The Journal of Peace and War Studies (JPWS) aims to promote and disseminate high quality research on peace and war throughout the international academic community. It also aims to provide policy makers in the United States and many other countries with in-depth analyses of contemporary issues and policy alternatives. JPWS encompasses a wide range of research topics covering peacekeeping/peacebuilding, interstate reconciliation, transitional justice, international security, human security, cyber security, weapons of mass destruction developments, terrorism, civil wars, religious/ethnic conflicts, and historical/territorial disputes around the world. JPWS is an annual peer-reviewed journal published by the John and Mary Frances Patton Peace and War Center (PAWC) at Norwich University—America’s first private military college and birthplace of the Reserve Officers’ Training Corps (ROTC).

Editor  
Yangmo Ku

Associate Editors  
Steven Sodergren  
Ali Askarov  
Miri Kim  
Michael Thunberg

Assistant Editor  
Vina Hutchinson

Editorial Board  
Kenki Adachi, Ritsumeikan University, Japan  
Felix Berenskoetter, University of London, England  
Scott Crichlow, West Virginia University, USA  
Clarissa Estep, West Virginia University, USA  
Lily Gardner Feldman, Johns Hopkins University, USA  
Lyle Goldstein, Defense Priorities, USA  
Linus Hagström, Swedish Defense University, Sweden  
Youngjun Kim, Korea National Defense University, South Korea  
Travis Morris, Norwich University, USA  
André Simonyi, Royal Military College Saint-Jean, Canada  
Kristina Soukupova, Czech Technical University, Czech Republic  
Lon Strauss, Marine Corps University, USA  
Lasha Tchantouridzé, Norwich University, USA  
Alexis Vahlas, University of Strasbourg, France  
Jindong Yuan, University of Sydney, Australia

The opinions expressed in this journal are those of the contributors and should not be construed as representing those of the John and Mary Frances Patton Peace and War Center, Norwich University or the editors of the Journal of Peace and War Studies.

Copyright © 2022 by the John and Mary Frances Patton Peace and War Center, Norwich University, Printed by Norwich University Press.  
ISSN 2641-841X(Print) • ISSN 2641-8428 (Online)
Not Your Father’s Disinformation: Emerging Technology, Social Media Advances, and the Growth of Smart Disinformation

Mary Manjikian

Abstract: Recent technological advances empower organizations engaged in online disinformation in new and unpredictable ways. Contemporary disinformation techniques share common ground with classic disinformation—in terms of goals, methods, and their role in more extensive subversion campaigns. However, today’s disinformation techniques differ in the volume of information produced, the speed at which it is produced, and the degree of customization that is carried out, as themes are targeted to appeal to specific “customer bases.” In addition, disinformation is adjusted based on the responses received. Comparing the 1980 AIDS disinformation campaign known as Operation Denver and the recent COVID disinformation campaign highlights differences between new and old disinformation strategies and tactics.

Keywords: Emerging technology; disinformation; cyberwarfare; grey zone conflict; hybrid war.

Introduction

Even before the advent of social media, Russia and its intelligence services were highly skilled practitioners of the intelligence tradecraft known as disinformation; Russia carried out active measures or political warfare characterized by disinformation, propaganda, deception, sabotage, destabilization, subversion, and espionage, both in the past and present. Indeed, the definition of disinformation, which appears in the 1972 classified KGB Dictionary, is still just as valid today. In that publication, disinformation data was described as “especially prepared data, used for the creation, in the mind of the enemy, of incorrect or imaginary pictures of reality, on the basis of which the enemy would make decisions beneficial to the Soviet Union.”

But how does today’s disinformation differ from that used in the past? This paper aims to demonstrate how disinformation today is fundamentally different from what has been in the past—mainly due to the changes in communications resulting from emerging technologies. Disinformation has always represented part of a larger strategy of covert intelligence operations aimed at influencing the outcomes of specific events (like elections)—as well as undermining public support for adversary governments. However, current Russian disinformation efforts include a larger number of actors—including public organizations, private institutions, and even organized crime—which are utilized in laundering money and purchasing accounts for the creation of deceptive online identities, including both false persons and automated bots.

In addition, while intelligence service branches have always coordinated with each other to seek common goals—with intelligence collectors, for example, sharing information
about the targets of disinformation campaigns and the likelihood that certain themes might be picked up and amplified by a key audience—this task has been facilitated by the creation of vast troves of open source intelligence, including social media intelligence. Identifying targets and tailoring themes to specific audiences is now easier than ever, since gathering information about audiences no longer requires the same degree of expensive or extensive intelligence collection. For example, analysis by Stephen McCombie et al. of Russian election hacking prior to the 2016 presidential election shows that the use of technologies like geofencing, which allows the targeting of online messaging to specific zip codes and areas, meant that voters in swing states were more likely to be the target of this messaging than those in states where the election was less contested. In this way, disinformation resources are deployed more efficiently, rendering disinformation operations more efficient as well.

In addition, today, troll farms have been enlisted to engage in activities like answering online polls and swaying the results. Posing as legitimate respondents, they can misrepresent public opinion and influence others who might see their opinions or desires reflected in these polls. Here, for example, David Goie points to an online Twitter poll established by a critic of British Prime Minister Theresa May and later analyzed by the Atlantic Council. In this way, current disinformation campaigns can be seen as less static and more interactive than previous campaigns.

Goie, therefore, describes disinformation today as part of a more extensive “suite” of complex active measures—in which states can both amplify key themes through social media engineering as well as engaging in more overtly aggressive activities such as taking down or defacing platforms offering alternate information, seamlessly integrating disinformation into a larger cyberwar agenda. In this way, disinformation today can be seen to exist as both an offensive and a defensive activity.

At the same time, there are more channels available to those wishing to “seed” disinformation themes. These channels include covert methods like the use of chat forums found on the dark web as an initial ground for testing and seeding themes, which will be more widely disseminated later. For this reason, the task of those engaged in “counter subversion” is complicated—it may be harder to find the source or sources of disinformation, and the weaponized information may be more effective at hitting its target and causing a behavioral change.

In addition, one of emerging technology’s critical characteristics is its unpredictability. Therefore, we should ask how technology evolves and how disinformation practices might evolve. The term “affordances” refers to the qualities or properties of an object that define or constrain its possible uses. (For example, solid material is more likely to be used to make tools, while a more flexible or soft material might be used to create other objects that require shaping. A sharp object may be used to stab one’s opponents more efficiently than a liquid object.)
Considering how disinformation practices are carried out, particularly on social media platforms, it becomes clear that today’s information environment contains affordances that empower different actors. In addition, social media today operates at a different speed and makes certain possible types of actions that were not possible in the days of newspapers and printing presses. Disinformation 2.0 is characterized by greater interactivity between the target and the attacker, more transparency for attackers regarding the responses received as a disinformation campaign, and the ability to constantly reshape the environment where interactions occur, refining narratives and segmenting them for different audiences.

This paper considers Operation Denver, a Soviet attempt to sow disinformation in Africa during the 1980s AIDS crisis. We then discuss the affordances provided to disinformation creators by today’s emerging technologies. Finally, we compare the contemporary information campaigns about COVID-19 to show how they differ from traditional medical disinformation campaigns like Operation Denver.

**Operation Denver: Disinformation 1.0**

In the early 1980s, the KGB conducted a successful disinformation campaign coordinated with the state-owned Novosti Press Agency. This campaign sought to undermine African support for US foreign policy initiatives by alleging that the AIDS virus was a biological weapon created by the US government. It began with placing an article in an Indian print newspaper, *The Patriot*, in 1983. *The Patriot* was a news source supported by the Soviet KGB through advertisements, beginning in 1962. (That is, the infrastructure needed to support the 1983 disinformation campaign had been created a full twenty years previously.)

In 1983, *The Patriot* ran an article quoting an anonymous scientist who alleged that the US Centers for Disease Control and Prevention (CDC) and the Pentagon (through its Center for Biological Warfare at Fort Dietrich, Maryland) had worked together to weaponize an African virus which eventually became the AIDS virus. A Soviet KGB agent placed the article, seeking to have its content disseminated widely beyond the original story. The placement of a story in the Indian newspaper created distance from its source—in the Soviet Union—and conferred journalistic credibility. The story was then picked up by other news outlets in the Indian subcontinent and eventually in Africa. The campaign was carried out mainly by official government actors—including the Soviet KGB, in coordination with actors like the East European Stasi.

Russia and its allies were limited in the number of simultaneous disinformation campaigns they could carry out in the 1980s since each campaign required establishing an expensive infrastructure (of false newspapers, etc.) that took time to build and needed to be managed by professional intelligence agents. In his analysis of Soviet disinformation, Max Holland notes that even at its height, the Soviet disinformation machine may have
produced between 300 to 400 disinformation “products” per year. Each product required a significant investment of human resources and funds compared to the large volume of disinformation produced today.

In his analysis, Holland also describes how the Soviet intelligence services coordinated with those throughout the Eastern Bloc in finetuning and producing targeted disinformation. However, the timeline for producing these products involved yearly meetings and five-year plans—compared to today’s lightning-speed responses! In one example, he describes Soviet efforts to circulate a fake Newsweek magazine with incriminating information about then-President John F. Kennedy. However, President Kennedy was assassinated in the month the magazine was circulated. The campaign was relaunched with new materials, which occurred one month later. Today, such a relaunch might occur in hours or even mere minutes.

In contrast to events today, the 1983 events can be described as scattershot—as a specific audience was not identified, nor was it possible to target the disinformation toward only a select group of readers. Finally, the campaign operated linearly. The information was “seeded” (placed in a newspaper abroad), “copied” to other sources in other nations, and amplified as it reappeared in other sources.

Disinformation 2.0 Today

In contrast to the environment for Operation Denver, today’s online information environment is characterized by several key features. First, platforms (and the information collected on platforms) are dynamic and connected. Information (including user information) can be easily moved from one platform to another through practices like retweeting a narrative, aggregating user information through application programming interfaces (API) or constructing data pipelines between platforms. The information does not simply exist in one location; it is siloed and only available to a discrete set of users.
Instead, information easily transfers across systems and borders. And users can be tracked across information platforms through customer relations management (CRM) software programs. As a result, an individual can be targeted multiple times using various methods. In this new environment, the attack surface is more significant than ever before—since there is more information available to people and more information available to manipulate.

Next, a disinformation operative no longer has to construct his platform by, for example, acquiring a newspaper. Instead, narratives can be served upon preexisting platforms for which others bear the cost of construction and maintenance. At the same time, their entrance as actors on these platforms is often cost-free or minimal. To establish credibility as an actor, one must merely purchase a domain name or establish an account. There are significantly fewer barriers to entry for disinformation actors operating in cyberspace today.

Furthermore, today’s disinformation environment is both dynamic and opaque. The opaque nature of the social media environment means one is not always entirely clear with whom one interacts. In this new environment, individual and corporate users may change their identities, and site references may also change their identities. As a result, it is difficult to ascertain the social media environment’s topography. Furthermore, it is much more difficult to gauge the credibility of an online source. Knowledge production is democratized in today’s new environment, flattening the hierarchy. Anyone in the environment can function as a knowledge producer. Simon Springer describes a “new epistemology” in which users often assume that all the information they encounter is equally valid and no sources enjoy the unique epistemic privilege.\(^\text{14}\)

The velocity at which information travels across and between platforms today also means that disinformation actions can occur much faster. In this new environment, offensive players appear to have an advantage since they reach their audience first and then describe the consumer’s reality. It is, therefore, more challenging for counter-propagandists to undo these established and entrenched narratives. Furthermore, it is harder for defenders to interpolate Russia’s strategy and track it in this rapidly moving environment since a strategy may be dynamic or quickly changing and can be conducted on multiple fronts.

Finally, individual users are more willing to outsource information-seeking activities (e.g., conducting a Google search) to entities—like Alexa or Siri. Information seeking may be automated, and one cannot properly speak of an empowered information consumer.

As noted earlier, affordances refer to a material or tool’s characteristics and the types of activities conducted using this tool as a result. In thinking about the affordances associated with the opaque, dynamic, and non-hierarchical online information environment, it becomes clear that some activities become more complex while others become easier. What activities can occur, and what do they mean to develop Disinformation 2.0?
Disinformation 2.0: Target Acquisition

One set of actions that differs markedly between Disinformation 1.0 and Disinformation 2.0 is the target acquisition process. The new disinformation environment allows for “reader” and “publisher” interactions that were impossible in a material, printed newspaper world. Traditionally, information was disseminated hierarchically, and readers were essentially information consumers. Today, in contrast, the audience or readers can speak back to the news, participate in the process of disseminating news, and participate in the co-creation of news and narratives. Users are not merely targets; instead, they are “co-authors” or “force multipliers” since they can react to narratives by upvoting and downvoting them, adding to the narrative, or sharing it with their network.¹⁵

While traditional disinformation practices sought to acquire a static asset (like a newspaper) and the static audience that followed this asset, disinformation merchants today seek to utilize a prebuilt or preexisting static asset—to acquire or co-opt an engaged audience. This audience comprises preexisting interest groups and influencers who can be deployed to disseminate a narrative while lending their credibility to it, imbuing it with additional authority and credibility. Since this strategy rests on targeting and acquiring dynamic users rather than a static target, any defense strategy against disinformation must consider what adversarial actors themselves do, the audiences they target, and the response they seek to elicit.

In addition, the ability to track followers in the online environment allows today’s disinformation merchants to access a much greater universe of data regarding the audience (or audiences) they are reaching. The availability of metadata allows adversarial actors to carry out new, highly sophisticated activities, including data market segmentation and predictive analytics, to better target and manipulate data themes and campaigns. By subscribing to software as a service (SaaS) tools—such as customer relations management software—disinformation actors can easily collect data, such as how long a visitor spends on a site; demographics associated with active site users; which types of users are most likely to like, forward, or share a post; what other platforms visitors are coming from; where in the country they are located; and the time of day and frequency of unique visits to the site. Visitors can quickly be sorted into categories to include highly engaged users, less engaged users, and those who are influencers. Today, user data can be targeted in granular ways—using techniques like geofencing.

Disinformation 2.0: Customized and Granular

While Disinformation 1.0 was “diffuse,” Disinformation 2.0 is granular. Open-source information, such as public opinion data, can identify a specific audience—such as those who believe in other conspiracy theories—to target a particular narrative toward them. One can understand a group’s perceptions and then use media manipulation to exploit the difference between perception and reality, shaping an alternate reality that they are the most likely to believe.¹⁶
Due to the dynamic nature of today’s online media environment, the strategic advantage or the ability to win market share is naturally granted to the individual or group that can act most quickly. Large government organizations with hierarchies and budgets have no inherent advantage in such an environment. Instead, lithe, agile organizations have the advantage. Such groups can better retool in response to information about environmental changes quickly. For this reason, Russia and China have outsourced much of their disinformation activity, setting up multiple public and private groups, some specializing in particular narratives or types of disinformation.

Disinformation 2.0: Iterative

At the same time, while Disinformation 1.0’s messaging was singular, Disinformation 2.0 is iterative. A particular target or target group may receive multiple messages through multiple channels (an SMS on their phone due to filling out a form or petition, a tweet, a targeted ad on Facebook, or an email, for example). Using the same technology that a political candidate might use to solicit donations or to encourage someone to vote, or which your university might use to solicit an alumni donation, a malicious actor in cyberspace might seek to recruit an individual into an extremist group or encourage an individual to adopt a conspiracy theory or further disseminate this information. The software can be used to carry out a “campaign” (or series of messaging opportunities) to bring a “prospect” along on a “customer journey”—to sell them anything from a new pair of sneakers to the realization that they should participate in an insurgency against their government.

The lack of a hierarchy, barriers to entry, and the ability to share information across platforms mean that actors can conduct coordinated campaigns using multiple attack vectors. Multiple actors can pursue an objective simultaneously, as illustrated in examining Russian disinformation activities regarding COVID-19. Here, public relations firms, government, contractors, think tanks, journalists, and academics worked together to fine-tune the package of narratives utilized to undermine international confidence in US vaccine and public health measures.

The graphic explanation of Disinformation 2.0 might therefore be pictured as follows:
One final affordance of the online environment that must be considered is how increasingly computer usage is becoming democratized. While previously, only people with PhDs in computer sciences and mathematics could put together a sophisticated predictive model that relied upon machine learning and algorithms. However, programs like IBM's Watson and Salesforce's Einstein are increasingly making these tasks accessible to anyone with a computer. The availability of off-the-shelf SaaS packages—often designed for other activities, like sales—allows disinformation merchants to adjust better the “product” they are selling. In this way, CRM software is a dual-use technology that can be activated for civilian and military use. The same database programs that can track which users have “liked” a new type of tennis shoe to send them a coupon via email or place a targeted ad on their Facebook page can also be used to “sell” users a political candidate or a disinformation theme.

CRM SaaS programs are being used to aid the dissemination of online disinformation in several ways. They can increase the efficiency or “hit rate” of online disinformation, mainly targeted at specific demographics. CRM databases likely allow adversary disinformation factories to better target or segment the market for online disinformation. They are less likely to waste resources creating information that will not be forwarded or picked up. Online disinformation groups can now shape a disinformation campaign through better interactivity using simple sales techniques. They can quickly determine which themes are most likely to appeal and even conduct experiments in which group A might receive one type of message while group B receives another. Messaging can thus be fine-tuned. It is dynamic.

The final way Disinformation 2.0 differs from Disinformation 1.0 is in the variety of actors who can participate in disinformation tradecraft today. While previous studies emphasized intelligence agents’ skills and training to participate in disinformation tradecraft, disinformation practices today may be carried out by multiple actors—including public servants and private citizens, those who work directly for the government, who are contractors. Disinformation practices rely on national civilians, private companies, and actors like public relations firms. For this reason, the US State Department's Global Engagement Center today refers to a “disinformation ecosystem” established by Russian intelligence, including pseudo-academic think tanks, relationships with academic departments, state-sponsored television stations, and civilian social media channels.\textsuperscript{19}

In addition, as Milena Dimitrova notes, “Disinformation as a service exists. Individuals or groups wishing to disseminate a false narrative may request service on the Dark Web and hire someone to carry out this work on their behalf.”\textsuperscript{20}

And finally, today’s attackers may be both humans and bots. Artificial intelligence (AI) elements of CRM programs may assist in market segmentation, carry out targeted tests of various disinformation narratives, and map out possible customer journeys for recruited groups.
Table 1 summarizes the specific technological affordances that cause Disinformation 2.0 to differ significantly from Disinformation 1.0.

**Table 1: Specific Technological Affordances in Disinformation 2.0**

<table>
<thead>
<tr>
<th>Characteristics of Platform</th>
<th>Linked/connected (more excellent attack surface)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Fewer barriers to entry</td>
</tr>
<tr>
<td></td>
<td>Non-hierarchical arrangement of information (leading to “new epistemology”)</td>
</tr>
<tr>
<td><strong>Attack Surface</strong></td>
<td>Opaque, Dynamic, Larger</td>
</tr>
<tr>
<td><strong>Characteristics of Information/Big Data</strong></td>
<td>Velocity: speed of information change advantages an attacker over a defender</td>
</tr>
<tr>
<td></td>
<td>Veracity: harder to verify information sources and attribution.</td>
</tr>
<tr>
<td></td>
<td>The high volume of information</td>
</tr>
<tr>
<td></td>
<td>Greater variety of types of data</td>
</tr>
<tr>
<td></td>
<td>The advantage for first movers is those who move most quickly.</td>
</tr>
<tr>
<td></td>
<td>Democratization of data manipulation skills due to off-the-shelf SaaS CRMs</td>
</tr>
<tr>
<td><strong>Weaponized information</strong></td>
<td>Faster, more dynamic, cheaper, more varied, easier to manipulate</td>
</tr>
<tr>
<td><strong>Actions Possible on platforms</strong></td>
<td>Interactivity: Users co-create narratives of information through liking and retweeting</td>
</tr>
<tr>
<td></td>
<td>Surveillance: can better segment information through knowing who is liking and sharing (availability of metadata)</td>
</tr>
<tr>
<td></td>
<td>Iterated “information journey” versus one-off encounter</td>
</tr>
<tr>
<td></td>
<td>Narratives can be dynamic—evolve in response to user reactions.</td>
</tr>
<tr>
<td></td>
<td>Narratives can be TESTED and modified by testing different narratives on different users</td>
</tr>
<tr>
<td><strong>Strategies</strong></td>
<td>Dynamic</td>
</tr>
<tr>
<td></td>
<td>Iterated</td>
</tr>
<tr>
<td></td>
<td>Interactive</td>
</tr>
</tbody>
</table>


### Types of Actors

<table>
<thead>
<tr>
<th>Types of Actors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large and small actors</td>
</tr>
<tr>
<td>Outsourcing: disinformation as a service, use of private providers</td>
</tr>
<tr>
<td>Overlaps between sales, public relations, and disinformation</td>
</tr>
<tr>
<td>Automated actors like bots</td>
</tr>
<tr>
<td>Use of automated algorithms to segment information test varied narratives</td>
</tr>
</tbody>
</table>

### Disinformation 2.0: A Smart Weapon

As this short history of disinformation’s technological evolution illustrated, today’s disinformation is, in actuality, a type of intelligent weapon. Smart weapons possess three significant characteristics. They can be controlled remotely, often from a distance, by operators who no longer need to be physically present. Intelligent weapons are also precision-guided, enabling the operator to be more precise in her targeting rather than simply blasting away at a target. Precision-guided munitions, guided by technologies like facial recognition, can be aimed only at a specific individual. Finally, intelligent weapons are dynamic—a bomb’s coordinates might be adjusted and readjusted while in flight in response to new information received about the environment.

These characteristics—remote guidance, precision guidance, and dynamic adjustments—also characterize disinformation vectors being “fired” today. First, as noted, disinformation is remotely guided by various actors who do not have to be physically present in a specific location to deliver a disinformation bomb.

Disinformation can now also be precision guided. With the 2012 advent of the Internet of Things, users are engaged in man–machine interactions, increasingly not merely accessing the web but producing and interacting with data. As a result, users today experience a customized environment that adapts and changes to their likes and dislikes. Every user receives unique curated information, different from anyone else. AI is used to curate user feeds, even without the user’s knowledge of these practices.

And this new customized environment doesn’t merely present information for the user to take or leave but is designed to draw the user in, taking them on a “customer journey.” And just as a uniquely designed customer journey may have an end goal of causing you to make a purchase, the consumer’s disinformation journey has an end goal of galvanizing them toward actions. Individuals can be recruited and activated in new and unexpected ways in this environment.

Finally, disinformation today represents a dynamic type of warfare. Russian analyst Evgeni Pashentshev describes another unique feature of the online environment today. Just
as an individual might manipulate our emotions toward a real-life environment through, for example, playing music or “staging” an apartment for sale, an online environment can be manipulated through invoking psychological practices. He describes how AI programs can gauge the emotional temperature of an online environment through sentiment analysis. Analyzing the words used and the images shared, disinformation warriors can determine which narratives might play well at a given time. (Are people feeling angry? Are they threatening violence?) Narratives can be fine-tuned to play well at a particular historical juncture (like an election) and match what audiences already feel.

In contrast to the single-themed Operation Denver, which was designed to “hit” all audiences in the same way, today’s COVID Disinformation 2.0 campaign had two prongs—those aimed at a diffuse audience and those which are highly targeted and specific (or segmented).

A diffuse or general goal of today’s disinformation campaigns is to sow confusion and chaos in the online environment. US adversaries may therefore contribute information of dubious quality and provenance to undermine user confidence in the online medium. Drawing on Luciano Floridi’s work, one can conceptualize the “infosphere” as a domain or field that can be degraded through various actions. Floridi suggests that just as a bad actor can pollute a familiar territory, such as the air or the water, rendering it unusable or unsafe for all users, an actor can degrade the online environment through the proliferation of spam or the unleashing of bots. Just as people’s activities are constrained if they cannot readily access safe drinking water or clean air but must instead devote time and energy to engaging in risk calculi before utilizing these resources, people’s abilities to utilize the online environment are degraded when questions exist as to its safety and potential harmfulness.22

Vladislav Surkov refers to this tactic as the “firehose of falsehood.” Here, the objective is to confuse those attempting to communicate in a chaotic online environment. The actual choice of narratives can include multiple narratives, some of which may even be contradictory. The aim is not to create a coordinated strategy but to introduce as much noise as possible in the environment.23 Productivity and efficiency suffer when individuals must navigate a chaotic, unpredictable environment characterized by high noise levels. And user trust in the environment is lessened as the impression may be created that all information encountered is untrustworthy.

When adversaries choose to “pollute” the online information, state and commercial actors are forced to devote significant resources to safeguarding that environment. The term “infodemic” describes the overall degradation of the information environment about COVID-19 information. Combatting the disease has been rendered more difficult because of attempts (by both Russia and China) to breed user distrust of official sources, confuse official and unofficial sources, and amplify conspiracy theories and rumors that have no basis.24 Such diffuse environmental degradation strategies rest on adversaries’ ability to insert large amounts of information into the environment. For this reason, states seek ways to
leverage economies of scale. Thus, degradation attempts may be automated and outsourced to domestic and foreign actors who specialize in creating online media campaigns.

At the same time, one can identify targeted narratives designed to appeal to a pre-selected group and often piggybacked onto or using existing infrastructure. A theme that emphasizes that “Big Pharma can’t be trusted” might be targeted toward those opposing vaccination on principle, those who oppose “Big Government,” and believing that government policies are frequently racist. In the US, the vaccine denial movement is already established, encompassing, for example, those who believe vaccines cause autism. Therefore, such groups might be predisposed both to believe Russian disinformation regarding the efficacy of a COVID vaccine and to amplify information that they receive that accords with their preexisting belief systems due to a phenomenon known as confirmation bias. The theme of COVID vaccines as harmful could thus find a ready-made home on anti-vaccine websites and within anti-vaccine channels on sites like Twitter, Instagram, and Pinterest. Thus, contemporary disinformation practices may be described as parasitic. By attaching themselves to legitimate platforms, Russian agents improved the impression of credibility and authenticity of their information. They saved the costs (and time) associated with creating accounts and developing followers.

In their analysis of Russian disinformation practices implemented in the 2013 Russian/Ukraine conflict, Ulises Mejia and Nikolai Vokuev describe how Russian agents utilized public members as “force multipliers,” coopting existing mass movements and seeding these movements with disinformation. In this way, they argue that citizens, often unwittingly, were led to amplify and recirculate disinformation. Rather than the “blast” of information that might have been produced in the past, disinformation in the Euromaidan era was more like a precision weapon. Russian authorities were much better able to control what information was passed, the exact moment it was passed, and the audiences that would receive it.

In addition, one can see how the theme of “COVID as a racist bioweapon” is merely a variant of the theme of “AIDS as a racist bioweapon.” One such set of “facts” already exists within an information environment, making it easier for the second set of “facts” to gain a foothold.

Table 2 describes the themes used in COVID disinformation campaigns, showing how they are deployed for both diffuse and segmented audiences.
<table>
<thead>
<tr>
<th>THEME</th>
<th>DIFFUSE</th>
<th>TARGETTED</th>
</tr>
</thead>
<tbody>
<tr>
<td>COVID AS DISEASE</td>
<td>US-Developed Bioweapon</td>
<td>US Racist Bioweapon</td>
</tr>
<tr>
<td>(military strategic)</td>
<td>Not from China</td>
<td>US military exercises in the EU spread COVID to allies.</td>
</tr>
<tr>
<td>POLICY RESPONSE</td>
<td>The US was unprepared</td>
<td>Russian foreign aid is being provided to the developing world.</td>
</tr>
<tr>
<td>(efficacy of response; motives)</td>
<td>WHO is lying?</td>
<td></td>
</tr>
<tr>
<td>TRUST (quality of information; sources)</td>
<td>USG is lying about deaths</td>
<td>The US is lying about vaccine efficacy.</td>
</tr>
<tr>
<td></td>
<td>USG is lying about the efficacy of the vaccine</td>
<td>The US is lying about vaccine side effects.</td>
</tr>
<tr>
<td></td>
<td>WHO is lying?</td>
<td>US/CDC is lying about alternative treatments and their efficacy</td>
</tr>
<tr>
<td></td>
<td>(Your sources of information are untrustworthy)</td>
<td>US/CDC is keeping alternative treatments from the American people</td>
</tr>
<tr>
<td>FREEDOM (civil rights during crisis/disease/ security)</td>
<td>CDC is lying about YOUR risk of contracting the disease</td>
<td>US/CDC is lying about the efficacy of masking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Shutdowns violate civil rights</td>
</tr>
<tr>
<td>VACCINE</td>
<td></td>
<td>Vaccine mandates should be opposed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Medical personnel should have the right to oppose vaccination</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Military personnel should have the right to oppose vaccination</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mandates represent a type of (Nazi) authoritarianism</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mandates are one more way the Left imposes its values on others</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vaccine is dangerous</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Russian vaccine is better</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The vaccine is a medical experiment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Microchip/Bill Gates</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alternative Treatments are Effective</td>
</tr>
</tbody>
</table>
Comparing Disinformation 1.0 and Disinformation 2.0

In contrast to Operation Denver, the COVID information campaign represented a new technological sophistication, offering multiple advantages to the attackers. First, the overall “attack surface” for disinformation campaigns was larger since, in addition to utilizing traditional print and broadcast media, today’s disinformation merchants can utilize additional techniques like instant messaging, social media, and websites—often in unison to amplify their messages, to build a more extensive web of sources containing the information (therefore achieving a larger illusion of credibility) and to bring the reader on a “journey” in which they encounter messaging in a variety of formats over a variety of times.

In addition, one can identify an evolution and a segmentation of themes—with some themes selected to appeal to a group like anti-vaccine activists. In contrast, others were targeted toward anti-government activists and conspiracy theorists. In the two years of the pandemic, some themes have been abandoned in favor of other themes, and vaccine themes have merged and piggybacked onto other themes, including elections, civil rights, and minority rights.

Table 3 provides a comparison of new and old disinformation practices.

<table>
<thead>
<tr>
<th>OLD Disinformation</th>
<th>NEW Disinformation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discrete (self-contained, professional tradecraft activity); “Home-grown.”</td>
<td>Co-optation of legitimate social movements and channels.</td>
</tr>
<tr>
<td></td>
<td>outsourcing of information production and replication</td>
</tr>
<tr>
<td></td>
<td>(Overlap between disinformation and public relations)</td>
</tr>
<tr>
<td>Long-term deeply rooted in cultivated sources; Strategic</td>
<td>“Agile,” dynamic, shifting; both strategic and tactical</td>
</tr>
<tr>
<td>One-way</td>
<td>Interactive</td>
</tr>
<tr>
<td>Scattershot</td>
<td>Targeted, segmented</td>
</tr>
<tr>
<td>One-off</td>
<td>Iterative (build on successes, use of AI to better target and predict effects); shares territory with online radicalization</td>
</tr>
<tr>
<td>Expensive</td>
<td>Cheap (through cooptation); low-entry costs</td>
</tr>
<tr>
<td>Dumb</td>
<td>“smart” disinformation – define</td>
</tr>
</tbody>
</table>

How to Combat Disinformation 2.0

Disinformation 2.0 departs significantly from earlier forms of disinformation and earlier disinformation strategies and tactics. How, then, should those who seek to disarm Disinformation 2.0 proceed?

First, the new disinformation cannot be combatted using old tactics and strategies. Instead, what is required is a new way of conceptualizing the problem. As shown throughout
this paper, the battlefield upon which today’s disinformation wars will be fought bears minimal resemblance to the previous battlefield. Today’s battlefield is multidimensional and dynamic and, most importantly, creates new relationships between those who create and those who receive disinformation.

Therefore, traditional notions of “defending the information domain,” which relies upon a territorial analogy, are no longer valid. Because information users are implicated in the co-creation and dissemination of disinformation, it is incorrect to conceptualize them as passive subjects who need to be defended. Instead, online radicalization is a reciprocal, iterated (or ongoing) process. The interaction between buyer and seller is not coercive but rather persuasive. Each participant acts agentically in the “dance of disinformation.”

The disinformation actor is thus better described as a “merchant”—intent on selling a particular narrative to a specific buyer and enlisting the buyer as an influencer who will encourage others to buy (or buy into) the narrative. The term “disinformation merchant” describes someone working in an information market where information of varying provenances and quality is available. Each agent competes for buyers in this market, competing against other “information merchants” offering competing products. As with an actual market, the information market is largely unregulated and open to all sellers. And, like an economic market, the information market is segmented. Some merchants may offer a niche product (i.e., anti-vaccine disinformation) and may work to capture that market segment while undercutting and driving out others in that information space.

This metaphor of competing for market share with other information merchants allows us to think of neither side as taking an offensive or a defensive position since the space does not implicitly belong to one or another player. Instead, both players must take an offensive or activist position to outcompete their opponents.

This is not to say that actors do not act strategically. Each side acts to identify vulnerable consumers of information and disinformation and then persuade (but not coerce) them to buy what is on offer. For example, Russian and Chinese governments may have identified Western audiences for anti-vax activism narratives. They appealed to existing groups, like those opposing other vaccines, and utilized their resources to spread anti-COVID vaccine information further.

The disinformation merchant then has two goals: to sow disinformation diffusely into the environment to degrade the overall quality of the information environment for all users equally; and to target specific individuals and groups to radicalize them toward the support of specific positions or the taking of specific actions.
Conclusion

Given the unique characteristics of Disinformation 2.0, what strategies and tactics would be most effective in combatting it? An anti-disinformation strategy might be constructed by looking at how, for example, nations and the international community have acted to control the dissemination and weaponization of nuclear materials, which have both peaceful civilian and military uses. In this situation, civilian and military facilities are subject to inspections and monitoring by the international community. Nations are required to furnish annual reports of their inspection and monitoring activities.

The US government should coordinate more closely with the top customer relations management software producers to combat online disinformation, including recruiting more personnel from this industry. Civilian companies should be required to conduct due diligence regarding their clients’ identities and activities—both those deploying software and those storing their results in the cloud. Legislation that creates regulations governing the inspections and monitoring of clouds like the Amazon commerce cloud or the Salesforce Business Cloud should be enacted.

Furthermore, stricter regulations need to be enacted governing the use of artificial intelligence programs to engage in customer segmentation and test customer relations content. Today, emerging concerns in the information space include the possibility of training personalized chatbots furnished with disinformation scripts. Just as US military regulations require a human in the loop during certain military operations, regulations should be enacted to require a human during the testing and deployment of narratives in the information space.

Finally, the US should enact stricter privacy laws governing the collection of user information, the storage of that information, and the sale. Here the European General Data Protection Regulation (GDPR) can serve as a model. Stricter rules governing who may collect user information, the requirement that users be informed (and consent) to collect such information, and regulations governing the storage and sale of user information can help stem online disinformation efforts.

Mary Manjikian is a professor at Regent University in Virginia Beach, Virginia. She received her BA from Wellesley College, an MPhil from Oxford University, and an MA and PhD from the University of Michigan. She is the author of Apocalypse and Post-Politics: The Romance of the End (Lexington, 2012); Threat Talk: Comparative Politics of Internet Addiction (Ashgate, 2012), The Securitization of Property Squatting in Western Europe (Routledge, 2013); and Gender, Sexuality and Intelligence: The Spy in the Closet (Palgrave, 2020). She also authored two textbooks: Cybersecurity Ethics: An Introduction (Routledge, 2017) and Introduction to Cyber Politics and Policy (Sage, 2019). She is also a former US foreign service officer with service in the Netherlands, Russia, and Bulgaria.
Endnotes


SUBMISSION GUIDELINES

The journal accepts a manuscript on the understanding that its content is original and that it has not been accepted for publication or review elsewhere. All papers will undergo anonymous peer review. The reviewers, who are selected based on their expertise in the area of the submitted papers, will evaluate the manuscripts on the basis of creativity, quality of scholarship, and policy relevance. Once accepted for publication, copyright resides with the journal. Authors should submit their manuscripts via e-mail to peaceandwar@norwich.edu

The length of a research article should be between 5,000 and 7,000 words, including endnotes and references. Each article must include an abstract of less than 200 words and 5-6 keywords. All manuscripts should be submitted in Microsoft Word format, and text should be double-spaced, Times New Roman font point 12 (including references) and left justified.

SPELLING AND STYLE: Note that we conform to Webster’s Collegiate Dictionary and The Chicago Manual of Style in matters of spelling, abbreviation, punctuation, etc. On first use of an acronym or abbreviation in the manuscript, please spell it out in full.

FIGURES AND TABLES: All figures and tables should be professional in appearance. Provide figures as separate data files instead of as pictures embedded within the Word document. Location of illustrations should be indicated by a note in the text (e.g., “Table 1 about here”).

BIOGRAPHICAL SKETCH: authors must include a brief biographical sketch, including institutional affiliation, primary publications, and relevant experience. Length should be 200 words or less.


Books: Feldman, Lily Gardner, Germany’s Foreign Policy of Reconciliation: From Enmity to Amity (Lanham, MD: Rowman and Littlefield Publishers, 2012), 20-33


For multiple notes referencing the same work, please use the following shortened note form after the first reference.
Feldman, Germany’s Foreign Policy of Reconciliation, 73-78.
CONTENTS

Russia’s Grand Strategy toward the West
Thomas Graham....................................................................................................................................1

The Domestic Foundations of Russian Foreign Policy
Peter Rutland........................................................................................................................................16

Lessons From Syria: What We Can Learn About the Russian Way of War
Nikolas K. Gvosdev.............................................................................................................................32

‘Terrorist Recruiters’ Versus ‘Terrorist Slayers’: Weaponizing Syria in Russian Information Warfare
Eszter Szenes and Mark W. Perry......................................................................................................47

The Aftermath of the 2008 Russo-Georgian War: Appeasement of Russia and the War in Ukraine
Lasha Tchantouridzé...........................................................................................................................77

The Russo-Chinese ‘Strategic Partnership’ Enters a New and Dynamic Phase
Lyle Goldstein and Vitaly Kozyrev....................................................................................................95

Not Your Father’s Disinformation: Emerging Technology, Social Media Advances, and the Growth of Smart Disinformation
Mary Manjikian.................................................................................................................................130

Bosnia and Russia: The Implications for European Security and US Interests
Nadina Ronc......................................................................................................................................148

Russian Information Operations: The Kremlin’s Competitive Narratives and Arctic Influence Objectives
P. Whitney Lackenbauer, Troy Bouffard, and Adam Lajeunesse.......................................................161

Volodymyr Zelenskyy’s Vision of Ukrainian Nationhood
Jessica Pisano.....................................................................................................................................187

Borderland No More? Shifting Security Dynamics in Ukraine
Angela Kachuyevskii.........................................................................................................................199

STUDENT RESEARCH

The Yugoslavia Civil War and the Allies in World War II
Caleb M. Reilly...................................................................................................................................211

Evaluating the Value of US Diplomacy Through Strategic Ambiguity
Ethan Owens......................................................................................................................................225