—though it has only progressed in fits and starts. In April 2018, a partnership was initiated between Facebook and an entity named *Social Science One*. The objective is to offer researchers access to one petabyte of data (1 million gigabytes) from its platform to study "the effect of social media on democracy and elections."[172] The newly created body consists of a commission of senior academics who act as a third party to manage the envisioned industry-academic partnerships.[173] Outside scholars are able to petition data sets for study through research proposals that are evaluated by the commission (which excludes projects that violate privacy, damage a company's market position, or infringe upon other studies). The accepted researchers will receive access to privacy-preserving data and can publish their findings on agreed topics without seeking approval from the participating company.

The emergence of big data today means that while social scientists have access to more data than ever before, this only represents a substantially smaller fraction of what actually exists—resulting in incomplete outcomes that often raise more

[170] Craig Timberg & Elizabeth Dwoskin, *Facebook Takes Down Data and Thousands of Posts, Obscuring Reach of Russian Disinformation*, Washington. Post (Oct. 12, 2017).

[171] Tucker et al., *supra* note 166, at 70.

[172] Social Science One: Building Industry-Academic Partnerships, *Our Facebook Partnership*, *at* <https://socialscience.one/our-facebook-partnership>.

[173] The Institute of Quantitative Social Science at Harvard and the Social Science Research Council are to provide logistical help.

questions than they answer (e.g., Albright's investigation detailed previously). Hence, researchers either publish their research findings with access to only partial data, or sign away academic freedom in nondisclosure agreements by working within a company and relinquishing final control over research and publishing decisions.

In light of what has been elucidated in this chapter concerning the dearth of access and study, we believe *Social Science One* to be a potentially groundbreaking development by creating a model that can be enlarged or replicated elsewhere. Furthermore, it demonstrates the growing understanding that we need to study what is happening on personalized newsfeeds.

Unfortunately, *Social Science One* has proven much more difficult to implement than first envisioned. While the project was unsurprisingly successful in attracting viable and valuable research proposals, getting Facebook to deliver the originally specified data was challenging.[174] The Co-Chairs and European Advisory Committee of *Social Science One* eventually released a bold statement in December 2019 that keenly captures our own concerns:

> In recent years digital platforms have made independent scientific research into potentially consequential phenomena such as online disinformation, polarization, and echo chambers virtually impossible by restricting scholars' access to the platforms' application programming interfaces (APIs). The Social Science One initiative, specifically designed to provide scholars with access to privacy protected data, has made important progress over the last 18 months, but Facebook has still not provided academics with anything approaching adequate data access.
>
> [. . .]
>
> The current situation is untenable. Heated public and political discussions are waged over the role and responsibilities of platforms in today's societies, and yet researchers cannot make fully informed contributions to these discussions. We are mostly left in the dark, lacking appropriate data to assess potential risks and benefits. This is not an acceptable situation for scientific knowledge. It is not an acceptable situation for our societies.[175]

In addition, the authors of this statement called for specific actions: (1) Facebook should make accurate and representative data available for scientific study; (2) all

[174] The problem revolved around Facebook's legal interpretation of the General Data Protection Regulation (GDPR) from the European Union and the consent decree under which it operates with the Federal Trade Commission of the United States. The company took the position that these restrictions inhibit any analysis by researchers of individual level data, even if it is aggregated or de-identified. This legal interpretation was not shared with the co-chairs of Social Science One. *See* Social Science One, *Unprecedented Facebook URLs Dataset Now Available for Academic Research through Social Science One* (Feb. 13, 2020), *at* <https://socialscience.one/blog/unprecedented-facebook-urls-dataset-now-available-research-through-social-science-one>. Reluctance by the social media platform created such a problem that in August 2019 the funders behind the Social Science One program instituted a deadline for Facebook to share the promised data with the researchers or said they would terminate their support. *See* Social Media and Democracy Research Grants, *Statement from Social Science Research Council President Alondra Nelson on the Social Media and Democracy Research Grants Program* (Aug. 27, 2019), *at* <https://www.ssrc.org/fellowships/view/social-media-and-democracy-research-grants/update-from-ssrc-president-alondra-nelson/>.

[175] *PublicstatementfromtheCo-ChairsandEuropeanAdvisoryCommitteeofSocialScienceOne*,Dec.11,2019, *at* <https://socialscience.one/blog/public-statement-european-advisory-committee-social-science-one>.

digital platforms should be required to do the same; (3) Facebook, Google, and Twitter should provide written analysis of any legal barriers that might prevent academic research; (4) European authorities should provide actionable guidance on what can and cannot be shared for research; (5) platforms and public officials should create "research safe harbors" (similar to that used for health and medical data) where scholars can access personally identifiable data with clear and robust limits; and (6) public authorities should help in creating independent verification of platform data since "[e]ven if the researchers and their analyses are considered credible, all findings rest on trust that the platforms have provided complete, accurate data."[176]

The public pressure worked. Two months later Facebook released an unprecedented URLs data set to *Social Science One*.[177] In order to comply with Facebook's interpretation of their legal obligations, an agreement was made to apply "differential privacy" to the data sets in order to prevent reidentification of individuals represented in the data through an introduction of calibrated "noise." This is not the place to delve into whether this adjustment allows full social scientific analysis without jeopardizing privacy,[178] and, in any event, it is far too early to expound upon this development as it broke while we were bringing this chapter to completion. At this point, all that can be said is that this is an enormously welcome development that holds great promise.[179]

VII. Conclusion

In this chapter, we have attempted to flesh out the central components of twenty-first-century *disinfo-ops*. One clear challenge—a holdover from the Soviet era—comes from the elusory nature of the operations themselves. As they are built on factual information with only slight distortions that are often pushed forward by unwitting agents who wholeheartedly believe in their cause, the narratives are extremely difficult to disprove—or even prove that they are part of an external campaign. Furthermore, when a belief has taken hold, demonstrating to someone that an incorrect assessment of the facts has been made largely means asking them to admit they have been improperly influenced or duped.

On top of this, we notably find vastly expanded opportunities to carry out campaigns using information and communication technologies. In the newly available political marketing/disinformation continuum, social media platforms and persuasion techniques play a key role in what has become information warfare. ICTs make persuasion techniques broader, more omnipresent, and yet more difficult to identify when hidden under millions of other messages and behind multiple identities. Moreover, the same large data set and technologies used to collect this data, track individuals, and target them with bespoke content are also used (or rented) as a service, by malevolent actors, including foreign states and criminal groups.

[176] *Id.*

[177] Social Science One, *Unprecedented Facebook URLs, supra* note 174.

[178] *See* Georgina Evans & Gary King, *Statistically Valid Inferences from Differentially Private Data Releases*, *at* <http://j.mp/38NrmRW>.

[179] *Cf.* Kalev Leetaru, *Facebook and Social Science One: The Academics Are Rushing to Mine Our Private Data*, FORBES (May 13, 2019).

These facts give shape to a novel type of interference that is wholly different than anything we have seen before; this calls for rethinking current international legal norms. We are seeing pervasive campaigns, operating below the threshold of armed conflict, that can cause genuine upheaval within a society as citizens vehemently disagree over the basic truths of events. And when elections and politicians running are targeted, the activity breaks down the trust that a people must have in the legitimacy of their leaders and the processes that elevate them to a position of authority.

It is hoped that this descriptive work provides useful information for prescriptive proposals of what ought to be done. It is thus fitting that this chapter appears within a volume that provides various propositions for combating foreign election interference through international law and other means. For our part, we would suggest that one place to start is by classifying such cross-border operations as a violation of the international law principle of nonintervention[180]—which certainly does not preclude the actions from transgressing other rubrics of international law at the very same time. Yet for any of these ideas to become policy, the first order of business must be governments who are ready and willing to confront today's digital *dezinformatsiya*.

We close with a potent analogy made by former Soviet leader and head of the KGB, Yuri Andropov: "[*Dezinformatsiya*] works like cocaine. If you sniff it once or twice, it may not change your life. If you use it every day though, it will make you an addict—a different man."[181] The pushers of this addictive drug have today found a way to inject a relentless flow of individually tailored content directly into the bloodstream of foreign citizens through ubiquitous handheld devices. More study must be done, yet we believe there is already enough to show that *disinfo-ops* represent a significant threat to democracy.

[180] *See* Barela, *Cross-Border Cyber Ops*, *supra* note 3; Barela, *Zero Shades of Grey*, *supra* note 3.

[181] Pacepa & Rychlak, *supra* note 2, at 196 (citing Andropov).