Tactics and Techniques of Information Operations: Gaps in US Response to Counter Malign Influence

Nicholas Harrell[1], Alexander Master[2], Nicolas Starck[2] and Daniel Eerhart[2]
[1]Purdue University, USA
[2]Army Cyber Institute, USA

nharrel@purdue.edu
alexander.master@westpoint.edu
nicolas.starck@westpoint.edu
daniel.eerhart@westpoint.edu

Abstract: The modern information environment has transformed the dynamics of international conflict and politics. A byproduct of the capabilities offered by ubiquitous hyperconnectivity is continuous efforts by state and non-state actors to shape, manipulate, distort, or exploit information to influence public perception. These operations can deliberately disrupt social cohesion or undermine the stability and security of governments and societies. A thorough understanding of modern information threats is necessary to maintain the rules-based international order. Information threats (e.g., campaigns spreading false health information, exacerbation of domestic social issues, attacks on national reputation) aim to sow distrust and discord to gain a competitive advantage. Over the past two decades, US government agencies have been forced to modify outdated policies to counter information threats, often with mixed results. Despite recent academic frameworks and policy efforts to address information threats, gaps remain in addressing those that cross authorities, disciplines, and boundaries by their nature. This survey systematizes the tactics and techniques used in the conduct of information operations. We then present case studies to elucidate gaps and align the features of information operations against current US counter malign influence policies.

Keywords: Information threats, Influence, Information operations, Taxonomy

1. Introduction

The adoption of information operations as a central component of malign actors' operations has increased the relevance of information operations for national security. However, detection of information operations is challenging and resource intensive in the ubiquitous and noisy information environment (IE). Although United States (US) companies continue to drive the growth of pervasive digital connectivity, there remains a limited capacity for governmental entities to manage information flows and disrupt the cascading spread of disinformation. International cooperation has been an increasingly important factor of success in recent years, as demonstrated by information campaign activity during the initial invasion of Ukraine in 2022 (Fick, 2023; Creed, R. and Flynn, M., 2024). We have witnessed how the US and Western European countries provide ongoing technical support for combating malign influence activity on the Internet. However, rapid advancements in generative artificial intelligence technologies that mimic language, voice, and visual content will likely lead to an insurmountable amount of noise in the IE, making detection challenging and costly. The fear of synthetic media (often dubbed "deepfakes") is evident in journalistic news coverage, with cases of criminals exploiting these technologies for nefarious intentions and national security experts frequently addressing information campaigns in the media (Mueller, J. and Gans, J., 2023). These novel technologies contribute to the challenges, and a lack of adequate language to describe information operations in national security policy also reduces the ability of nations to identify and counter information operations. Formalizing a taxonomy to identify and describe the fundamental features of information operations in the modern IE is necessary for effective national security policy and to address their use by malign actors.

The ability to generate unrest and confusion in discourse is enticing to nefarious actors. John Lansing, Director of the US Agency for Global Media highlighted in a House Appropriations Committee: "We are living through an explosion of disinformation, lies, and distortion spread by those very same authoritative regimes that our networks report on...by my observations, Russia's goal is to destroy the very idea of an objectionable, verifiable, set of facts. ... where nothing is empirically truthful, any lie will do. And if everything is a lie, the biggest liar wins" (House Appropriations Committee, 2024). The US uses international news stations through radio and satellite as one approach to combat malign foreign influence. The US has created several international media networks to address censorship and influence challenges, allowing citizens living under authoritative regimes to get alternative perspectives to their home nation's censored media (Osipova-Stocker, 2022). However, few efforts focus on dismantling the nefarious coordinated operations that use democratized media networks as their

"roadways." Many of these operations involve information threats by foreign entities, aiming to sow distrust and discord and gain a competitive advantage.

Contributions. Using information laundering as a lens of evaluation, we characterize the actors, tactics, and techniques used in contemporary information campaigns. We organize the survey outputs into a taxonomy of information laundering. We then use case studies to demonstrate validity of the taxonomy, while illuminating gaps in US response actions to malign information proliferation.

2. Background

Codified institutional information operations sub-agencies are not a new concept among Western governments. While the IE has played a pivotal role in all Western conflicts, World War I served as the first case study in systemized government information and influence activities, with the establishment of the Committee on Public Information (CPI) in 1917. During World War II (WWII), the Office of War Information (OWI), the Office of Strategic Services, and the Psychological Warfare Division continued to evolve and improve their ability to influence strategic objectives in the IE. The Trout Memo inspired Operation Mincemeat and featured 54 deception tactics designed to mislead adversaries. In retrospect, the Trout Memo serves as a turning point for disinformation activities, where, suddenly, deception can serve as a core strategy for achieving strategic objectives.

NATO did not formally codify information operations within its doctrine until the mid-1990s; however, many examples of information operations tactics used by the United Kingdom (UK) and the US in WWII (Hutcherson, 1994, Army Field Manual 100-6, 1996). The UK established the Special Operations Executive (SOE) in 1940 to conduct espionage, sabotage, and propaganda campaigns in occupied Europe (Seaman, 2013). Their tactics consisted of disseminating fake news and rumors to demoralize German troops and civilians. "Black propaganda" consisted of efforts to discredit Axis powers through fake radio broadcasts or counterfeit materials. The Political Warfare Executive (PWE), which cooperated with the SOE, broadcasted fake German media that undermined German military leadership (Lopez, 2020). The US created the OWI to design posters, films, and radio broadcasts to discredit foreign broadcasts and boost morale (National Archives and Records Administration., 1941-47). Joint deception efforts, such as leaflet drops over North Africa and Italy and Operation Fortitude leading up to D-Day, aimed to create confusion. The mentioned organizations eventually became more formalized during the establishment of NATO in 1949. It provided a platform for coordinated efforts to combat Soviet narratives during the Cold War, with initiatives like Radio Free Europe/Radio Liberty in 1950 and the Public Diplomacy Division (PDD) in the 1960s (Johnson, 2012). While these formal efforts by the US proved useful at the time, the IE and the nature of information threats evolved - while the organizations and concepts within the US government remained stagnant.

Technological advancements have changed the structural dynamics and scale of threats in the IE. During the Vietnam War, the North Vietnamese used multi-pronged disinformation campaigns to build a negative sentiment among South Vietnamese about American Imperialism (Flammer, p. 206-213, 1973). These sentiments spread by television, radio, and then word-of-mouth. Comparatively, the 2023 Israel-Hamas conflict demonstrated how a single adverse action caught on video can be propagated across social media platforms without international boundaries. In the current environment, smaller news websites, pseudo-news sites, and fake news sites proliferate the world wide web (Korta, 2018). In 2024, over half of US adults were reported as receiving some form of their news on social media ("Social Media and News Fact Sheet", 2024). The Internet and social media platforms have made reaching audiences easier and less costly than ever before. Bots and trolls masquerading as legitimate users only require a computer and an Internet connection.

Cambridge Analytica, a firm known as one of the most prominent pioneers of microtargeting (Wylie, 2019), demonstrated how psychometric profiling can be used to influence public opinion. Similarly, Russian propaganda groups paid for Facebook advertisements to publish US election-related ads targeting specific focus groups.[1] While the US has identified the threats of malign information campaigns following the attention on the IRA's operations, nation-state tactics have only evolved into more sophisticated attacks in recent years. For example, in African nations like Burkina Faso and Mali, Russian forces have begun hiring real, local citizens to spread disinformation on their authentic social media accounts, using the local language and dialect, avoiding some of the mechanisms used to detect influence networks during the 2016 US Election (Peltier, E., 2024). The evolution

[1] https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html

in threat tactics in the IE has outpaced the doctrine and organizational structures within the US intended to address these threats.

2.1 Problem Space

Malign foreign influence persists due in part to systemic issues. First, commercial entities like social media networks are integral to Western markets, providing numerous jobs and economic stability. However, gaining access to these entities for use in propagating messages is trivial, allowing malign actors to prevail. Second, many US citizens perceive the ability to express themselves on these platforms freely as a fundamental constitutional right, which challenges the US government from intervening in malign and nefarious activities – for fear of a perception of government censorship (Master and Garman, 2023). Succeeding in the IE is critical to achieving national security objectives. This demand raises the importance of how nation-states define, organize, and engage in operations in the IE.

3. Methodology

The guiding research question for this study was: Does the United States' approach to defining, organizing, and mitigating malign information operations create opportunities that its adversaries can exploit? Our methodology consisted of a narrative literature review to analyze the current body of knowledge relating to information operation techniques through the conceptual lens of information laundering. We chose this theoretical framework based on its capability of capturing global and regional intermediaries related to influence campaigns. The tactics and techniques identified during the review were used to analyze and articulate the threats in the chosen use cases. By decomposing elements of the use cases into a structured analysis, we extract a hierarchical taxonomy that demonstrates different domains of components involved in these campaigns.

4. Survey of Elements of Information Campaigns

4.1 Hybrid Warfare

Hybrid warfare, which shares similar tactics in military doctrine consisting of irregular war and counterinsurgency, is an operational framework that supports nation-states' higher-level strategic initiatives. Hybrid warfare can be defined broadly as a domain of tactics that are utilized by nation-states and large entities to circumvent legal frameworks and exert influence over their adversaries without escalating a large conflict (Chivvis, 2018).

Russia's information strategy outside Western countries is to propagate anti-west rhetoric. Moscow finds it more conducive to engage with local "bosses and kingpins" based on enduring personal loyalties (Marten, 2019, pp. 155-170). This strategy serves a broader economic agenda for Russia, which is grappling with stagnation and the threat of an impending recession. By enhancing its reputation in regions with limited Western influence, Putin aims to diversify Russia's economic portfolio and mitigate the impact of financial challenges (Marten, 2019, pp. 155-170).

4.2 Coordinated Inauthentic Behavior

Coordinated Inauthentic Behavior pertains to information threats that use a large complex network of bots and trolls to increase the reach and dissemination of certain content. These messages are legitimized through automation, such as fake news sites, bots, and troll networks (Weber & Neumann, 2021). We see other terminology like these efforts in strategic research initiatives (e.g., NATO Stratcom) defined as information laundering (Rodriguez, Information Laundering in Germany, 2020). Information laundering pertains to the broader IE and not just social media.

4.3 Information Laundering

Information laundering provides a framework for identifying the actors, tactics, and techniques of information campaigns. Information laundering is the process of flooding the IE with an abundance of slightly altered media to build authenticity (Klein, 2012), and filtering information through intermediaries to obscure the source of information. The framework is pragmatic and can be used to analyze individual and regional events. The extended Information Laundering framework (Rodriguez, Information Laundering in Germany, 2020) captures many of the tactics identified in disjoint literature, providing the best baseline for developing a taxonomy. The study will primarily employ the framework developed by Rodriguez (Rodriguez, Information Laundering in Germany, 2020) while also integrating key definitions and concepts from seminal works to offer a comprehensive understanding of the subject (Rodriguez, Information Laundering in Germany, 2020). In this

study, we emphasize the importance of viewing information laundering as a critical component of information campaigns within hybrid warfare.

Rodriguez integrated concepts from several authors to provide a more comprehensive set of techniques and indicators across distinct phases of information propagation (Rodriguez, Information Laundering in Germany, 2020; Meleshevich & Schafer, 2018, Puschmann et al., 2016, pp. 143-150). The foundation for the concept of information laundering originated from a nuanced lexicon for the actors involved in social media-based information laundering, drawing analogies to financial money laundering (Meleshevich & Schafer, 2018). Other work emphasizes the roles of enablers, accelerators, and amplifiers during the layering phase (Korta, 2018). While these works were useful contributions, they focused on computational means and failed to provide a comprehensive framework for modern information operations. The extended information laundering framework offers the most extensive foundation for assessing modern information operations by introducing a singular cohesive framework that encompasses the essential concepts from these previous works. Rodriguez demonstrated the applicability of the extended framework by applying it to the assessment of multiple Russian information operations against distinct targets in the Baltic States and Germany (Information Laundering in the Nordic-Baltic Region, 2020; Rodriguez, Information Laundering in Germany, 2020). This study offers further refinements to the taxonomy in the extended information laundering framework and demonstrates its applicability for assessing the posture of the US towards information threats.

4.3.1 Phases

The literature identifies the three phases of information laundering — placement, layering, and integration — which are analogous to money laundering phases (Korta, 2018). While these are presented as distinct phases, the role of chance and human error can result in the unintentional or simultaneous completion of phases (Information Laundering in Germany, 2020).

The placement phase initiates the information laundering process. Notably, the information laundering framework presumes the existence of curated content or a narrative that a threat is attempting build legitimacy within the public. The targeted identification or development of that content is outside the scope of this assessment. Instead, information laundering focuses on the placement of that content where it will gain the most legitimacy with the target audience.

A divergence in the literature pertains to the relevance of the technical cyberspace means associated with placement. Some authors focus on computational techniques such as site impersonation, domain spoofing, fraudulent document modification, and account takeover as critical to the identification and tracking of information operations (Korta, 2018; Farwell, 2014). These authors argue that leveraging legitimate sources as one of the most effective ways to achieve virality, or high user engagement, and popularity when disseminating information online (Korta, 2018). Others argue that identifying structural features and similarities of campaigns without a focus on technical means is a more effective approach. This literature divergence is also relevant given the prominence of the cyberspace domain in the modern IE. The US considers the cyberspace domain as a subcomponent of the IE. Therefore, having an accurate understanding of the dynamics and an appropriate taxonomy for the cyber components of information operations is crucial for the US to respond to information threats effectively.

The layering phase involves synchronizing propagation techniques with significant events like natural disasters, war, conflict, or protests (Rodriguez, Information Laundering in Germany, 2020). The concept of “accidental actors,” individuals who unwittingly contribute to the spread of harmful information, adds unpredictability to the outcomes (Rodriguez, Information Laundering in Germany, 2020).

In the integration phase, success is defined as the penetration of misleading information into legitimate discourse (Rodriguez, Information Laundering in Germany, 2020). The literature overlooks post-integration detection, focusing instead on achieving authenticity. The prevalence or frequency of sharing information is a positive sign of successful integration (Rodriguez, Information Laundering in Germany, 2020).

4.3.2 Spreaders

This classification framework is essential for understanding the entities and roles involved in information laundering to influence public perception. For information to achieve maximum potential spread, there are various entities within the IE that facilitate the dissemination of information. This study categorizes these entities into enablers, accelerators, amplifiers, and proxies (Korta, 2018; Rodriguez, 2020; Meleshevich & Schafer, 2018). These roles can be fulfilled by individuals, organizations, and technical systems. It is also useful to identify the

various properties of these entities, such as their locality or authority, which affect the available means of mitigation.

4.3.3 Enablers

Enablers serve as the foundational platforms where information is initially disseminated. According to Korta (2018), the Internet can be segmented into four types of enablers:

- Discover: Search engines that help users find information.
- Information: Platforms like news websites and research journals.
- Opinion: Blogs and discussion forums.
- Expression: Social networks, online shopping, and gaming platforms.

Intuitively, we can see the level of interaction, such as two-way communication, purpose, and statefulness, dictate the categories of enablers. Korta (2018) emphasizes the complexity of tracking propaganda across these platforms due to their interconnected nature. Rodriguez corroborates this by illustrating the complexity through multiple use cases (Rodriguez, Information Laundering in Germany, 2020).

4.3.4 Accelerators

Accelerators are mechanisms that exploit the characteristics of enablers to increase the reach or virality of information. Korta (2018) identifies four sub-categories:

- Echo Chambers: Communities that reinforce existing beliefs.
- Filter Bubbles: Similar to echo chambers, these communities have limited exposure due to platform algorithms.
- Advertising: Paid promotions to targeted audiences.
- Computational Propaganda: Automated systems designed to disseminate information.

While Meleshevich & Schafer (2018) attempt to frame these accelerators using money laundering terminology, Korta (2018) offers a more modern and relevant classification, making it a more suitable reference for this study.

Accelerators can be further divided into passive and active types. Like echo chambers, passive accelerators enhance narratives without direct intervention from the disseminators. However, active accelerators involve deliberate targeting through computational propaganda and online advertising (Korta, 2018). From Korta (2018), we see that computational propaganda assumes the use of bot networks.

4.3.5 Amplifiers

Amplifiers are unique entities that do not create content but significantly contribute to spreading information. Korta (2018) identifies two types:

- Ideologically Motivated Amplifiers: Entities that align with the launderer's objectives to sow discord or confusion.
- Financially Motivated Amplifiers: Entities that aim to profit from the spread of information without ideological alignment.

4.3.6 Proxies

Proxies denote actors disseminating pro-state media without being original content creators. Additionally, "accidental actors" are those who inadvertently contribute to spreading laundered information without explicit involvement. Determining intent (accidental or intentional) is complex, so such actors will be broadly categorized as "proxy actors."

While literature elaborates on the role of bots in facilitating information propagation, it often falls short of categorizing them as a distinct component within information spreaders. Bots can create a false sense of agreement among users, a technique called astroturfing, creating an appearance of ideas that stem from a given community - when bots are manufacturing conversations in the discourse (Echeverria & Zhou, 2017). Nefarious actors can purchase communities of bots to appear more influential (Echeverria & Zhou, 2017). Bots leverage cognitive factors to mimic target audiences and overwhelm grassroots discussions (Chessen, M., 2017).

4.3.7 Spreader properties

The terminology describing entities in information dissemination varies across scholarly works. The most significant property for classifying these entities is their location of origin:

- Domestic Actors: Entities linked to and operating within the primary nation of interest.
- Foreign Actors: Entities external to the nation of interest, not directly affiliated with its domestic affairs.

The classification of location of origin is especially relevant for the US government. The authorities and capabilities of the US, which define the means of mitigation and response, are constrained by locality. An operation that relies on domestic proxies will require intervention by the Department of Justice and their domestic authorities, while a foreign accelerator may be targeted by several federal organizations including the Department of Defense and Intelligence Community.

4.3.8 Techniques

We use the definitions described in (Rodriguez, 2020) as the basis of our taxonomy. However, we recognize that the lexicon of information operations is continually expanding and changing, within US governance. While other frameworks, such as DISARM are indispensable for mitigating immediate disinformation threats and coordinating responses across stakeholders, the information laundering model adds value by uncovering the systematic exploitation of intermediaries and the mechanisms that legitimize false narratives. The US Department of Defense uses terminology like Mal-information, Disinformation, and Misinformation to describe information flows and intent. Other relevant actors, such as social media platforms, have developed their own terminology to characterize information. For example, Facebook/Meta introduced the concept of Coordinated Inauthentic Behavior. Given this wide variance, we attempt to integrate and standardize these concepts while noting when terminology may not be relevant for broader audiences.

Table 1: Definitions of common techniques used in information laundering campaigns (Rodriguez, Information Laundering in Germany, 2020). Added Synthetic Media (Barnes, 2020)

Technique	Definition
Synthetic Media	Artificially created content (e.g., text, voice, sound, video) for the purposes of misleading or deceiving an audience. Sometimes described as “deep fakes.”
Deceitful translation	Imprecise translation that excludes or incorporates targeted messages to modify the content, context, or meaning of the original text.
Disinformation	Articles include false or fabricated information to mislead or deceive the audience.
Misappropriation “woozle effect”	Factual data or contexts are strategically manipulated to mislead, including framing truthful information in a fabricated context.
Misleading headlines	Sensationalized, ambiguous headlines (often "clickbait") attract interest, but may not be factually incorrect.
Potemkin Villages	Articles created by deceptive platforms that endorse each other to create an illusion of credibility, promoting disinformation.
Smurfing	Multiple accounts or websites controlled by the same actor disseminate hard-to-trace information, contributing to source magnification.
Astroturfing	A practice of masking the sponsors of a political message or event to make it appear as though it originates from or is supported by grassroots participants.

Rodriguez abandons the common phrasing of “fake news” and delineates disinformation from many different techniques (Rodriguez, Information Laundering in Germany, 2020). Some of the techniques seem similar but share distinct differences, such as Smurfing and “Potemkin Village.” Smurfing consists of one actor, while “Potemkin Village” consists of more than one.

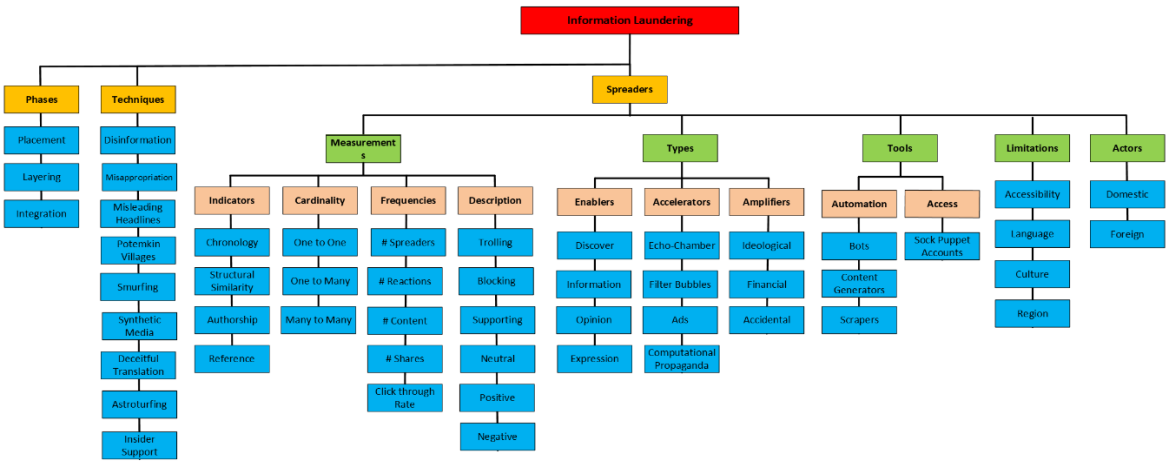

Figure 1: Taxonomy of Information Laundering

4.3.9 Indicators

Rodriguez (2020) outlines the indicators used to analyze information laundering use cases. These indicators include Chronology, Structural Similarity, Authorship, and Reference. These indicators measure the connectedness of content across the IE.

- Chronology: The timing of publication, particularly relevant for news articles published simultaneously or in close succession (applies to social media content too).
- Structural Similarity: The degree of resemblance in informational content across different platforms or articles.
- Authorship: Whether content shares the same or related authors across different platforms.
- Reference: Does the content have valid references or links?

5. Case Studies

5.1 Russia "RT" Information Campaign, 2022[2]

Overview: Pro-Russia media outlet RT (Russia Today) strategically launched a vast information campaign, leveraging the influence of US companies to generate content within the IE. This campaign, based on thousands of Russia-curated videos, was carefully designed to align with Russian interests. By operating through a US shell company, RT attempted to maintain a dominant IE presence while obfuscating its own identity.

Placement: Two employees of Pro-Russia news agency RT paid a company in the US to launder videos in the English language that aligned with Russia's national interest. The videos targeted US foreign and domestic issues. Much of the content fostered support against funding Ukraine's effort against Russia. The initial placement was on popular Western social media platforms. Many original posts were linked to spoofed domains (Potemkin Villages) that consisted of Russia ideologically aligned narratives.

Layering: After placement, the bot networks consistently generated computational propaganda for four months, which slowly fostered support from echo chambers and filter bubbles as the narratives became more indexed within the expressive platforms. Then, search engines (discovery enablers) started recommending many of the commentators that were hired by "US Company 1". US Company 1 continuously paid producers who paid the commentators to continue to commentate on the Russian-aligned content (financially motivated amplifiers).

Integration: The authors assess that integration into the IE was not just a goal, but a reality once the commentators and Russia-aligned content became highly indexed on expression and discovery platforms.

[2] https://www.justice.gov/opa/media/1366266/dl; https://www.theguardian.com/technology/2023/sep/09/x-twitter-bots-republican-primary-debate-tweets-increase; https://www.gov.uk/government/news/uk-exposes-sick-russian-troll-factory-plaguing-social-media-with-kremlin-propaganda

5.2 PRC's Transnational Repression Operations (912 Special Project Working Group)[3]

Overview: An elite task force funded by the People's Republic of China (PRC) conducted information operations in the US for over a decade. The operations deliberately targeted PRC dissidents and worked with US Telecommunications Company to remove dissidents from the company's platform. This operation was part of a larger transnational repression campaign that used many different hybrid warfare tactics to suppress global humanitarian initiatives that targeted the PRC calling for democratic reforms.

Placement. Determining the exact placement is difficult due to how long this campaign has existed. However, through the case files, we see that thousands of sock puppet accounts tied to bots and trolls were created that disseminated computational propaganda that targeted PRC dissident behavior. The malign content was primarily dominant on Western social media.

Layering. This campaign is distinct from Russian campaigns as we know that the PRC had insider help within US telecommunication companies that were able to direct 912 SPWG's activities on social media networks allowing the group to control grassroots discussions (astroturfing). 912 SPWG paid US individuals (financially motivated amplifiers) to maintain accounts and contacted pro-PRC (ideologically aligned amplifiers) individuals to disseminate pro-PRC content. Insiders were able to suppress and remove dissident contributions to the platforms. These amplifiers allowed deeper penetration into passive accelerators (echo chambers and filter bubbles). Simultaneously, other hybrid tactics were executed by other entities including cyber-attacks and attempted kidnapping.

Integration. We view SPWG as reaching successful integration as they operated covertly for a decade and continuously suppressed PRC dissidents while amplifying pro-PRC computational propaganda. This campaign is distinct from the previous campaign as it was more targeted and deliberate utilizing paid domestic proxies to support its transnational suppression tactics.

6. Discussion and Conclusion

The growing ubiquity of technological information dissemination tools lowers the barrier to entry for disinformation actors. Any nation seeking an advantage in the IE (and willing to manipulate information or amplify false narratives) no longer exclusively competes with well-financed nation-states. Instead, any country, group, or actor has the means to compete and distort communal perceived reality within the IE. This proliferation of actors increases the difficulty in the identification and attribution of information operations as an initial step toward mitigation. This paper, through our survey and taxonomy, aims to clarify murky areas within the information advantage discussion. Contextualizing campaign strategies and clarifying the lexicon ensures the community of interest in this space can have meaningful discourse about information operations.

While we provide a tool kit for categorization, precise identification of campaigns in real-time is a continual challenge. The need for identification capability is due to the dynamic and asymmetric nature of hybrid warfare that relies upon creativity and unique approaches to achieving operational objectives. The wider US policy direction prioritizes reactive illumination and disruption of adversary campaigns rather than proactive engagement in the information space. Counterintuitively, this approach nests well under US morays and policy guidance. While adversaries rely upon deception, the US relies upon the perception of legitimacy and promotion of truth. Therefore, deception may be employed to obfuscate tactical maneuvers but must be avoided when seeking to gain the confidence of other nations.

The prioritization of operations in the IE within government structures is crucial to enable responses to the efforts of great power competitors. Prioritization of information operations not only enables the US to disrupt adversary campaigns but also ensures the establishment of relevant knowledge within the organizations tasked with engaging in competition below the threshold of armed conflict. Examples such as the recent creation of the Theater Information Advantage Detachments and the codification of doctrine[4] for managing Information service-wide (US Army) is an indication of US prioritization of operations in the IE. Other cases, such as the

[3] https://www.state.gov/wp-content/uploads/2023/09/HOW-THE-PEOPLES-REPUBLIC-OF-CHINA-SEEKS-TO-RESHAPE-THE-GLOBAL-INFORMATION-ENVIRONMENT_Final.pdf; https://therecord.media/34-charged-spreading-prc-disinformation-harassing-chinese-dissidents; https://www.newsweek.com/us-charges-china-backed-hackers-14-years-cyberattacks-1883487

[4] Army Doctrine Publication (ADP) 3-13 Information. https://armypubs.army.mil/ProductMaps/PubForm/ADP.aspx

shuttering[5] of the Global Engagement Center within the Department of State and litigation of the legality of US government coordination efforts with private companies to mitigate information operations, illustrate political and legal tensions with proactively engaging disinformation as a whole-of-government approach. The effectiveness of these organizations is also contingent on individuals with knowledge of information operations and data comprehensiveness matriculating into decision-making positions throughout the executive branch of government. The integration of more refined concepts of information operations, including information laundering, will improve the ability of the individuals and organizations within the US government to engage against malign information operations effectively.

Acknowledgements

We would like to express our gratitude to the Army Cyber Institute for their financial support. We also thank our peer reviewers for their detailed and helpful feedback that improved this manuscript's quality.

References

Aceves, W.J. (2019). Suing Russia: How Americans can fight back against Russian intervention in American politics. Fordham International Law Journal, 43(1).

Africa Center for Strategic Studies (2023). Tracking Russian interference to derail democracy in Africa. *Africa Center*. Available at: https://africacenter.org/spotlight/russia-interference-undermine-democracy-africa/ (Accessed: 11 October 2023).

Al-Rawi, A. and Rahman, A., 2020. Manufacturing rage: The Russian Internet Research Agency's political astroturfing on social media. *First Monday*. doi: 10.5210/fm.v25i9.10801.

Barnes, C. and Barraclough, T., 2020. Deepfakes and synthetic media. In *Emerging technologies and international security* (pp. 206-220). Routledge.

Chessen, M., 2017. Understanding the psychology behind computational propaganda. *Advisory Commission on Public Diplomacy, May*.

Chivvis, C.S., 2017. Understanding Russian "Hybrid Warfare": And What Can Be Done About It. *Rand Corporation*, *17*. doi: 10.7249/ct468.

Creed, R. and Flynn, M. (2024). Information advantage: A combined arms approach. Military Review, May-June, pp. 50-56. Available at: https://www.armypubs.army.mil/ (Accessed: 10 October 2024).

Cybersecurity and Infrastructure Security Agency (2022). Preparing for and mitigating foreign information operations targeting critical infrastructure. *CISA*. Available at: https://www.cisa.gov/ (Accessed: 10 October 2024).

Dayspring, S.M. (2015). Toward a theory of hybrid warfare: the Russian conduct of war during peace. PhD thesis. Monterey, California: Naval Postgraduate School.

Echeverria, J. and Zhou, S. (2017). Discovery, retrieval, and analysis of the 'Star Wars' botnet in Twitter. In *Proceedings of* the 2017 IEEE International Conference on Advances in Social Networks Analysis and Mining, pp. 1-8.

Farwell, J.P. (2014). The media strategy of ISIS. Survival, 56(6), pp. 49-55. doi: 10.1080/00396338.2014.985436.

Fick, N. and Krach, K. (2023). Krach Institute Freedom Lecture featuring Ambassador Nate Fick. YouTube. Available at: https://www.youtube.com/watch?v=NBJyiLmDmDQ (Accessed: 20 October 2023).

Flammer, P.M. (1973). Communist propaganda in South Vietnam. *Brigham Young University Studies*, 13(2), pp. 206-213.

Hiley, V.R. (2021). A preliminary investigation into the presence of woozles in applied behavior-analytic publications. 2021.

House Appropriations Committee (2024) United States Efforts to Counter Russian Disinformation & Malign Influence [Online]. Available at: https://www.youtube.com/watch?v=lzZF81sifuw (Accessed: 25 October 2024).

Johnson, A. R. (2012, December 6). Radio Free Europe and Radio Liberty. Wilson Center. Retrieved December 20, 2024, from https://www.wilsoncenter.org/publication/radio-free-europe-and-radio-liberty

Keller, F.B., Schoch, D., Stier, S., and Yang, J. (2020). Political astroturfing on Twitter: How to coordinate a disinformation campaign. Political Communication, 37(2), pp. 256-280. doi: 10.31235/osf.io/a5gk6

Klein, A. (2012). Slipping racism into the mainstream: A theory of information laundering. Communication Theory, 22(4), pp. 427-448. doi: 10.1111/j.1468-2885.2012.01415.x.

Korta, S. (2018). Fake news, conspiracy theories, and lies: an information laundering model for homeland security. *Homeland Security Affairs*, 2018.

Lopez, B., 2020. Muriel Spark and the art of deception: constructing plausibility with the methods of WWII black propaganda. The Review of English Studies, 71(302), pp.969-986. doi: 10.1093/res/hgaa039

Master, A. and Garman, C., 2023. A worldwide view of nation-state internet censorship. Free and Open Communications on the Internet, 2, pp.1-21. Available at: https://petsymposium.org/foci/2023/foci-2023-0008.pdf (Accessed: 08 October 2024).

Marten, K. (2019). Russia's back in Africa: Is the Cold War returning? *The Washington Quarterly*, 42(4), pp. 155-170. doi: 10.1080/0163660x.2019.1693105.

[5] https://web.archive.org/web/20250102192304/https://www.state.gov/bureaus-offices/under-secretary-for-public-diplomacy-and-public-affairs/global-engagement-center/

Meleshevich, K. and Schafer, B. (2018). Online information laundering: The role of social media. Alliance for Securing Democracy, 9(8).

Mueller, J. and Gans, J. (2023) 'Fears grow over AI's impact on the 2024 election', *The Hill*, 25 December. Available at: https://thehill.com/homenews/campaign/4371959-ai-artificial-intelligence-2024-election-deepfake-trump/ (Accessed: 25 October 2024).

National Archives and Records Administration. (1941-47). Miscellaneous OWI broadcasts, 1941-47. National Archives and Records Administration. https://www.archives.gov/research/guide-fed-records/groups/208.html

Osipova-Stocker, Y., Shiu, E., Layou, T., & Powers, S. (2022). Assessing impact in global media: Methods, innovations, and challenges. *Place Branding and Public Diplomacy*, *18*(3), 287-304. doi: 10.1057/s41254-021-00240-4.

Peltier, E. (2024) 'Russia signs satellite deal with three West African military juntas', The New York Times, 24 September. Available at: https://www.nytimes.com/2024/09/24/world/africa/russia-satellite-west-africa.html (Accessed: 25 October 2024).

Puschmann, C., Ausserhofer, J., Maan, N., and Hametner, M. (2016). Information laundering and counter-publics: The news sources of Islamophobic groups on Twitter. In Proceedings of the International AAAI Conference on Web and Social Media, 10, pp. 143-150. doi: 10.1609/icwsm.v10i2.14847.

Ribeiro, F.N., Saha, K., Babaei, M., Henrique, L., Messias, J., Benevenuto, F., Goga, O., Gummadi, K.P., and Redmiles, E.M. (2019). On microtargeting socially divisive ads: A case study of Russia-linked ad campaigns on Facebook. In Proceedings of the Conference on Fairness, Accountability, and Transparency, pp. 140-149.

Rodríguez, B. (2021). Information Laundering in Germany. NATO Strategic Communications Centre of Excellence.

Rodríguez, B. (2021). Information Laundering in the Nordic-Baltic region. NATO Strategic Communications Centre of Excellence.

Rossetti, M.L. and Zaman, T. (2023). Bots, disinformation, and the first impeachment of US President Donald Trump. PLOS ONE. Available at: https://doi.org/10.1371/journal.pone.0283971 (Accessed: 10 October 2024).

Seaman, M., 2013. 'A New Instrument of War': The origins of the Special Operations Executive. In Special Operations Executive (pp. 7-21). Routledge.

Satariano, A. and Mozur, P. (2023). The people onscreen are fake. The disinformation is real. The New York Times, February. Available at: https://www.nytimes.com/2023/02/07/technology/artificial-intelligence-training-deepfake.html (Accessed: 10 October 2024).

"Social Media and News Fact Sheet" (17 September, 2024). Pew Research Center, Washington, D.C. https://www.pewresearch.org/journalism/fact-sheet/social-media-and-news-fact-sheet/ (Accessed 21 October 2024).

US Department of State (2024). The Kremlin's disinformation campaign in Africa. US Department of State. Available at: https://www.state.gov/disarming-disinformation/ (Accessed: 10 October 2024).

Weber, D. and Neumann, F. (2021). Amplifying influence through coordinated behavior in social networks. *Social Network Analysis and Mining*, 11(1), p. 111.

Wylie, C., 2019. Mindf*ck: Cambridge Analytica and the Plot to Break America. 1st ed. New York: Random House.