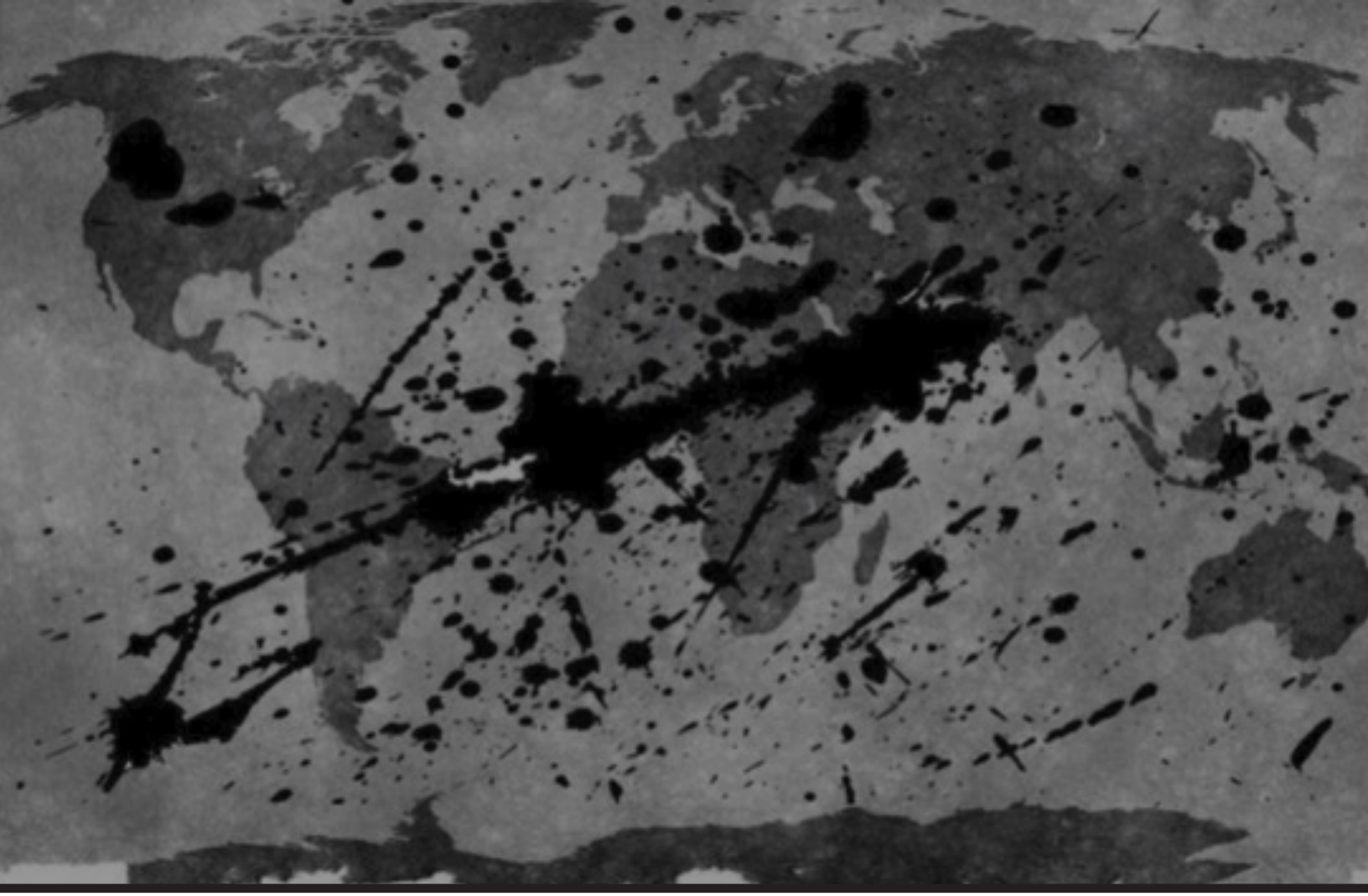


Brief No. 12.6

Disinformation Ink Spots

A Framework to Combat Authoritarian Disinformation

Lincoln Zaleski

P | I | P | S

Disinformation Ink Spots
A Framework to Combat Authoritarian Disinformation Campaigns

APRIL 2020

Lincoln Zaleski

P | I | P | S
The Project on International Peace and Security
Global Research Institute
College of William & Mary

Disinformation Ink Spots
A Framework to Combat Authoritarian Disinformation Campaigns

Modern disinformation campaigns, enabled by emerging technologies, allow authoritarian regimes to exploit inherent democratic vulnerabilities. This white paper provides a conceptual framework for understanding authoritarian disinformation campaigns, building on the ink spot approach to countering insurgencies. Using an array of precision targeting and data collecting technologies, authoritarian regimes identify key individuals and groups in the United States to reinforce, shape, and connect. The regimes seek to create a domestic network of influential "ink spots." Hostile or antagonistic governments then use these sympathetic spots to undermine U.S. policy and democracy through constant reinforcing and manipulation of identity and beliefs.

The Ink-Spot Disinformation framework strengthens the United States government understanding of the nature of authoritarian disinformation campaigns and provides a new conceptual foundation for U.S. disinformation defense and deterrence.

Introduction

Authoritarian regimes, such as Russia, use information warfare to target inherent vulnerabilities in liberal democratic institutions, societies, and economies. These regimes undermine liberal democracy by amplifying social polarization, promoting societal and political entropy, and discrediting objective reality.[1] Modern disinformation warfare combines old practices of propaganda and disruption with new technologies and strategies, creating a more effective, less detectable information campaign.

While the United States has identified many individual information warfare tactics, no consensus has emerged about a strategic framework for understanding how disinformation campaigns operate.[2] The lack of a framework is partly due to the highly adaptive nature of information warfare and the belief among some practitioners that a strategic framework is of little utility.[3] However, this paper argues that a broad conceptualization of disinformation warfare is necessary for understanding how adversaries seek to manipulate democratic politics and for devising defenses. This paper provides such a framework—Ink-Spot Disinformation—based on the ink-spot approach found in the counterinsurgency literature.

Technology and the New Information Warfare

The nature of modern information warfare combines new technologies with traditional practices and objectives to enable a highly adaptable and effective information campaign.

Established Disinformation Practices

During the Cold War, the Soviet Union used "active measures" to sow discord against the United States among Western allies, the American public, and the global population.[4] Active measures was a catch-all phrase for Soviet influence operations, which included practices such as:

- *Written and oral disinformation*. Soviet dezinformatsiya involved the dissemination of untrue or manipulated statements, intended to discredit non-Communist leaders and influence populations in favor of Soviet goals. As an example, in late 1979, the Soviet Union spread a rumor in the Middle East through newspapers and clandestine radio stations that the United States was behind the seizure of the Great Mosque of Mecca.[5]

- *Forgeries and false rumors*. The Soviet Union produced false documents, usually fake US military doctrines or war plans, to sow discord between the United States and a target country.

- *Manipulation and control of foreign media*. The Soviet Union hired local journalists to submit stories to foreign media outlets sympathetic to Soviet ideological goals. To influence India, the Soviets used local journalists to publish false documents and favorable articles in the newspaper *Blitz.*[6]

- *Political action and the use of agents-of-influence operations*. The Soviet Union exploited individuals with political, economic, or media influence to secure active collaboration with Moscow.[7]

- *Use of foreign communist parties and international front groups*. The Soviet Union actively collaborated with communist parties and front organizations abroad, such as the World Peace Council and the World Federation of Trade Unions.[8] These organizations enabled Moscow to reach audiences that were not sympathetic to Soviet information.

- *Support for international revolutionary and terrorist organizations.* The Soviet Union engaged in direct outward support for national liberation and terrorist organizations, but also supported these campaigns by manipulating public support through disinformation. In El Salvador, the Russians supported an insurgency against the US-backed government by rallying public support for the insurgents through media outlets.[9]

- *Transnational repression of political opponents*. Soviet operatives also assassinated and intimidated political opponents around the world to protect Soviet secrets and minimize counterinfluence.

These methods of influencing the public allowed the Russians to operate in the "gray zone" of warfare, where the actions damaged the United States, but did not warrant a declaration of war.[10] The Russians could successfully demoralize the American population, drive a wedge between allied nations, and weaken global perceptions of the United States, while claiming plausible deniability.

However, active measures were not unconnected influence campaigns conducted by the Soviet Union. These operations were parts of a hierarchical, coordinated process to gain an advantage in

a perceived ongoing, existential conflict with the West.[11] While developing these tools of influence, the Russians believed that warfare was a duel of information systems and whoever controlled the narrative message would win the war.[12] Each active measure listed above delivered targeted messages within Western society, promoting Russian ideological expansion, protecting Russian information control, and eroding Western domestic influence.

In order to engage in ongoing ideological-psychological warfare, Soviet influence operations were massive, employing up to 15,000 intelligence officials for the sole purpose of deploying traditional active measures.[13] Despite the high cost, the Russian belief in the importance of information control and the drive to win the "rivalry of civilizations" against the West led the Soviet Union to adopt active measures as a fixture of their foreign policy.[14] Soviet active measures are the key building blocks of the current authoritarian disinformation campaign model.[15]

The success of Soviet active measures in altering foreign government policies remains unproven. However, Soviet active measures were largely successful in persuading targeted individuals. By repeating false information through radio services or newspapers and manipulating narratives, active measures successfully created echo chambers of repeated messaging, among other psychological methods of persuasion, which were successful in convincing populations of Soviet propaganda. In addition, the Soviets were often successful in masking the true source of the active measures, strengthening their intended message.[16]

However, while Soviet active measures often successfully deceived individuals, their actions remained traceable to target governments and limited in scope.[17] Active measures could deliver convincing messages; however, the Soviet strategy could not reach a large target audience through top-down targeting. Russian influence failed to permeate every level of society, and the American populous remained largely resilient to the Russian propaganda.[18] Government counter-narratives dominated US airwaves and prevented any fifth column or pro-Soviet majority from gaining significant influence in American society.[19]

New Technologies in Disinformation Campaigns

Post-Cold War Russia sought ways to expand active measures to fully penetrate American society and promote the Russian global model of illiberalism. Other authoritarian regimes began learning from Russian active measures, spreading disinformation worldwide.[20] However, while the psychology and tactics were capable of delivering a message, the operations of active measures remained expensive and limited to an unspecific population or government agency.[21] Attacking countries needed active measures to be more covert and their messages to have a more targeted delivery in order to anonymously and directly reach the masses.

In the past two decades, new technology has drastically altered the infospace, allowing for free and easy data collection on a massive scale, as well as access to nearly every individual in the world through global networks. Online interconnectivity allows ideas and ideologies to spread unchecked across the web. The US government monopoly over public information is nearly non-existent, locating and targeting individuals is incredibly simple, and anonymity is a hallmark of the internet.[22]

Because of new technology, the psychological impacts of active measures have intensified.[23] On-line echo chambers reinforce pre-existing beliefs, trolling and sensationalism silence truthful narratives, and fragmentation of information sources further polarizes US society. Constant repeated messaging on every platform convinces individuals that their pre-existing biases are correct and that the opposition is not intelligent enough to have a civil discourse, forming strong collective ideologies.[24]

The new technologies increase data collection, target identification, and accessibility; manipulate social reality; and decrease detection, creating an incredibly dangerous opportunity for promoting non-objective reality. These technologies enable the success of the current disinformation warfare.

Figure 1: Emerging Technologies in Information Warfare

Goal of Information Campaign	New Technologies Used	Role of Technology in Achieving Goal
Increase Data collection	Security and surveillance systems	Vast audio/visual, camera and sensor networks collect data on individual habits
Increase Data collection/Target identification	Artificial Intelligence (AI)	AI collects data on individual habits and determines individual susceptibility to disinformation campaigns
Increase Data collection	Hacking	Stealing existing datasets improves the attacking country's datasets
Target Identification	Algorithmic Decision-making	Algorithms recognize patterns to determine the most vulnerable targets
Target Accessibility	Social Media Bots	Identified individuals receive repeated false messaging through targeted bots
Manipulation of Social Reality	Virtual/Augmented Reality (VR/AR)	VR/AR make falsehoods visible reality
Manipulation of Social Reality	Deepfakes	Information campaigns utilize deepfakes to propagate undetectable fake information
Avoid Detection	Blockchain/ledger systems	Ledger-based systems prevent traceable footprints
Target Accessibility	Direct Messaging	Direct Messaging of identified targets assists in precision individual targeting

Using new technologies, disinformation campaigns can now identify specific targets and operate undetected, strengthening the psychological impact and capabilities of active measures.[25] Modern disinformation campaigns seek to remain in the "gray zone" and avoid direct conflict, as a quick

attack against American society could be classified as cyberwarfare. Technology-enabled active measures are slow and piecemeal, with each seed of doubt building up over time.[26] Additionally, these new campaigns continue alongside active measures and capitalize on plausible deniability as a mechanism for attack.[27]

The combination of traditional practices and new technology in disinformation campaigns is not new information. The aforementioned emerging technologies strengthen and enable active measures, allowing for precise individual targeting and decreased detection. However, the capability to target individuals discreetly does not alone guarantee a successful disinformation campaign. Aggressors must identify the specific targets of active measures to create the illiberal network successfully. The US government understands how information warfare campaigns unfold, how messages are delivered, and how emerging technologies are dangerous; however, strategists in the United States have largely overlooked how the targeting strategy of disinformation campaigns provides insight into US vulnerabilities.[28]

Strategy of New Information Warfare

Current disinformation campaigns follow a similar strategy to the "ink spot" counter-insurgency technique used in Iraq and Afghanistan.[29] The "ink spot" or "oil spill" approach to counterinsurgency focuses on retaking insurgent-held territory while outnumbered. This technique follows a clear-hold-build strategy. First, small groups of counterinsurgents are placed at strategic locations within the territory. Next, these counterinsurgents clear surrounding territory of insurgent fighters and hold the territory to prevent a resurgence of violence. Finally, counterinsurgents build relationships with the local populace, seeking to prevent further harboring of insurgents. When identifying specific targets, or "ink spots," in liberal democracies, the authoritarian disinformation model uses a two-pronged approach to gain political influence: the traditional top-down approach and the emergent bottom-up approach.

Traditional Top-Down Targeting in Disinformation Campaigns

Authoritarian regimes continue to use the targeting strategy developed under the Soviet Union to deploy active measures. The traditional top-down approach to authoritarian disinformation campaigns includes targets identified under Soviet active measures and requires less precise target identification. Using state economic resources, the attacking regime seeks to acquire data and political influence through target country corporations and corrupt politicians.[30] Within liberal democratic society, these traditional ink spots can be separated into two categories:

1. *Corporate Ink Spots*. Disinformation campaigns target local corporations seeking financial links with the attacking country. By leveraging economic linkages, the authoritarian regime develops an "unvirtuous cycle."[31]

   The unvirtuous cycle follows a four-step process. First, the attacking regime establishes partnerships between target corporations and large, state-run corporations in the attacking

country. Second, through these partnerships, attacking country corporations increase their local political power and visibility in the target country. Third, as the political and economic power of regime affiliates increases within the target country, the regime corporation can successfully lobby the target government. Finally, as lobby efforts succeed, authoritarian regimes advance their interests within the target state and expand their patronage network with more domestic corporations, furthering local partnerships and repeating the cycle.

Through politically motivated partnerships and investments, authoritarian regimes gain footholds within the target state, which they continue to manipulate through a combination of lobbying, energy blockades, bribery of officials, media manipulation, and expansion of economic connections.[32] The "unvirtuous cycle," lubricated by corruption, is intended to shape policies and decisions in favor of the influencing regime.[33]

2. *Influential Individual Ink Spots*. Disinformation campaigns target corrupt politicians or influential individuals who are willing to undermine their own democratic system for personal economic or political gain. Authoritarian regimes seek to coopt these ink spots through a system of bribery, including campaign financing, endorsements, and blackmail, in order to gain further political influence within the target society.

   By identifying influential individuals and politicians, authoritarian regimes gain political sway within the target government.[34] Coopted individuals promote the attacking regime's policies inside the target country in exchange for campaign donations and political favors. While new technology broadens and strengthens this strategy, this type of top-down economic manipulation was an active measure prior to the new age of disinformation.[35]

Emergent Bottom-Up Targeting in Disinformation Campaigns

The new aspect of modern technology-enabled disinformation campaigns is the ability to identify and target small groups or individuals within liberal democratic society. In contrast to top-down targeting, which takes significant resources to influence corrupt politicians and corporations, bottom-up targeting is much cheaper and the target groups are easier to influence. Specifically, attacking regimes seek the ability to identify collectives with the potential to gain political influence.

Identity can initiate powerful change. Nationalist and politically active identity groups spread a message of division between the in-group and the out-group, recruiting new members to the collective and attempting to disrupt the status quo.[36] The key conditions for identity-based manipulation are feelings of shame due to personal identity and an intent to return to an imagined way of life in which one's identity and value systems are dignified.[37] Authoritarian regimes identify key targets based on these two conditions: whether the potential target feels marginalized and whether the potential target seeks to change the status quo.

The bottom-up "ink-spot" approach to understanding disinformation campaigns conceptualizes two categories of ink spots:

1. *Marginalized-Identity Ink Spots*. Disinformation campaigns target disenfranchised groups with a collective identity and desire to change status quo. Attacking regimes highlight and exaggerate the differences between the identity group and the outside society, exploiting feelings of marginalization.

2. *Co-ethnic Ink Spots*. Disinformation campaigns target co-ethnic and diaspora communities with pre-existing connections and shared language with the attacking regime.[38] Attacking regimes use language-based messaging or cultural nostalgia to target co-ethnic communities, contributing to feelings of marginalization and encouraging collective political action.

Both of these "emergent" ink spots are targeted through the identify-cultivate-link strategy of disinformation, described in the following section.

Ink-Spot Disinformation

The identified targets or "ink spots" are the foundation for a new conceptual framework for disinformation.[39] As mentioned above, the key to a successful disinformation campaign is successful targeting; therefore, a population-centric campaign has the most success. Drawing from the counterinsurgency literature, the actions of most attacking regimes closely mimic the clear-hold-build or "ink spot" approach to counterinsurgency.[40]

The emergent "bottom-up" half of ink-spot disinformation is targeted through an identify-cultivate-link campaign, as outlined below.[41]

First, authoritarian disinformation campaigns identify potential ink spots that are susceptible to the embedded message of influence through several methods:

- *Firehose of Falsehood.* The attacking regime releases false news stories across social media and record individuals who click on fake stories in order to identify susceptible targets.[42]

- *Institutional Research*. The attacking regime engages in institutional intelligence collection by government agencies or contracted groups to single out historically disenfranchised or politically mobile fringe organizations for potential targeting.[43]

- *Identification through Influencers*. The attacking regime gathers data on individuals who engage with conspiracy theory promoters, fringe or nationalist individual influencers, or other individuals with radical beliefs, seeking to identify potential marginalized ink spots.[44]

Second, disinformation campaigns cultivate these ink spots with messages of influence to harden their pre-existing beliefs and ideology and encourage them to continue promoting the desired change to the status quo:

- *Repeated Messaging*. Attacking regimes encourage political action among ink spots through a string of targeted false news stories. These narratives capitalize on pre-existing biases, seeking to reach a successively larger audience as the repeated messaging is shared through social media.

- *Economic incentives*. Attacking regimes cultivate the ink spot perspective by running nationalist campaign ads; donating to campaigns that promote in-group/out-group politics; and directly funding influencers, political organizations, and identity groups.[45]

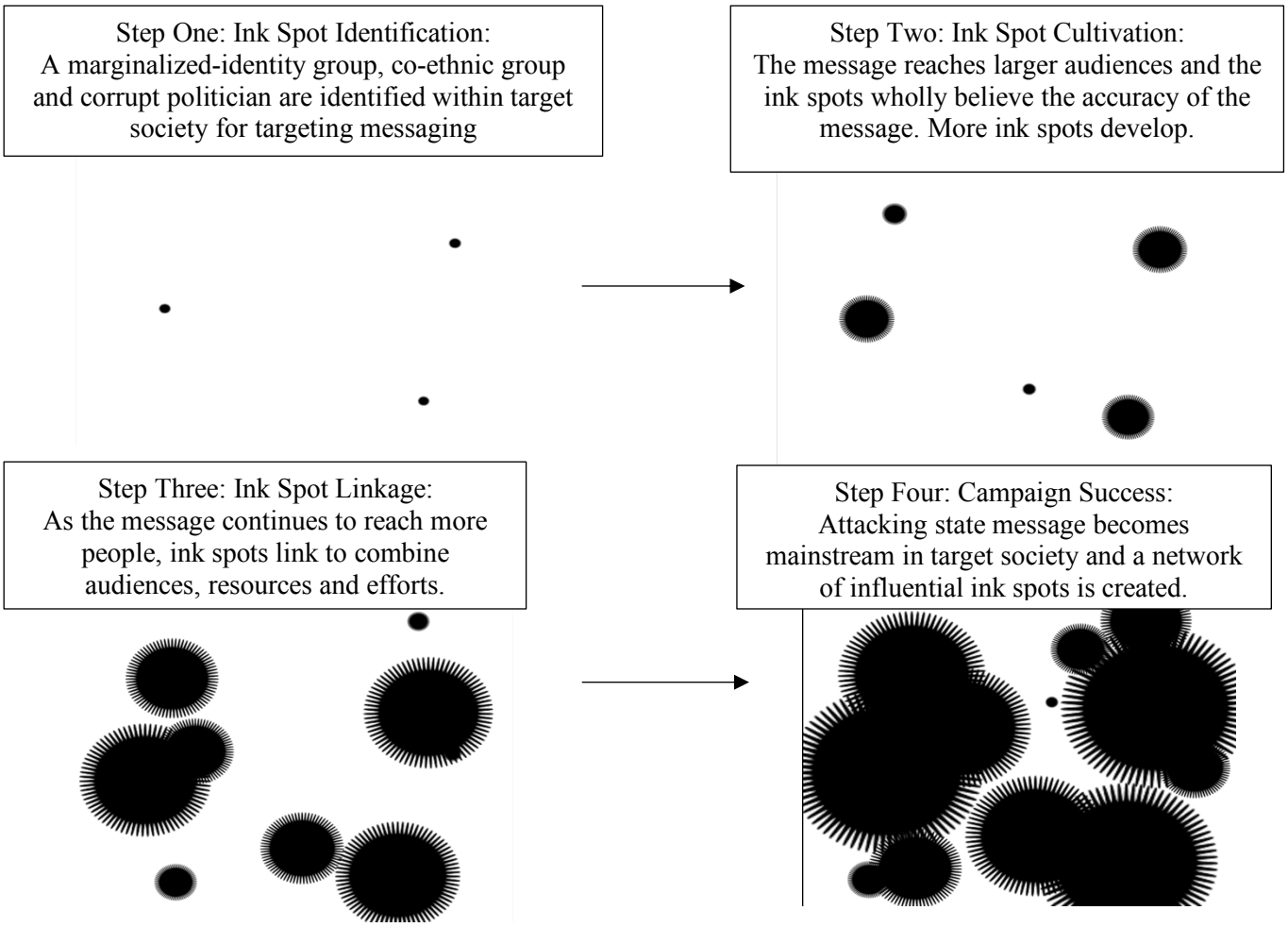
Finally, after the ink spots are sufficiently convinced of the message of influence and engage in political activity to change the status quo, disinformation campaigns create a network of ink spots through direct and indirect linkages. This network can be repeatedly tapped to promote different messages of influence within the society, as susceptible ink spots have already been identified and fortified, making the ink spots more vulnerable to different influence messages over time:

- *Direct Linkage.* Authoritarian regimes encourage further recruitment of individuals to the identity groups and directly connect like-minded politicians and identity groups, eliminating the collective action problem.[46] Through direct linkages, top-down traditional ink spots are included in the disinformation network.

- *Indirect Linkages.* Through the natural flow of information, smaller marginalized-identity ink spots combine with other spots over shared experiences or similar ideologies. In addition, as the message of influence reaches a successively larger audience, more individuals interact with the ink spots, allowing the influence narrative to grow.

The end goal of these campaigns is to gain enough political influence within the target society to enact change and create a permanent network that the attacking regime can continually tap into for different influence campaigns. Ink-Spot Disinformation is illustrated out below in Figure 2:

Figure 2: Ink-Spot Disinformation



As outlined above, authoritarian regimes seek out ink spots to act as hubs for networks of illiberalism within liberal democratic societies and as foundations for a permanent front against the target government. For bottom-up ink spots, authoritarian regimes target the collective value system, using false information and ideological persuasion to emphasize collective feelings of marginalization and encourage political action against the status quo. For top-down ink spots, authoritarian regimes target corrupt individuals using campaign financing, illicit funding protection, bribery, and blackmail to continue to gain influence within the target society. In most cases, the ink spots are unknowingly targeted and fortified by the authoritarian regime, particularly when the regime deploys fake news. Although the ink spots are continuously cultivated throughout the course of the attack, the attacking regime also encourages the establishment of new ink spots.[47]

Why are Liberal Democracies Vulnerable to Disinformation Ink Spots?

The current understanding of the vulnerabilities of liberal democracies is incomplete, and few frameworks exist to understand their weaknesses.[48] Many vulnerabilities to information warfare campaigns have been discussed individually; however, a comprehensive checklist of the inherent weaknesses of liberal democracies has not been provided. To identify, deter, and respond to foreign Ink-Spot Disinformation, the United States and other liberal democracies must understand the extent of their vulnerabilities.[49]

Vulnerability Checklist

The first set of liberal democratic vulnerabilities are response constraints, which prevent the government or liberal democratic society from retaliating against disinformation campaigns. Some response constraints are inherent to the specific laws within the liberal democracy, such as freedom of speech and right to privacy, which limit the government's ability to censor the populace or the media. Other response constraints vary based on the state, such as population size.

Liberal democracies have two categories of constraints to responding to Ink-Spot Disinformation.

1. Institutional vulnerabilities:

   Constitutional limitations. Liberal democracies are more vulnerable to Ink-Spot Disinformation if constitutions limit the government's ability to censor information, discredit the personal ideologies of citizens, or prevent societal polarization.[50]

   Corruption. Liberal democracies are more vulnerable to Ink-Spot Disinformation if public officials are economically or politically corrupt. More top-down targeting can occur when more individuals are corrupted, as the unvirtuous cycle operates best in highly corrupt societies.[51]

2. Tactical vulnerabilities:

   Small Relative Government. Liberal democracies are more vulnerable to Ink-Spot Disinformation if the state has a large population or covers large geographic area, as the government has less central control over the population.[52]

   Connection to the Attacking State. Liberal democracies are more vulnerable to disinformation campaigns if the state has connections to the attacking regime, such as close proximity, a significant co-ethnic diaspora, or a similar language or culture.[53]

The second set of liberal democratic vulnerabilities are target vulnerabilities. Some states have inherent social or economic conditions that are more susceptible to targeting in an Ink-Spot Disinformation campaign. To reiterate, authoritarian regimes target four types of ink spots: local

corporations seeking to establish financial ties with the regime, corrupt politicians, marginalized identity groups, and co-ethnic populations.

Liberal democracies have two categories of target vulnerabilities that advantage perpetrators of Ink-Spot Disinformation.

1. Societal vulnerabilities:

   Inherent Societal Factions. Liberal democracies are more vulnerable to Ink-Spot Disinformation when natural divisions already exist within the target society. Preexisting divisions within a state can be easily exploited to create polarization via a disinformation campaign. Societal factions include the existence of geographically concentrated marginalized populations, a history of civil war or past secessionist movements, any active secessionist movements or autonomous regions, and the existence of nationalist or populist movements.[54]

   Changing demographics. Liberal democracies are more vulnerable to disinformation campaigns when the demographic make-up of the society is in flux. Rapid change polarizes society between those who seek to maintain the status quo and those who accept new societal changes, allowing for societal exploitation by disinformation campaigns.[55] Demographic changes include high levels of migration, growing or shrinking religiosity, and an aging population.

2. Economic vulnerabilities:

   Current or recent recession. Following economic hardship, population groups in liberal democracies with fewer economic opportunities are more vulnerable to disinformation campaigns.[56]

   Reliance on information-based financial markets. Liberal democracies with economies that heavily rely on the free flow of truthful information are more vulnerable to disinformation campaigns.

   Transitioning economy. Liberal democracies with a transitioning economy, such as from manufacturing to services, are more vulnerable to a disinformation campaign. In transitioning economies, disinformation campaigns can exploit the population that is excluded due to lack of training, expertise, or education.[57]

   Increased economic connectivity with attacking state. Liberal democracies with financial and economic linkages with the attacking state are more vulnerable to disinformation campaigns. Economic interconnectivity enables traditional top-down disinformation.[58]

   Dependency on energy imports. Liberal democracies that import a large proportion of their energy resources are more vulnerable to disinformation. Most authoritarian regimes operate top-down disinformation campaigns using large state-run corporations, especially

energy corporations. Liberal democracies that are dependent on energy imports are more vulnerable to top-down targeting.[59]

Using the framework outline above, it is apparent why some liberal democracies are more vulnerable to disinformation campaigns than others. For example, Italy has freedom of press and speech, corruption, nationalist movements, high migrant populations, a history of secessionist movements, a weak economy, and imported energy dependence. Italy will be significantly more vulnerable than a country like Iceland, which has a small, homogenous centralized population, a strong economy, no past secession, and no blatant corruption. While Iceland is still vulnerable to disinformation campaigns in other ways, this checklist helps to identify countries that are most likely to succumb to Ink-Spot Disinformation.

Policy Recommendations

The key to combatting authoritarian-led Ink-Spot Disinformation is increasing the cost of the campaign for the aggressor. The high expense of traditional disinformation was one major reason that the Soviet Union failed to export the active measures model broadly during the Cold War. The cost of research, identification, messaging, and coordination was too high for most regimes without modern technology. However, with Ink-Spot Disinformation, countries can use the cheaper bottom-up approach, rather than the expensive traditional top-down approach.[60] If the United States can raise the cost of bottom-up disinformation, fewer countries will engage in Ink-Spot Disinformation and current information campaigns will shrink in capacity.

In light of liberal democratic vulnerabilities to Ink-Spot Disinformation, many scholars have proposed internal defensive solutions to prevent further successful targeting.[61] Common proposals to combating disinformation include education campaigns to teach the targeted populace about disinformation or tougher regulations on social media and technology companies to prevent false information from becoming widespread.[62] Other proposals focus on strengthening vulnerabilities, combatting local corruption, and using criminal and civil legal action to address internal weaknesses.[63] More drastic solutions call for significant policy changes, such as proposals for a censored or private internet, or a government-led domestic counter-information campaign, which would seek to identify ink spots and "de-radicalize" members before they are targeted by authoritarian regimes.[64]

However, to increase the cost of bottom-up Ink-Spot Disinformation, a counteroffensive disinformation campaign targeting the inherent vulnerabilities of authoritarian regimes should be considered.

Authoritarian states have significantly fewer response constraints than liberal democracies, as most authoritarian actors are willing and able to shut down the internet and censor the population. However, authoritarian regimes have vulnerable targets inherent in their structure that can be exploited and converted into liberal democratic ink spots. Authoritarian regime vulnerabilities are laid out below.

Authoritarian Institutional Vulnerabilities:

- *Corruption.* Authoritarian regimes are more vulnerable to disinformation campaigns if more public officials are economically or politically corrupt. More top-down targeting can occur when more individuals are corrupt, as the attacking regime can capitalize on influential individuals' self-interests in return for political favors.

- *Oligarchy or Single Party Government.* Authoritarian regimes with an oligarchy or non-meritocratic single-party government are more vulnerable to disinformation campaigns. Party infighting and internal power struggles create vulnerabilities within single party governments that can be exploited through disinformation to weaken the regime.[65]

- *Recent Elections.* Authoritarian regimes with recent elections are more vulnerable to disinformation campaigns. Newly elected leaders often lack the public legitimacy needed to govern, providing an opportunity for disinformation campaigns that emphasize the failures of the regime. In addition, if authoritarian leaders are reelected, public perceptions of corruption and election rigging can be exploited through disinformation.[66]

Authoritarian Tactical Vulnerabilities:

- *Weak Central Government.* Authoritarian regimes are more vulnerable to Ink-Spot Disinformation if the state has a large population or covers large geographic area, as the central government has less control over the population. While larger states with strong surveillance infrastructure, such as China or Russia, have largely addressed this vulnerability, other states, such as Iran, have difficulty maintaining centralized control over their periphery.

- *Connection to the Attacking State.* Authoritarian regimes are more vulnerable to disinformation campaigns if the state has connections to the attacking regime, such as proximity, a significant co-ethnic diaspora, or a similar language or culture. Shared language and culture prevent mistranslated messages of influence and a deeper understanding of nationalist or anti-government sentiments that can be exploited.

Authoritarian Societal Vulnerabilities:

- *Inherent Societal Factions.* Authoritarian regimes are more vulnerable to Ink-Spot Disinformation when divisions already exist within the target society. Preexisting divisions within a state can be exploited to create polarization by a disinformation campaign.

- *Changing demographics.* Authoritarian regimes are more vulnerable to disinformation campaigns when the demographic make-up of the society is in transition.

- *External Influencers.* Authoritarian regimes are more vulnerable to disinformation campaigns when the regime's legitimacy or authority is usurped by external actors. Third party influencers that threaten authoritarian regime legitimacy include disgruntled diaspora, political exiles, external religious authorities with domestic followers, and cults

of personality surrounding historical figures. Unlike liberal democracies, most authoritarian regimes have significant numbers of external actors with wide domestic support that can undermine the legitimacy of the regime, as authoritarian regimes tend to expel political dissidents.

Authoritarian Economic Vulnerabilities:

- *Rentier regime based on international markets.* Authoritarian regimes are more vulnerable to disinformation campaigns when the economy is dominated by a single export. Rentier states are highly dependent on information-based market fluctuations, creating opportunities for disinformation attacks to cause significant economic losses.

- *Current or recent recession.* Authoritarian regimes are more vulnerable to disinformation campaigns during a recession. Authoritarian regimes with centrally planned or controlled economies are significantly more vulnerable to economic hardship than liberal democracies, allowing disinformation campaigns to inflict larger costs on the authoritarian regime during a recession.[67]

- *Transitioning economy.* Authoritarian regimes with a transitioning economy, such as from manufacturing to services, are more vulnerable to a disinformation campaign.

- *Increased economic connectivity with attacking state.* Authoritarian regimes with financial and economic linkages with the attacking state are more vulnerable to disinformation campaigns. Centrally planned regimes are particularly susceptible to economic disinformation campaigns, as the reaction time of the economy is significantly slower than free markets.

These inherent vulnerabilities provide opportunities for the United States to operate an offensive disinformation campaign, raising the costs of authoritarian Ink-Spot Disinformation. While this approach is unlikely to completely prevent disinformation campaigns from targeting liberal democracies, higher social and economic expenses will limit the scope of further attacks. In addition, counter-disinformation campaigns will incentivize attacking regimes to negotiate a "cease-fire" where both the offensive and counteroffensive disinformation attacks stop, preventing the further spread of ink spots.

The key difference between an authoritarian offensive disinformation campaign and a liberal democratic counteroffensive is the ability of authoritarian regimes to bar access to the internet or retaliate against a social ink spot. As a result, liberal democracies must be aware of potential threats to domestic populations and avoid disinformation campaigns to provoke general chaos in authoritarian states. In order to protect populations and maximize costs to the regime, a combination of vulnerabilities should be used. For example, a disinformation campaign that sows discord amongst the political elite, promotes nationalism, and targets government data sources, should raise significant social, political and economic costs for attacking regimes, while maximizing external coverage of the regime's attempts to halt the creation of an ink spot network.

In addition, as more countries engage in disinformation campaigns, the threat of US-led disinformation campaigns will act as a deterrent to emerging authoritarian disinformation networks. Countries such as Vietnam and Guatemala have begun to explore disinformation campaigns, predominantly targeting political exiles abroad.[68] With the creation of successful counteroffensive practices, the United States can deter the use of Ink-Spot Disinformation in smaller regimes through the threat of increased costs.

Conclusion

Ink-Spot Disinformation offers a conceptual strategy for current technology-enabled disinformation campaigns based on target identification and exploiting inherent weaknesses within liberal democratic society. These campaigns are not limited to Russia. The model of Ink-Spot Disinformation has been exported to other authoritarian regimes, including Iran and China.[69] The Iranian government targets Arabs worldwide to highlight pro-Palestinian sentiments in mainstream news, which suggests that the Iranian regime under economic sanctions opts for the cheaper bottom-up approach to Ink-Spot Disinformation.[70] With authoritarian regimes around the world expanding their influence capabilities through strategic and technological advancements, liberal democracies are highly vulnerable to disinformation ink spots and have few options to prevent these attacks.

Retroactive and defensive measures to Ink-Spot Disinformation campaigns are not sufficient in preventing authoritarian influence within liberal democratic society. The United States should launch counter-offensive disinformation campaigns against authoritarian regimes that engage in Ink-Spot Disinformation in order to increase the social and economic cost of disinformation campaigns. Ultimately, authoritarian regimes will realize that widespread domestic dissent and economic failure at home reveal their own inherent vulnerabilities to disinformation, deterring further information warfare. By targeting inherent authoritarian weaknesses, counter-offensive disinformation campaigns can limit the scope of Ink-Spot Disinformation at home.

Acknowledgements

The author thanks Professor Amy Oakes, Professor Dennis Smith, COL Adrian T. Bogart, III, USA, and Nathan Liu for their helpful comments and edits that drastically improved this paper. In addition, support from Professor Paula Pickering, Gen. Mark Matthews, an anonymous contributor, U.S. Army Mad Scientist Team, COL Brad Duplessis, USA, CDR Daniel Orchard-Hayes, USN, and Joint Forces Staff College was crucial to the completion of this project. Finally, thank you to the Global Research Institute at William and Mary for their help in disseminating this project.

[1] David Douglas, Robert Hodson, Jonathan Czarnecki, and Adrian Bogart, "Multi-Domain Entropy," *Small Wars Journal* (July 19, 2017), accessed February 25, 2020, https://smallwarsjournal.com/jrnl/art/multi-domain-entropy.
[2] Tim Hwang, "Maneuver and Manipulation: On the Military Strategy of Online Information Warfare." *Strategic Studies Institute* (May 2019): vii, https://pdfs.semanticscholar.org/a721/f7191e9c0fb90706be070c6f65e02993745d.pdf
[3] "Even assuming that the cyber domain has yet to stop evolving, it is not clear that a classic strategic treatment of cyber war is possible, or, even if it were, it would be particularly beneficial." Martin C. Libicki, "Why Cyber War Will Not and Should Not Have Its Grand Strategist." *Strategic Studies Quarterly* 8, no. 1 (Spring 2014): 23, https://www.jstor.org/stable/10.2307/26270603.
[4] Seth G. Jones, *Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare,* (Washington DC: Center for International and Security Studies, 2018), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181002_Russia_Active_Measures_FINAL1.pdf?Ex9sT7k1B2w8lNPcs4cTrZwJcN1sT0.H; Keir Giles, "The Next Phase of Russian Information Warfare." *NATO Strategic Communications Centre of Excellence* (May 20, 2016), https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles; Steve Abrams, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," *Connections QJ* 15, no. 1 (2016): 5–31, http://dx.doi.org/10.11610/Connections.15.1.01.
[5] "Soviet Active Measures: Forgery, Disinformation, Political Operations," *Special Report no.88, Bureau of Public Affairs, United States Department of State* (October 1981): 1-4, https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf
[6] "Soviet Active Measures: Forgery, Disinformation, Political Operations," 2.
[7] "Soviet Active Measures: Forgery, Disinformation, Political Operations," 2.
[8] "World Federation of Trade Unions: Soviet Foreign Policy Tool," *Foreign Affairs Note, United States Department of State* (August 1983): 1-4, http://insidethecoldwar.org/sites/default/files/documents/Department%20of%20State%20Note%20World%20Federation%20of%20Trade%20Unions%20Soviet%20Foreign%20Policy%20Tool%20August%201983.pdf
[9] "Communist Interference in El Salvador," *Special Report no.80, Bureau of Public Affairs, United States Department of State* (February 23, 1981): 1-7, https://library.brown.edu/create/modernlatinamerica/wp-content/uploads/sites/42/2013/08/Special-Report-on-Communist-Interference-in-El-Salvador.pdf
[10] See for example Clint Watts' written statement prepared for the US Senate Select Committee on Intelligence. *Disinformation: A Primer In Russian Active Measures And Influence Campaigns: Statement Prepared for the Committee on Intelligence,* Senate, 165th Cong., 1st sess., March 30, 2017. https://www.intelligence.senate.gov/sites/default/files/documents/os-cwatts-033017.pdf.
[11] Jolanta Darczewska and Piotr Żochowski, "Active Measures: Russia's Key Export," *Point of View* no. 64 (June 2017), Centre for Eastern Studies (OSW); 8-12, https://www.osw.waw.pl/sites/default/files/pw_64_ang_active-measures_net_0.pdf
[12] Roland Heickero, "Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations," *Swedish Defense Research Agency (FOI)* (March 2010): 12-21. http://www.highseclabs.com/data/foir2970.pdf
[13] Abrams, "Beyond Propaganda," 8.
[14] The Primakov Doctrine provides the Russian understanding of the Post-Cold War world. In 1996, Russian Foreign Minister Evgenii Primakov promoted a multipolar world, stating that a US-led unipolar globe was "unacceptable" to the Russians. When coupled with the Gerasimov Doctrine, which promotes permanent ideological warfare with Russian adversaries, the Primakov Doctrine drives Russian foreign policy to use constant information warfare and hybrid warfare to undermine US hegemony and influence around the world.
Eugene Rumer, "The Primakov (not Gerasimov) Doctrine in Action," *Carnegie Endowment for International Peace*, June 5, 2019. https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254
[15] Ivo Juurvee, "The resurrection of 'active measures': Intelligence services as a part of Russia's influencing toolbox," *Strategic Analysis* (April 2018): 1–8, The European Centre of Excellence for Countering Hybrid Threats, 2, https://www.hybridcoe.fi/publications/strategic-analysis-april-2018-resurrection-active-measures-intelligence-services-part-russias-influencing-toolbox/.
[16] A full analysis of the psychology of active measures is beyond the scope of this study. Some scholarship about the psychological success of Soviet active measures includes topics such as directionally motivated reasoning, success of repetition, establishing echo chambers, implicit egotism, and narrative control. Directionally motivated reasoning

is the natural human tendency to seek true information without dramatically altering existing viewpoints. People are easily targeted by presenting false information that falls into pre-existing worldviews. D.J. Flynn, Brendan Nyhan, and Jason Reifler, "The Nature and Origins of Misperceptions: Understanding False and Unsupported Beliefs about Politics," *Political Psychology* 38, no. S1 (February 2017): 127–150, https://doi.org/10.1111/pops.12394; Ziva Kunda, "The Case for Motivated Reasoning," *Psychological Bulletin* 108, no. 3 (1990): 480–498, http://dx.doi.org/10.1037/0033-2909.108.3.480. Humans are more likely to believe something is true if it is repeated by multiple sources. Michael J Mazarr, Ryan Michael Bauer, Abigail Casey, Sarah Heintz, Luke J. Matthews, *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment,* RR-2714-OSD (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/pubs/research_reports/RR2714.html. People are increasingly walled off from one another, engaging only with content that fits cognitive predispositions and preferences. Active measures can easily manipulate these echo chambers. Shawn Powers and Markos Kounalakis, eds., "Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation," *U.S. Advisory Commission on Public Diplomacy* (May 2017): 4, https://www.hsdl.org/?view&did=800873. Implicit egotism is the tendency for recipients to more likely believe messages when they are being delivered by someone they perceive as being similar to themselves. Samantha M. Korta, "Fake News, Conspiracy Theories, and Lies: An Information Laundering Model for Homeland Security," *The Journal of the NPS Center for Homeland Defense and Security* (March 2018): 4, http://hdl.handle.net/10945/58322; Powers and Kounalakis, "Can Public Diplomacy Survive the Internet? Bots, Echo Chambers, and Disinformation," 21. Controlling and "winning" the mainstream narrative leads to the prominence of mainstream untrue narratives. Some untrue narratives create a confirmation bias, where a collective views the truth separately than the majority of the populace, leading to feelings of marginalization that are easily exploited. R.S. Zaharna, "Reassessing "Whose Story Wins": The Trajectory of Identity Resilience in Narrative Contests," *International Journal of Communication* 10 (2016): 4407–4438, https://ijoc.org/index.php/ijoc/article/viewFile/5121/1775.

[17] Abrams, "Beyond Propaganda," 13.

[18] "An extreme example of the gap between distribution of a message and the influence exercised by that message is Eastern Europe. After total control of the media for over 40 years, it is now apparent that Soviet propaganda has not had an enduring impact on public attitudes in Eastern Europe toward the Soviet Union. In retrospect, it can now be viewed as only a useful adjunct to Soviet power in maintaining control over the population. Again, one must conclude that actions speak louder than words." Richards J. Heuer, Jr., "Assessing Soviet Influence Operations" (unpublished study for intelligence analysts, May 1990), 25, http://www.pherson.org/wp-content/uploads/2013/06/07.-Assessing-Soviet-Influence-Operations_FINAL.pdf.

[19] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," *Institute for National Strategic Studies, Strategic Perspectives*, no. 11 (June 2012): 63, https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-11.pdf.

[20] Office of the Director of National Intelligence, *Joint Statement from the ODNI, DOJ, FBI and DHS: Combating Foreign Influence in U.S. Elections,* October 29, 2018, https://www.dni.gov/index.php/newsroom/press-releases/item/1915-joint-statement-from-the-odni-doj-fbi-and-dhs-combating-foreign-influence-in-u-s-elections.

[21] Heuer, "Assessing Soviet Influence Operations," 3.

[22] Walter Isaacson, "How to Fix the Internet: Anonymity has poisoned online life," *Atlantic,* December 15, 2016, https://www.theatlantic.com/technology/archive/2016/12/how-to-fix-the-internet/510797/; L. Jean Camp and Y.T. Chien, "The internet as public space: concepts, issues, and implications in public policy," *ACM SIGCAS Computers and Society* 30, no. 3 (September 2000): 13–19, https://doi.org/10.1145/572241.572244.

[23] Mazarr et al., "The Emerging Risk of Virtual Societal Warfare," 65.

[24] Matt Chessen, "Understanding the Psychology behind Computational Propaganda," *U.S. Department of State* (May 2017); 19–22. https://www.hsdl.org/?abstract&did=800873.

[25] Peter M. et al., "Combatting Targeted Disinformation Campaigns: A Whole-of-Society Issue," *Department of Homeland Security's Public-Private Analytic Exchange Program* (October 2019): 10–14, https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.

[26] Clint Watts, "So What Did We Learn? Looking Back on Four Years of Russia's Cyber-Enabled 'Active Measures'," *Alliance for Securing Democracy* (January 18, 2018), https://securingdemocracy.gmfus.org/so-what-did-we-learn-looking-back-on-four-years-of-russias-cyber-enabled-active-measures/.

[27] Rory Cormac and Richard J. Aldrich, "Grey is the new black: covert action and implausible deniability," *International Affairs* 94, no. 3 (May 2018): 477–494, https://doi.org/10.1093/ia/iiy067.

[28] One example of Russian-led disinformation that led to mainstream narrative control: Jade Helm conspiracies led to the Texas governor using state militias to oversee US military training operations. Dan Lamothe, "Remember Jade Helm 15, the controversial military exercise? It's over," *Washington Post*, September 14, 2015, https://www.washingtonpost.com/news/checkpoint/wp/2015/09/14/remember-jade-helm-15-the-controversial-military-exercise-its-over/. Another example: an incendiary article highlighting racial differences at a Black Lives Matter rally. "Tensions at rival White & Black Lives Matter protests flare in Houston (VIDEO)," *RT*, October 2, 2016, https://www.rt.com/usa/361346-blm-wlm-protests-houston/.
[29] "Strategy for Victory in Iraq: Clear, Hold, and Build," *Office of the Press Secretary, The White House* (March 20, 2016,) https://2001-2009.state.gov/p/nea/rls/63423.htm.
[30] Heather Conley et al., *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Washington DC: Center for Strategic and International Studies, 2016), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/1601017_Conley_KremlinPlaybook_Web.pdf; Alina Polyakova et al., *The Kremlin's Trojan Horses* (Washington DC: Atlantic Council, 2016), https://www.atlanticcouncil.org/in-depth-research-reports/report/kremlin-trojan-horses/
[31] Heather Conley et al., *The Kremlin Playbook 2: The Enablers* (Washington DC: Center for Strategic and International Studies, 2019), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190326_KP2.pdf; Conley et al., *The Kremlin Playbook,* 17–21.
[32] Peter Pomerantsev and Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money* (New York: Institute of Modern Russia, 2014), 22, http://www.interpretermag.com/wp-content/uploads/2014/11/The_Menace_of_Unreality_Final.pdf
[33] Conley et al., *The Kremlin Playbook,* 17–21.
[34] Alina Polyakova et al., *The Kremlin's Trojan Horses 2.0: Russian Influence in Greece, Italy, and Spain* (Washington DC: Atlantic Council, 2017), https://www.atlanticcouncil.org/in-depth-research-reports/report/the-kremlin-s-trojan-horses-2-0/.
[35] See for example Alina Polyakova's written testimony to the US House Committee on Appropriations. *United States Efforts to Counter Russian Disinformation and Malign Influence: Testimony to the Committee on Appropriations' Subcommittee on State, Foreign Operations, and Related Programs*, House, 116th Cong., 1st sess., July 10, 2019, 1. https://www.brookings.edu/testimonies/u-s-efforts-to-counter-russian-disinformation-and-malign-influence/
[36] W. Lance Bennett and Steven Livingston, "The disinformation order: Disruptive communication and the decline of democratic institutions," *European Journal of Communication* 33, no. 12 (2018): 122–139, SAGE, https://doi.org/10.1177/0267323118760317.
[37] Fukuyama (2019) discusses the nature of polarization in US society, specifically that two forms of identity politics have arisen: politics that demand recognition of dignity of individuals and politics that demand recognition of dignity of collectives. The dignity of collectives is key to understanding targeting. Following the decline of religion as the dominant value system for a majority of Americans, a cacophony of moral systems emerged, causing many individuals to seek a collective with similar morals. However, due to the multitude of value systems within US society, many of these collectives felt marginalized, where the lack of recognition for their perceived ability to make good moral decisions led to feelings of shame and unfairness. As a result of the feelings of societal mistreatment, nationalism begins to develop, as the collective experiences intense nostalgia for a strong imagined community where the divisions and confusions of pluralist modern society do not exist. Francis Fukuyama, *Identity: The Demand for Dignity and the Politics of Resentment,* (New York, NY: Farrar, Straus and Giroux, 2018).
[38] Andrei Soldatov and Irina Borogan, *The Compatriots: The Brutal and Chaotic History of Russia's Exiles, Émigrés, and Agents Abroad* (New York, NY: PublicAffairs, 2019), 21.
[39] Few other strategic frameworks exist for disinformation; however, Hwang's Information Warfare by Maneuver follows a three-step approach to modern information warfare. Firstly, successful campaigns practice Effective Obfuscation, where the campaigns maintain low profiles and are challenging to detect. Secondly, campaigns practice Effective Iteration, where successful campaigns are highly adaptive, decentralized and agile to navigate chaotic noise of cybersphere. Finally, modern disinformation campaigns practice Effective Automation, where successful campaigns capitalize on mechanization of the internet and utilize algorithms and artificial intelligence to identify potential targets and expand operational capacity. While Information Warfare by Maneuver is very sensical, increased stealth, adaptability and mechanization have all been tenets of warfare before the existence of cyberspace. This strategic framework does not successfully address identifying targets, campaign goals or unique characteristics

of information campaigns. However, Hwang's framework is helpful for understanding how information campaigns work and which regimes will be most successful at utilizing disinformation campaigns. Hwang, "Maneuver and Manipulation."

In addition to Hwang's framework, the leading source for modern Russian information theory is the Gerasimov doctrine, a 2016 article written by Russian General Valery Gerasimov. In this short article, Gerasimov outlines "modern war" and emphasizes the use of "non-military means to achieve political and strategic goals." Gerasimov also highlights a simultaneous ongoing war in all realms, including the information space multiple times, intending to create a permanent front: "Among such actions are the use of special operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected."

This quote highlights the Russian thought process surrounding information warfare: there is no peacetime and information warfare must be constantly updated in order to create a functioning permanent "front" or fifth column within the target country. The Gerasimov Doctrine allows some insight into the Russian model, yet remains too vague to apply to a true strategic framework. Valery Gerasimov, "The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military Review* 96, no. 1 (January-February 2016): 25, https://jmc.msu.edu/50th/download/21-conflict.pdf.

The final strategic framework of disinformation is the concept of "Net-war." Initially discussed by Arquilla and Ronfeldt, Hwang also discusses the importance of Net-war as a strategic concept at the turn of the century. "Net-war" seeks to "disrupt, damage or modify what a target population knows or thinks it knows about itself." As a result, engaging in Net-war is engaging in information warfare, specifically targeted at certain populations rather than an en-masse general disinformation campaign. Like modern information warfare, the beginning or end of net-wars are unclear and easily outmaneuver hierarchical structures through their decentralized networks of dispersed, yet interconnected nodes. In sum, net-war has no central organizer or leader, but maintains the fog of war and anonymity through a vast network of attackers. The main key for each of these strategic frameworks is technology. Net-war argues that technology creates a new form of warfare, unlike anything we've seen before. Gerasimov argues that technology provides new opportunities for utilizing existing strategic frameworks. Hwang calls for the combination of theory and technology to create the most successful attacks. As mentioned above, this paper argues that old measures combined with new technology create the structure of information warfare; however, the key to a successful campaign is successful targeting. John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (Spring 1993): 141–165.

[40] David Ucko, "Clear-Hold-Build-Fail? Rethinking Local-Level Counterinsurgency," *War on the Rocks*, November 7, 2013. https://warontherocks.com/2013/11/clear-hold-build-fail-rethinking-local-level-counterinsurgency/.

[41] The Identify-Cultivate-Link framework is the disinformation equivalent of "clear-hold-build," drawing from similarities between territorial ink spots under the counter-insurgency framework and societal ink spots under the disinformation framework.

[42] Christopher Paul and Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, PE-198-OSD (Santa Monica, CA: RAND Corporation, 2016), https://www.rand.org/pubs/perspectives/PE198.html.

[43] Russian Intelligence Services (RIS) and organized Russian "troll farms" have participated in identifying vulnerable targets for disinformation campaigns through intelligence gathering operations regarding identity groups, corporations and politicians. Other states' intelligence agencies likely participate in similar actions in other authoritarian disinformation campaigns. Juurvee, "The resurrection of 'active measures'," 3; Vera Zakem et al., *Mobilizing Compatriots: Russia's Strategy, Tactics, and Influence in the Former Soviet Union*, ADA626362 (Arlington, VA: Center for Naval Analyses, 2015), n.p., https://www.cna.org/CNA_files/PDF/DOP-2015-U-011689-1Rev.pdf.

[44] Michael Isikoff, interview by Steve Inskeep, *Morning Edition*, National Public Radio, July 11, 2019, https://www.npr.org/2019/07/11/740608323/the-origins-of-the-seth-rich-conspiracy-theory.

[45] Gabriel Gatehouse, "Marine Le Pen: Who's funding France's far right?" *BBC News*, April 3, 2017, https://www.bbc.com/news/world-europe-39478066.

[46] Disinformation campaigns link identity groups together in order to more effectively change the status quo. While not all ideologies may not be collectively shared, the change in status quo is a collective goal for each identity group. As a result, while direct linkages help the identity groups achieve their individual goals and overcome the collective action problem, disinformation messaging is also furthered, as the messages reach a larger audience.

[47] New ink spots are created through fake news shared between an existing ink spot and another previously unidentified group, through business ventures between economic ink spots and unidentified targets or through the splintering of old ink spots.
[48] For one example of an existing framework for democratic weaknesses, see Hwang, "Maneuver and Manipulation," 51.
[49] For a case study of vulnerabilities in Southern Europe, see Polyakova et al., *The Kremlin's Trojan Horse 2.0*.
[50] Jill I. Goldenziel and Manal Cheema, "The New Fighting Words? How U.S. Law Hampers the Fight Against Information Warfare," *University of Pennsylvania Journal of Constitutional Law* 22, no. 1 (November 2019). 81–170, https://ssrn.com/abstract=3286847.
[51] Conley et al., *The Kremlin Playbook*, 17–21.
[52] Bayer et al., *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*, PE 608.864 (Brussels: European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, 2019), http://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf
[53] Liberal democracies are more vulnerable to information campaigns when the attacking regime and the target regime have a shared language or culture.
[54] The existence of marginalized groups creates natural divisions within a populace, due to racism, perceived unfairness and nationalist sentiments. States with natural societal divisions between concentrated ethnic groups or other marginalized minorities will be more at risk of a successful foreign information campaign targeting that group and further polarizing existing splits.
Past secessionist movements or civil wars show inherent divisions within a state that will continue to permeate through all levels of society and can be easily exploited to create polarization by an information campaign. Aaron Spitler, *Rewriting the Past, Remaking the Present: Historical Narratives in Russian Disinformation Campaigns* (Williamsburg, VA: The Project on International Peace and Security), https://www.wm.edu/offices/global-research/projects/pips/white_papers/spitler_final.pdf.
Ongoing secessionist movements and autonomous regions show a failure to maintain a single national identity and highlight societal divisions ripe for exploitation.
[55] Frederick C. Turner, "The Implications of Demographic Change for Nationalism and Internationalism," *The Journal of Politics* 27, no. 1 (February 1965): 87–108, https://www.jstor.org/stable/2128002.
[56] James D. Fearon and David D. Laitin, "Ethnicity, Insurgency, and Civil War," *American Political Science Review* 97, no. 1 (February 2003): 75–90, https://www.jstor.org/stable/3118222.
[57] OECD, *Regions in Industrial Transition: Policies for People and Places* (Paris: OECD Publishing, 2019), https://www.oecd.org/cfe/regional-policy/Draft_policy_highlights_RIT_FINAL.pdf.
[58] Conley, *The Kremlin Playbook 2*.
[59] Polyakova et al., *The Kremlin's Trojan Horses 2.0.*
[60] Paul Mozur, "A Genocide Incited on Facebook, With Posts From Myanmar's Military," *New York Times*, October 15, 2018, https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html.
[61] Daniel Funke and Daniela Flamini, "A guide to anti-misinformation actions around the world," The Poynter Institute, last modified August 13, 2019, https://www.poynter.org/ifcn/anti-misinformation-actions/.
[62] Darrell M. West, *How to combat fake news and disinformation* (Washington DC: Brookings Institution Center for Technology Innovation, 2017), https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/
[63] Conley, *The Kremlin Playbook,* 26–35.
[64] Matt Burgess, "To fight fake news on WhatsApp, India is turning off the internet," *Wired*, October 18, 2018, https://www.wired.co.uk/article/whatsapp-web-internet-shutdown-india-turn-off.
[65] Anthony Nadler, Matthew Crain, and Joan Donovan, "Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech," *Data and Society Research Institute* (October 2018,) 1-5, https://datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf
[66] Joakim Ekman, "Political Participation and Regime Stability: A Framework for Analyzing Hybrid Regimes," *International Political Science Review*, Vol. 30, No.1 (January 2009), 7-31, https://www.jstor.org/stable/pdf/20445173.pdf?refreqid=excelsior%3A12beb749a279e126b7e13c2e22895365
[67] Robert H. Dix, "The Breakdown of Authoritarian Regimes."
The Western Political Quarterly 35, no. 1 (December 1982): 554–573, https://www.jstor.org/stable/447341.

[68] Samantha Bradshaw and Philip N. Howard, "The Global Disinformation Order," *Computational Propaganda Research Project*, (Oxford, UK: University of Oxford, 2019.)
[69] Ariane M. Tabatabai, "A Brief History of Iranian Fake News," *Foreign Affairs*, August 24, 2018, https://www.foreignaffairs.com/articles/middle-east/2018-08-24/brief-history-iranian-fake-news.
[70] Jack Stubbs and Christopher Bing "Special Report: How Iran spreads disinformation around the world," *Reuters*, November 30, 2018, https://www.reuters.com/article/us-cyber-iran-specialreport/special-report-how-iran-spreads-disinformation-around-the-world-idUSKCN1NZ1FT