December 2024

ATAC
ASYMMETRIC THREATS ANALYSIS CENTER

Government Responses to Asymmetric Threats:

The State of the Literature on Information Operations from 2002 to 2022

Dr. Nazli Avdan

START
NATIONAL CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM

APPLIED RESEARCH LABORATORY FOR INTELLIGENCE AND SECURITY

UNIVERSITY OF MARYLAND

ABOUT THE AUTHOR

The author of this summary is Dr. Nazli Avdan, from the University of Kansas. Dr. Elizabeth Radziszewski, Dr. Louis Wasser, Dr. Amy Pate, Ms. Salma Bouziani, Ms. Madeline Room, Dr. Sean Doody, Ms. Larissa Mycyk, Ms. Nancy Haugh, Dr. Caroline Orr, and Mr. Cody Wilson provided valuable assistance in the development of this report.

Questions about this report should be directed to Dr. Elizabeth Radziszewski at eradzisz@umd.edu.

ABOUT THE PROJECT

This interim report is part of the Global Responses to Asymmetric Threats: Phase 1 of Irregular Warfare Net Assessment Data Structure project, part of the Asymmetric Threat Analysis Center (ATAC), a joint program between START and UMD's Applied Research Lab for Intelligence and Security (ARLIS). ATAC is funded by the Department of Defense under award no. HQ003421F0481. Any opinions, findings, and conclusions or recommendations expressed in this report are those of the authors and do not necessarily reflect the views of the Department of Defense.

ABOUT START

The National Consortium for the Study of Terrorism and Responses to Terrorism (START) is a university-based research, education and training center comprised of an international network of scholars committed to the scientific study of terrorism, responses to terrorism and related phenomena. Led by the University of Maryland, START is a Department of Homeland Security Emeritus Center of Excellence that is supported by multiple federal agencies and departments. START uses state-of-the-art theories, methods and data from the social and behavioral sciences to improve understanding of the origins, dynamics and effects of terrorism; the effectiveness and impacts of counterterrorism and CVE; and other matters of global and national security. For more information, visit start.umd.edu or contact START at infostart@umd.edu.

ABOUT ARLIS

The Applied Research Laboratory for Intelligence and Security (ARLIS), based at the University of Maryland College Park, was established in 2018 under the sponsorship of the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)). As a University-Affiliated Research Center (UARC), ARLIS' purpose is to be a long-term strategic asset for research and development in artificial intelligence, information engineering, and human systems. ARLIS builds robust analysis and trusted tools in the "human domain" through its dedicated multidisciplinary and interdisciplinary teams, grounded both in the technical state of the art and a direct understanding of the complex challenges faced by the defense security and intelligence enterprise. For more information, visit www.arlis.umd.edu/about-arlis or contact ARLIS at info@arlis.umd.edu.

Table of Contents

Introduction

Information operations have attracted renewed attention among pundits and scholars in recent years. Information operations are nothing new; in fact, the old empires of China and Russia reportedly relied on them.[1] However, the advent of social media has significantly reshaped their utility and usage on the world stage, broadening their scope and impact. Specifically, social media platforms have introduced new dynamics by enabling rapid dissemination of information and fostering user-generated content. Social media has thus significantly reshaped the scholarly discourse around information operations. Alongside scholarship on social media platforms such as Facebook, Twitter, and Instagram,[2] research has also studied traditional media and its role in direct propaganda.[3] Taken together, both strands of scholarship highlight how media can amplify disinformation and influence public opinion.

In this report, I present an overview of the existing state of research on the nature and the effectiveness of states' use of information operations against other states and on states' responses to adversaries' information operations from 2002-2022. Information operations are defined as "actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome."[4] They can comprise false news, disinformation campaigns, or networks of fake accounts. They can also rely on conventional, digital, or social media.

This report is based on research conducted for the Global Responses to Asymmetric Threats project, which is part of a broader research effort, Irregular Warfare Net Assessment Data Structure (IW-NEADS). The goal of IW-NEADS is to engineer a data resource that is highly relevant to assessment, analysis and prioritization across several pillars of irregular warfare (IW), to include identification and aggregation of relevant variables in existing datasets, review of the theoretical frameworks associated with information operations (IOs), counterterrorism (CT), and counterinsurgency (COIN), and identification of research lacunae, both in terms of available data and existing analysis. IW-NEADS will produce a knowledge matrix that: 1) systematically surveys existing research; 2) provides links to available data; 3) facilitates gap analysis by enabling scholars to identify and fill prioritized research gaps; and 4) provides pedagogical resources for training and practitioner education in the utilization of the aforementioned outputs consonant with the goals of the IW Annex of the National Defense Strategy.

This report provides a comprehensive overview of the literature on information operations, specifically in the context of interstate relations, covering empirical and theoretical works as well as review articles. I begin by introducing the methodology used by the research team to extract the literature. Next, the report will document summary findings on the distribution of research across article type, publication venue, publication year, methodology, and the geographic scope of information operations discussed in pieces of scholarship. The report will then identify the distribution of literature across two types of information operations, i) states' responses to information operations by adversaries and ii) states' use of information operations to target another state. In cases where a piece of literature focuses on

[1] Weedon, Nuland & Stamos (2017).
[2] For example: DiResta, Grossman & Siegel (2022).
[3] For example: Boyte (2017) studies how the U.S. used both traditional media (Radio Free Europe) in conjunction with social media platform (Twitter) in responses to Russian IOs. Also see Sartonen et al. (2016) for a comparison of IO tactics on social media and traditional media.
[4] Weedon, Nuland & Stamos (2017:4).

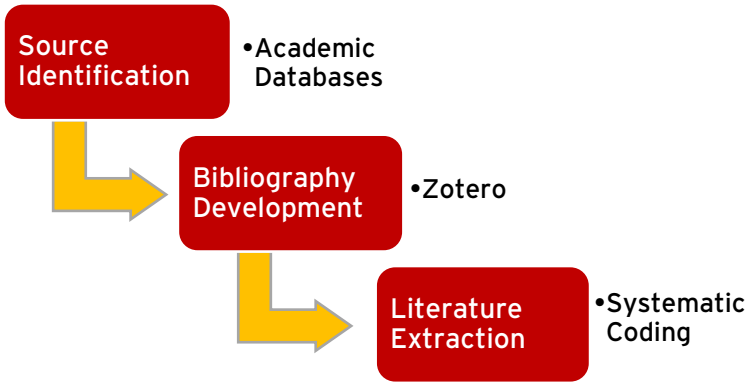
government responses, the report will provide summaries of the type of lever of state power that was used in such responses. The report will distill insights about the focus of each operation covered in these studies.

Next, the report identifies dependent variables (for empirical pieces) or key focus of the article (for theoretical and review articles) and independent variables (for empirical pieces only). By detailing dependent variables, the report highlights outcomes related to information campaigns that have attracted the most attention in the literature. By discussing independent variables, it sheds light on the causes and determinants of outcomes related to information campaigns that the literature has concentrated on. The report then provides insights on the empirical literature's findings related to i) strategic approach selection and effectiveness of government responses to adversaries' information operations, and ii) strategic approach selection and effectiveness of adversaries' information operations. Lastly, the report will identify lacunae in scholarship and conclude with a discussion of future avenues for scholarship.

Methodology

The process for collecting and analyzing the existing state of the literature on information operations follows the same three-phase step that was used to extract relevant sources for previous data on government responses to counterinsurgency (COIN) campaigns.[5] During the three-phase process, the research team identified relevant scholarship, using the search terms, "information operations" and "influence operations." The team then assembled a bibliography and extracted data from the literature. The extraction focused on academic articles, reports, and book chapters, which ensured a wide coverage of the literature.

Figure 1: Knowledge Matrix Development



[5] Radziszewski et al. (2023).

Source Identification

For this project, the research team focused on pieces that covered either government responses to other states' information operations, or information operations enacted by states against their adversaries.[6] Importantly, the report does not focus on governments' use of information operations in domestic contexts, such as when governments use information campaigns against domestic opposition. Exceptions to this exclusion criterion would be cases where the domestic use of information campaigns helped a government formulate foreign policy against an adversary. For instance, a study that examines the Chinese government's use of propaganda to mobilize public support either for an aggressive or more pacifist policy against adversaries[7] would be included in the extraction of scholarship. In addition to the implementation of search strings, the team manually combed reputable political science journals to ensure reliability and inclusion of relevant material that the keyword search may have missed.

Literature Extraction

Mirroring the process from previous reports on COIN to systematically analyze the corpus of scholarship, the project leader crafted a literature extraction guide, which was iteratively modified to ensure reliability and precision. Coders were instructed on how to properly extract pertinent information from the literature. Any discrepancies were resolved during individual and team meetings. The research team conducted the coding process on a shared spreadsheet, which was accessible only to team members. Successively, senior members of the research team reviewed the coding to ensure thoroughness, consistency, and accuracy.

Each piece of literature was coded across several relevant dimensions. For social scientific literature published in academic journals (quantitative or qualitative pieces), the research team recorded the hypotheses, research questions, and the dependent and independent variables used to test the hypotheses, and the suggested testing of the hypotheses (for theoretical studies). The team then summarized the findings for each hypothesis and recorded the method utilized to produce the study's findings. For all publications, the team included indicators capturing the temporal and geographic scope of each information operation examined in a piece. For publications with a temporal focus, the team recorded the start and end years of the analysis. To examine the geographic focus of the information operations that are the subject of a particular article, the team noted the presence or absence of each UN geographic sub-region and the DoD's Combatant Command areas of responsibility (AORs). Finally, for studies that concentrated on five or fewer specific countries as the focus of information operation, the team coded for the presence of specific countries using the country codes from the Correlates of War (COW) country list.

The study also recorded several variables that categorize the different types of information operations covered in the literature, distinguishing between cases where a state uses information operations to initiate an attack against another state and cases where the government responds to another state's use of information operations in an attack. For cases where the state is the initiator, the coding would record whether the focus of the operations was the adversary's military, political/legal institutions, economic

[6] The research team focused on government's use of information operations against non-state actors in the context of COIN in another report, see Doody (2023). The focus on government's use of information operations against non-state actors in the context of counterterrorism is the subject of the team's forthcoming research and related report.
[7] Wang (2021).

institutions, and/or general population. For cases that focus on government response to an adversary's use of information operations as a weapon, the coding registers whether the response focused on the adversary's military, political/legal institutions, economic institutions, or the general public. The coding also notes if the targeted state responded to an adversary's information operation through defensive measures in the context of its military, political/legal institutions, economic institutions, or the general public.

Finally, for the pieces of literature that focus on government responses to adversary's use of information operations as a weapon, the research team also coded for the national lever of power employed in a response, using an expanded DIMEFIL schema. These levers include diplomatic, information, military, economic, financial, intelligence, law enforcement, development, and governance. More specifically, "diplomatic" responses indicate the use of negotiation and dialogue and ensuing treaties or policies; "information" responses indicate the deployment of information and narrative to shape events, strategies, and perceptions to advance interests; "military" responses indicate the use of coercive threats and actions to compel adversaries; "economic" responses denote the deployment of economic instruments and policies, including macroeconomic policy, trade policy, and foreign aid to advance interests; "financial" responses denote the use of formal or informal financial systems, usually through denial of access, "intelligence" responses denote the conversion of diverse data related to the environment, future capabilities and intention, and relevant actors into coherent information to allow decision advantage to advance interests. Responses coded as "law enforcement" include the use of international, foreign, or domestic legal frameworks and their enforcement to advance interests; responses coded as "development" involve activities designed to advance the capacity of the recipient, typically but not exclusively its economic capacity. Finally, responses are coded as "governance" if they include activities to improve the efficacy and legitimacy of institutions. The research team derived this information from the research question, hypothesis, or central focus of empirical pieces, and for all other pieces from the main focus in the study's introduction.

Summary Findings

Research Type

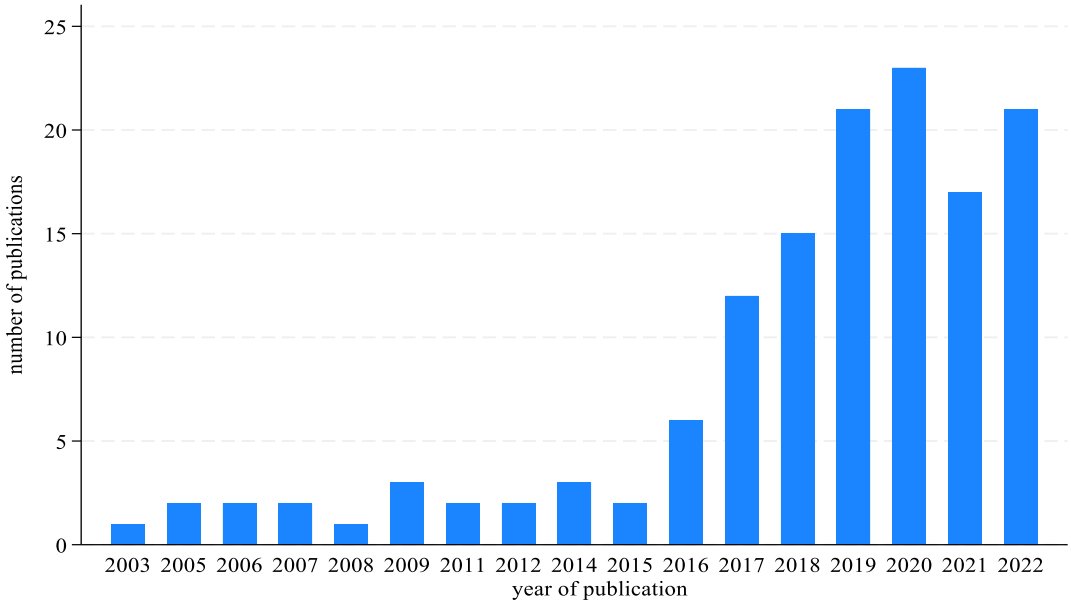
The research team extracted and coded 136 pieces of literature. Of the entire corpus 25 pieces of the literature have a dominant focus on states' responses to adversaries' use of information operations while 109 pertain to state initiation of IOs against other states. The literature contains empirical pieces that engage in either qualitive or quantitative testing and non-empirical pieces that review existing insights on the topic or provide a theoretical platform for outlining linkages between variables without hypothesis testing. We exclude pieces that adopt strictly a policy perspective from this report. Most of the pieces covered in this report adopt an empirical approach, comprising approximately 76 percent of the corpus of literature reviewed. About a quarter of the material reviewed for this report (excluding policy pieces), adopts a non-empirical approach. Within the latter category, nearly one fifth of the pieces are classified as theoretical studies (18%). The rest, 5.5 percent of pieces, are categorized as review articles.

Frequency of Publications over Time

The frequency of publications from 2002 through 2022 shows that interest in information operations has gained momentum over time. The distribution is left skewed, as shown in
Figure 1

Figure 2, indicating that in the early 2000s, there were fewer published works on the topic. Interest begins to increase steadily from the mid-2010s, with a clear peak in momentum in 2017. The latter likely reflects the aftermath of the 2016 U.S. presidential election where attention turned to information manipulation and potential interference. Disinformation surrounding Brexit also likely played a role in the upsurge of scholarly interest around 2016 and 2017.[8] 2020 shows another uptick, likely because of the uncertainty during the time of the global pandemic as well as during the presidential election.[9] Finally, interest peaks again in 2022, in the aftermath of Russia's invasion of Ukraine.

Figure 2: Publications on Information Operations, 2002-2022



Methodological Focus

Existing findings on information operations literature lean more qualitative than quantitative. Considering the entire research literature on information operations, almost 60 percent of articles are categorized as using qualitative methods while 26 percent are classified as using quantitative methods. Considering only the empirical research scholarship, 83 percent are classified as using qualitative methods, and 36 percent as using quantitative methods. Only three percent of empirical research articles utilize mathematical models. Notably, these categories are not mutually exclusive; that is, some articles are mixed methods and contain both quantitative and qualitative methods.

[8] Brooker (2021).
[9] Freelon & Wells (2020).

Qualitative research skews considerably toward case studies of countries' utilization of information operations against their adversaries. The top four utilized approaches among qualitative studies are: case studies (55 percent of all empirical articles; including single longitudinal case studies and comparative/multiple case studies); content analysis (20 percent), discourse analysis (8 percent), and historical case studies (7 percent). Most case studies leverage secondary qualitative sources, such as published scholarship (books and articles), as well as journal articles, open-source materials from government resources, and secondary literature review.[10] The second common type of qualitative analysis is content analysis, including analysis of government resources, state documents, policy speeches, newspapers/magazines, and social media accounts. The third most common methodological approach, discourse analysis, includes the analysis of speeches and messages on social media, news sites, and other open-source platforms. A handful of studies (6%) have conducted primary data collection through surveys[11] and interviews.[12] Finally, the rest of the surveyed studies deploy mixed methods, combining quantitative and qualitative approaches. The Table 1 below displays the breakdown.

Table 1: Most Frequent Qualitative Tools in the Study of Information Operations

Type of Qualitative Tool	% of the Literature
Case Studies	62
Content Analysis	20
Discourse Analysis	8
Surveys and Interviews	6
Other (mixed methods)	4

Turning to quantitative approaches, the top four most-utilized approaches within this body of work are descriptive and bivariate statistics (34 percent of all empirical articles), network analysis (20 percent), multivariate analysis (20 percent), and simulations and agent-based modeling (15 percent) and other (11 percent). The Table 2 below displays the breakdown.

[10] Within case studies, most scholars focus on a single country's use of information operations against a country or within a region and/or a country's responses to an information operation. Boyte (2017) exemplifies this type of study. This is a case study of Russia's use of social media to disseminate propaganda in the Ukraine conflict, 2013-2015, and U.S./NATO counter responses.

[11] For example: Katerynych (2022) conducts a comparative case study approach of the information security environment in Poland and Ukraine. The study contains a qualitative analysis of Polish and Ukrainian journalists' perceptions of Polish and Ukrainian information security development based on original survey data.

[12] For example: Deibert et al. (2012) study employs mixed methods that draw on research including primary data collection through interviews and documents and the creation of timelines incorporating information from different sources.

Table 2: Most Frequent Quantitative Tools in the Study of Information Operations

Type of Quantitative Tool	% of the Literature
Descriptive and Bivariate (e.g., correlations, factor-analysis)	34
Network Analysis and Mapping	20
Multivariate Analysis (e.g., logit, surveys)	20
Simulations and Agent-based	15
Other	11

Bivariate analysis includes studies that perform cross-tabulations and provide correlation matrices with diagnostic statistics such as Pearson's r coefficients,[13] include t-tests to assess the strength of association between variables,[14] or perform factor analysis. Network analysis contains studies that examine clustering of messages, mapping of social media accounts, mapping of social media responses, and mapping of the network of fake and conspiracy news accounts to identify clusters of users.[15] Multivariate analysis encompasses studies that employ logistical regression, time-series analysis (e.g., Granger causality),[16] and ANOVA. The simulations and agent-based modeling category comprises a mix of approaches including the use of simulations (e.g., Monte Carlo), agent-based modeling, and the use of various machine-learning models. The "other" category includes cutting-edge methods specific to the study of social media. For instance, one study utilizes novel multilevel image processing, using pixel-level analysis to uncover patterns in visual media, and inspection of photographic quality and color intensity.[17]

Overall, the literature on IOs is trending toward innovation in methodological sophistication with the application of more sophisticated tools to investigate information operations on social media platforms. These tools are particularly well-suited to the quantitative content analysis of social media messages. This can be evidenced also when considering quantitative studies that rely on multivariate analysis. While more conventional methodologies such as survey analysis, ANOVA, and logistic regression are common in this strand of scholarship, more sophisticated methods are also gaining traction. For example, one study pairs Monte Carlo simulations with Dynamic Exploratory Graph Analysis (DynEGA), to estimate the latent structure of topics published in social media, drawing on 236 influential Twitter accounts.[18] These simulations represent newer methodological tools for conducting quantitative content analysis.

---

[13] For example: Watanabe (2017) provides correlations and performs bootstrapping to detect similarity in news coverage related to Ukraine's democracy between Russia's state-run agency and Reuters.
[14] For example: Lundberg & Laitinen (2020) conduct t-tests of Twitter troll messages and messages from Nordic Tweet Stream.
[15] For example: Hindman & Barash (2018) utilize mapping of the network of fake and conspiracy news accounts to identify clusters of friends, subgroups, segments, influential accounts, conversation leaders, and subject matter focus using machine learning techniques.
[16] For example: Lukito (2020) conducts Vector Autoregression (VAR) analysis, including Granger causality tests of IRA's messaging on three separate social media platforms (Facebook, Twitter, and Reddit).
[17] Bastos et al. (2021).
[18] Golino et al. (2022).

Despite this trend, qualitative research remains predominant in the study of information operations, whereby case studies that draw on secondary resources are the most popular methodology of choice for scholars.

Geographic Focus

The research team coded the geographic focus of an information operation according to the focus or target of the information operation. This coding takes into consideration the identity of the target state and/or where the operation is taking place. The scope of geographic coverage was coded as follows: 1) subnational (information operation occurs in a single country), 2) single country 3) two countries (usually representing cases where there is an information operation attack and a response involving an information operation 4) multiple countries within a single Department of Defense region[19] 5) multiple countries in multiple regions 6) and global operations. To give an example from the literature, Deibert et al.'s (2012) examination of Russia's operations against Georgia is coded as involving two countries because it also details Georgia's counter-response to Russia's information operations. It transpires across two DoD regions: Western Asia (which includes Georgia) and Eastern Europe (which includes Russia).

The Table 3 below portrays the breakdown of research pieces by geographic scope. Notably, there are no studies in our trove of research material that pertain to information operations leveraged at the subnational level within a single country. This is to be expected given that we pruned research studies that examine IOs as domestic policy (with no foreign policy calculus or purpose in mind). The modal category of work includes single-country focused studies, comprising nearly a third of the literature. Next, work that encapsulates three or more countries occupying multiple regions comprise 22 percent, and third, scholarship on three or more countries within the same region comprise another 17 percent. Work that focuses on two countries stands at 5 percent, representing a surprisingly slim fraction of the literature. Global focus is relatively rare, making up around 4 percent of the data. Also worth noting, a sizeable percentage—nearly one fifth—of published scholarship has no geographic focus.[20]

Table 3: Distribution of Studies by Geographic Scope

Geographic Scope	% of the Literature
Single country	32.35
Two countries	5.15
Three or more countries within same region	16.91
Three or more countries spanning multiple regions	22.06
Global focus	4.41
No specific geographic focus	19.12

[19] The regions are defined according to the Department of Defense (DoD) categorization.
[20] Articles that are strictly review or theoretical pieces usually fall in this category.

Next, the report considers the distribution of the published scholarship by geographic region in the literature. The research team coded up to 20 geographic regions for each article under consideration. The analysis revealed that Eastern Europe has attracted the most attention, comprising 40 percent of research studies. North America comes in at a close second; 36 percent of articles reviewed have at least one country in the region of North America. Third, Northern Europe comprises about a quarter of the published material while Western and Southern Europe represent approximately 18 percent and 15 percent of the literature. Countries in Western Asia are of interest in about 14 percent of the literature. Other subregions of Asia have garnered modest interest; Eastern Asia, South Asia, and Southeastern Asia constitute 8 percent, 5 percent, and 3 percent of the literature, respectively. The African continent has been mostly ignored by the literature; the only region of interest has been North Africa, standing at less than three percent of scholarship. South America is the region of least interest, among the regions that have been represented in the scholarship; fewer than 2 percent of articles focus on countries in South America. The rest of the DoD defined regions have garnered no attention. Lastly, about 22 percent of articles surveyed have no geographic focus. 67 percent of these articles comprised theoretical or review pieces.

Evidently, there is disproportionate focus in the research literature on Eastern Europe and North America. This is perhaps not surprising considering the temporal trajectory of the literature; as noted earlier, scholarship has gained momentum in response to critical events on both sides of the Atlantic: Russia's annexation of Crimea in 2014, the 2016 U.S. Presidential election, the Brexit referendum in 2016, and Russia's invasion of Ukraine in 2021.

If we dig deeper into the top five countries of focus, we note that the literature is slanted toward a heavy focus on the United States, followed by a focus on Ukraine, and Russia. Importantly, for articles with five or fewer countries of focus; the team listed up to five countries.[21] Tabulating across all recorded countries of focus gives us a snapshot of current geographic focus in the research literature. The U.S. has appeared as a country of focus in nearly a third of the surveyed articles. Ukraine has appeared in nearly 20 percent of the literature. Russia comes in at third place, comprising 12.5 percent of the relevant scholarship. There is also considerable focus on Germany and Afghanistan, as depicted in the Table 4 below.

Table 4: Top Five Countries of Focus

Country Focus	% of the Literature
United States	27.21
Ukraine	19.12
Russia	12.50
Germany	5.15
Afghanistan	3.68

[21] 5.7 percent of empirical studies have global focus (more than five countries); in other words, of empirical studies that have a geographic focus recorded, approximately 94% cover five or fewer countries.

Distribution of Information Operation Literature

We coded the type of information operation separately for publications that focus on initiated IO threats or attacks against adversaries, and those that focus on states' responses to IO threats or attacks against them. Accordingly, we discuss each in turn.

States' Initiation of IO Threats or Attacks

We recorded four types of IOs: 1) attacks/threats targeting the military of another state 2) attacks/threats targeting the political and/or legal institutions of another state 3) attacks/threats targeting the economic institutions of another state and 4) attacks/threats targeting the general population of another state.[22] These categories are not mutually exclusive in that a study may be coded as fulfilling more than one indicator if it focused on a threat or attack against multiple targets. For example, one study[23] examined how IRA's (the Russian Internet Research Agency)[24] activity on various social media platforms (including Twitter and Instagram) affected Black communities in the U.S., and how it has played a role in voter suppression. The study also examined how IRA activity stoked Texas secessionist sentiment, spread insurrectionist sentiment, and sought to sow discord at all levels of government. Thus, this article would be coded as impacting the general population (minority communities, general population in Texas) and the political system (through voter suppression, partisan effects, impact on general elections). An IO targeting the adversary's military may deploy IOs to support kinetic operations, undermine the capabilities of the adversary's forces, cast aspersions on these forces, present them in a negative light or cast doubt on their legitimacy or ability. For example, one study examined Russia's use of IOs as a tool of warfare against Ukraine, whereby Russia combined military tactics with IOs to achieve strategic victory against Ukraine.[25] The study showed how at key military installations Russia paralyzed Ukrainian forces by surrounding them with cordons of pro-Russian personnel, thereby ensuring that TV cameras were ready at these spots to film propaganda in the event that Ukraine attacked the pro-Russian protesters.

Table 5 shows the partitioning of the literature by type of information operation the research literature deals with. One striking finding that emerges is the prevalence of scholarly focus on attacks/threats aimed at the general population. Almost 90 percent of research works surveyed are coded as focusing on threats or attacks targeting the general population of the adversary. Second, there is also striking attention paid to threats or attacks against the political /legal institutions of the adversary; nearly 79 percent of studies fit this category. Military institutions receive more modest consideration, capturing attention about 40 percent of the time. Finally, economic institutions receive modest attention by scholars; a quarter of research studies tackle threats/attacks aimed at the economic institutions of another state.

[22] These four types of IOs correspond to four separate indicators.
[23] DiResta et al. (2018).
[24] The Russian Internet Research Agency (IRA) is a Kremlin-backed organization known for conducting online disinformation campaigns. The IRA gained international notoriety for its role in spreading propaganda and misinformation, particularly during the 2016 U.S. presidential election.
[25] Allen & Moore (2018).

Table 5: Types of Information Operations within Literature on States' Use of Information Operations against Adversaries

Types of Information Operations Focus	% of the Literature
Military of the state is threatened or attacked	38.89
Political/legal institutions of the state are threatened or attacked	78.7
Economic institutions of the state are threatened or attacked	25
The population of the state is threatened or attacked	89.81

States' Responses to IO Threats or Attacks

Turning to the strand of scholarship that focuses exclusively or predominantly on the state's response to an information operations threat or attack, we coded responses along eight dimensions, whether the military institutions, political/legal institutions, economic institutions, or general population was involved in the response. Unlike in the case of state use of information operations as an attack, here responses to such attacks are not limited only to the realm of information operations. We also demarcated between responses that concern the target state's institutions or involve the institutions of the attacker. This yields eight separate indicators for a response that involves 1) the military institutions of the state that is responding 2) the military institutions of the attacker 3) the political/legal institutions of the state that is responding 4) the political/legal institutions of the attacker 5) the economic institutions of the state that is responding 6) the economic institutions of the attacker 7) the general population of the attacker 8) the general population of the state that is responding. We also recorded 9) if the article explicitly focused on the lack of a response.

For example, one study[26] traces Baltic states' responses to Russia's information warfare. As the study considers target states' responses that cover public discussions and educational investments, laws that prohibit people wearing Soviet symbolic insignia (such as the sickle and hammer), and the reinstatement of military conscription in some cases (Lithuania), it is coded as involving a response pertaining to the general population, the political/legal institutions, and the military institutions of the responding state.[27]

To illustrate a case that casts attention to the institutions of the adversary, one report[28] reviews existing research and solutions to formulating responses to Russian influence on social media. The study discusses U.S. counter-responses, detailing legislation targeting the adversary (including sanctions), policy aiming to improve transparency of foreign influence, and legislation requiring political ads to disclose their source of funding. These measures are coded as requiring responses targeting the economic and political/legal institutions of the adversary. The study also considers how the U.S. can counter disinformation abroad by encouraging social media platforms to be more vigilant in monitoring

[26] Šukyté (2017).
[27] More specifically, educational maneuvers would involve the general population, military conscription would involve the military draft, and legal change would pertain to the political/legal institutions.
[28] Bodine et al. (2018).

messages, working with influencers, and conducting research on social media disinformation. These recommendations are categorized as responses concerning the general population (social media users, influencers, researchers) of the adversary (Russia) and the target (the U.S.).

Table 6: Types of Responses within Literature on States' Response to Information Operations Threats/Attacks

Types of Responses Focus	% of the Literature
Military of the state that is responding is involved	36
Military of the attacker is involved	0
Political/legal institutions of the state that is responding are involved	68
Political/legal institutions of the attacker are involved	20
Economic institutions of the state responding are involved	4
Economic institutions of the attacker are involved	12
The general population of the state that is responding is involved	68
The general population of the attacker that is responding is involved	8
No response	4.55

Table 6 displays the patterns from the extracted literature. Several findings stand out. First, there is commensurate focus on responses involving the political and legal institutions and the general population of the state that is responding to an adversary's information operation attack. Sixty-eight percent of articles pay heed to responses involving these facets. Thirty-six percent of works are coded as detailing responses involving the military institutions of the defending state, and 12 percent are coded as dealing with responses involving the defender's economic institutions.

These patterns are somewhat different when it comes to considering responses targeting the adversary's institutions. First, there is greater emphasis on targeting the opponent's economic institutions than there is on targeting one's own economic institutions. This may be, in part, due to a reliance on economic sanctions as coercive statecraft in responses to IOs. A second difference is the lack of focus on responses that pertain to the military institutions of the attacker. It is not clear whether it is because the literature does not focus on such responses or because states do not retaliate militarily against an adversary's information operation attack. A third difference is that there is heavier focus on responses that involve the target's own general population than on responses that involve the adversary's general population. This may be because it is more difficult to craft effective responses that reach the public of an adversary while limiting escalation. Fourth, a notable finding is the scarcity of studies that emphasize a lack of response. One study that does, for example, focuses on Russia's disinformation regarding Brexit. The study characterizes the target, the UK, as having launched an inadequate and delayed response, suggesting

that the government failed to act before the political integrity of the electoral process was already compromised by Russia's IO.[29]

All told, in the more prodigious scholarship focused on states' deployment of IOs, responses involving the general population dominate, followed closely by responses involving the political/legal institutions of the state. In the relatively smaller scholarship on states' responses to IOs, there is more documentation of responses that target the adversary's institutions, rather than the target state's institutions.

Lever of Power

Shifting focus to the lever of power deployed in states' responses to information operations,[30] as discussed in the first section of the report, we coded levers according to the DIMEFIL schema. To recap, articles are coded for whether the lever of power in a state response could be categorized as diplomatic, information, military, economic, financial, intelligence, law enforcement, development, and/or governance. Again, these indicators are not mutually exhaustive, meaning that one article's focus can tap multiple levers of power.

Table 7 documents the categorization of responses according to the levers of power. Notably, 64 percent of surveyed literature that deals with state responses to IOs is classified as recording information-based responses. The second dominant category concerns responses built around law enforcement, occupying 40 percent of articles' focus. Close behind the law enforcement category, 36 percent of the focus is on governance-based measures. Fourth, articles are focused on responses involving the military 32 percent of the time. Fifth, 20 percent of articles are focused on diplomatic responses. There is commensurate focus on economic and financial levers of power, each occupying attention 8 percent of the time. The least attention is paid to responses predicated on development, only drawing interest 4 percent of the time.

Table 7: Distribution of Scholarship on States' Responses based on the Lever of Power

Lever of Power in States' Responses to IO	Description of Lever of Power	% of the Literature
Diplomatic	The use of negotiation and dialogue and resulting treaties or policies to advance interests	20
Information	The deployment of information and narrative to shape events, strategies, and perceptions to advance interests	64
Military	The coercive application or threat of force in order to compel	32
Economic	The use of economic instruments and policies, including macroeconomic policy, trade policy, and foreign aid, to advance interests	8

[29] Silvestre et al. (2022).
[30] The research team did not code the lever of power for literature pieces that focus on state use of information operations in attacks given that information lever of power is always the focus of such pieces.

Financial	Financial responses involving the use of financial systems, either formal or informal, and typically the denial of access to such systems, to advance interests	8
Intelligence	The conversion of diverse data related to the environment, future capabilities and intention, and relevant actors into coherent information to allow decision advantage to advance interests	24
Law Enforcement	The use of international, foreign, or domestic legal frameworks and their enforcement to advance interests	40
Development	Activities designed to enhance the capacity of the recipient, typically but not exclusively the economic capacity	4
Governance	Activities designed to enhance the efficacy and legitimacy of institutions	36

What is Explained: Information Operations Relevant Dependent Variables

The survey of empirical, theoretical, and review articles on information operations identified five categories of dependent variables (DV) and concepts. These categories refer to pieces that examine a state's use of information operations to target an adversary and a state's responses to being targeted by information operations by an adversary. The dependent variable categories are: 1) strategic approaches to achieving geopolitical goals 2) effectiveness/impact 3) evolution in operations 4) vulnerability of targets to IO attacks 6) other.

The "strategic approach" category as outcome refers to the strategic roadmap, that is, states' decisions to pursue specific geopolitical objectives, such as alienate an adversary's population by driving a wedge between the citizenry and the government, counter an adversary's information campaign, or pursue a broader goal of weakening the enemy.

A study that examines Russia's information warfare in Estonia exemplifies an outcome of interest in this category, as the study is interested in Russia's approach to achieving its regional objectives.[31] An analysis of European states' approaches to countering Russian disinformation also fits under the strategic approach bucket.[32]

The "effectiveness" category refers to the effectiveness of an operation to achieve a strategic objective,[33] perceived effectiveness,[34] or effectiveness in planning an information operation.[35] This category also

[31] Veebel et al. (2021).
[32] Hellman & Wagnsson (2017).
[33] For example: Mölder & Sazonov (2018) explore the effectiveness of Russia's information operations in challenging the Western liberal order.
[34] For example: Katerynych (2022)'s outcome of interest is the perception of information security effectiveness.
[35] For example: Van Niekerk & Maharaj (2011) focus on the likelihood that an attack will succeed or fail based on preparation and effect of attack.

covers societal impact of information operations, such as that on public attitudes,[36] or the ability to effectuate change in the behavior of the target, such as the ability to penetrate society,[37] or obtain concessions.[38] For studies that examine responses to information operations, this category covers effectiveness, efficacy, and success in countering the influence of information operations, or minimizing their consequences.[39]

The "evolution" category captures change, continuity, innovation, and incremental development in information operations.[40] It can cover the evolution of specific tactics, such as the evolution of Russia's IRA (Internet Research Agency) information campaigns.[41] This category also captures progress and advancement in motivations that guide information operations by states.[42]

The "vulnerability" category pertains to the societal resilience and vulnerability of targets, including agents and institutions targeted by IOs, capturing the ability of targets to withstand or ameliorate the effects of these operations. This category also includes studies that examine sensitivity to specific tactics, such as the use of artificial intelligence (AI).[43] The vulnerability bucket also taps the difficulty of countering the impact of information operations.[44] For articles examining states' deployment of information operations, it also taps the vulnerability of target states, for example by measuring levels of exposure to IOs.[45]

Finally, the "other" category refers to residual cases that do not neatly fit under the four categories that nevertheless might be indirectly relevant to information operations undertaken by adversaries and state responses. These studies, for example, relate to perspectives on the use of IOs, that undergird the strategic vision or mission guiding information operations.[46] Here, we also include studies that tackle the operationalization of IOs, since they may indirectly guide states' approaches to their deployment.[47]

Table 8 shows the breakdown of categories for dependent variables. The percentages displayed are for all dependent variables identified in the surveyed scholarship. The most prevailing interest in the literature on information operations is in explaining strategic approaches that states deploy. Strategic approaches encompass both those that are deployed by states responding to IOs and those wielded against adversaries

---

[36] Harris (2020), for example, analyzes the ability of Russia's operations to stimulate pro-Russian sentiment abroad.
[37] For example: Bastos, Mercea & Goveia (2023) examine how the use of a particular Twitter profile picture with the target group attains social embeddedness.
[38] For example: Jensen, Valeriano & Maness (2020) model effectiveness of IOs as the change in strategic behavior and/or concessions from the target of Russian cyber operations.
[39] For example: Morabito (2021) looks at the effectiveness of U.S. defense against information operations.
[40] For example: Starbird (2020) examines the evolution of Russia's information operations targeting NATO, showing continuity from past policies.
[41] For example: François, Nimmo & Eib (2019) trace the evolution of IRA's information campaigns.
[42] For example: Greenberg (2021) traces the advancement of Russia's geopolitical posture in the MENA region.
[43] For instance, Gorwa & Guilbeault (2020) study the challenges and difficulties states confront in countering bots.
[44] Janda et al. (2017) measure the level of responsiveness to the threat of hostile influence operations. They create a rating system based on political acknowledgment of the threat by state representatives, government countermeasures, and counterintelligence responses. The lower the level of responsiveness, the more vulnerable the target state is to IOs.
[45] For example: Hjforth & Adler-Nissen (2019) measure target publics' potential exposure to Russian disinformation related to MH17 flight and to non-disinformation.
[46] Chong (2014), for example, examines Asian perspectives on the use of IOs. The author criticizes non-Asian perspectives for being too heavily grounded in conventional understanding of the wartime/peacetime dichotomy. Here, perspectives are not per se capturing a strategic approach but may relate to the strategic vision underpinning IOs.
[47] For example, Freelon & Wells (2020) distinguish between scholarly perspectives focused on the content of IOs versus the reception of IOs.

in IOs that states initiate. Dependent variables that are categorized as falling under the "strategic approach" bucket comprise nearly half of the literature covered in this report (47%). The second popular category is that of "effectiveness," pertaining to the success, efficacy, and effectiveness of information operations, at 41.53 percent. These bigger buckets are followed by dependent variables classified as falling under the "evolution" bucket, representing research focused on studying change in information operations, and constituting 4.4 percent of outcomes of interest. This category is followed closely by dependent variables categorized as representing the 'vulnerability' at 3.27 percent. The residual, "other" category captures the remaining 4 percent of the coded outcome variables.

Table 8: Dependent Variables (DVs) in the Literature on Information Operations, Disaggregated by Category, Breakdown by All DVs Identified

Distribution of Dependent Variables Across Categories Dependent Variable	% of Variable
Strategic Approach	46.99
Example: States' decisions to pursue specific geopolitical objectives, such as alienating an adversary's population by driving a wedge between the citizenry and the government, countering an adversary's information operation.	
Effectiveness	41.53
Example: Success/failure of info ops; impact on sociopolitical outcomes including public opinion; effects on target behavior.	
Evolution	3.91
Example: Continuity or change in the nature of info ops; incremental development and innovation.	
Vulnerability	3.49
Example: Target capability in cushioning effects of info ops; resilience or sensitivity to effects of info ops.	
Other	4.08
Example: Foreign policy postures, perspectives, and legal frameworks related to info ops.	

State Response to Information Operations and State Use of Information Operations: Disaggregating by Article Focus

To recap, in our survey of the literature, we coded two types of articles 1) those that focus on a state's initiation of information operations as an attack or threat against an adversary 2) those that cover a state's responses to an attack involving information operations or threat launched against itself. The team created a binary indicator for whether each piece focused on information operations as a challenge or threat against an adversary, and/or whether it focused on information operations as a response to another state. Thirty-one articles were also coded as containing insights on the use of IOs in both contexts (as threats/attacks and as responses to threats/attacks). By classifying articles into mutually exhaustive categories, the team sought to avoid double counting studies. The goal here was to codify literature as work that deals either exclusively or predominantly with responses to or initiation of IOs. To do so, for all pieces that had elements of both, the research question, hypotheses, dependent variable, and findings were reassessed. The primary research question, hypothesis and attendant dependent variable drove the decision to place studies in either category and the findings served to cross-check the accuracy of coding.[48] The goal here was to analyze dependent and independent variable buckets separately for two strands of the literature, to lend an understanding of differences and similarities among studies that deal exclusively or predominantly with responses to or initiation of IOs.

Table 9 displays the distribution of categories of dependent variables for articles that deal with states' responses to information operations. As in the aggregate analysis, the top two buckets are "strategic approach" and "effectiveness." There is slightly more interest in terms of outcome variables in the former category, comprising 42.42 percent of the literature. About 36 percent of outcome variables relate to the effectiveness of IO responses. The third most popular category, "evolution" captures approximately 12 percent of the scholarship, and the "other" category comprises the remaining 6 percent. Interestingly, when it comes to analyzing states' responses to IOs, "vulnerability" draws the least interest, with only 3 percent of dependent variables falling in this category.

[48] To illustrate, Thornton et al. (2016) examines the effectiveness of Baltic states' responses to hybrid warfare threats by Russia. While the study provides a descriptive account of Russia's approaches to influence campaigns, its hypothesis pertains to states' responses. Specifically, the author hypothesizes and finds support for the claim that Baltic states' liberal values weaken the effectiveness of their responses to Russia's IOs. The study's dependent variable taps the effectiveness of Baltic states' responses to Russia's IOs. The study is coded as pertaining primarily to state responses because the research question, hypothesis, and dependent variable capture states' responses. To provide a contrasting example, Čižik (2017) focuses on how Russia is using soft power to influence decision-making in Central Europe. The dependent variable is Russia's effectiveness in influencing public views and decision-making in Eastern Europe. The author argues and shows that Russia has used online alternative media, trolls, and close connections with politicians and right-wing parties to influence public views and decisions in Czechia, Hungary, and Slovakia. Thus, the research question, hypothesis, and dependent variable all pertain to the initiation of an influence campaign by Russia. The study is originally coded as having elements of both, because the findings cover a descriptive account of Baltics' responses to Russia's IOs. In a nutshell, the analytic component deals with the use of IOs as the hypothesis and dependent variable relate to the initiation of an IO, even though the study describes target states' responses. However, there are no hypotheses that relate to responses. As such, the study is coded as primarily as examining the initiation of IOs.

Table 9: Disaggregating Dependent Variables by Categories in the Literature on States' Responses to Information Operations

Distribution of Dependent Variables Across Categories Dependent Variable	% of Variable
Strategic Approach	42.42
Effectiveness	36.36
Evolution	3.03
Vulnerability	12.1
Other	6.1

Table 10 shifts attention to the strand of the scholarship focused on states' deployment of information operations against adversaries. At first glance, the patterns mirror those observed in Table 9. When compared to Table 9, the "strategic approach" category is slightly more dominant within this strain of the literature, comprising 48.64 percent of the literature. That is, scholars are most interested in exploring how deploying IOs against adversaries impacts strategic objectives. However, the "effectiveness" category comes in at a close second outcome of interest, comprising 42.6 percent of the literature. Again, the "evolution" category captures more attention than the "vulnerability" category, with each bucket constituting 4.7 percent and 2.7 percent of the scholarship. Lastly, the remaining category, "other" category comprises a small portion of the literature (1.35%) of the scholarship.

Table 10: Disaggregating Dependent Variables by Categories in the Literature on States' Use of Information Operations

Distribution of Dependent Variables Across Categories Dependent Variable	% of Variable
Strategic Approach	48.64
Effectiveness	42.57
Evolution	4.73
Vulnerability	2.7
Other	1.35

What is the Cause: Information Operations-Relevant Independent Variables

The surveyed literature yields six main categories of independent variables for *empirical studies*, which is the subset of the scholarship examined here. These categories include tactics deployed, the capabilities of the state, geopolitical and historic context, ideational and attitudinal factors, domestic institutions, and other.

The "tactics" category includes independent variables that typically pertain to micro-level operational elements such as the content of messages, the type of agent sending the message, the platform utilized, and technical characteristics of information operations.[49] Technical characteristics of messages can include micro elements such as message length, lexicon, pronoun usage, gender pronouns,[50]and narrative style.[51] Other technical aspects can include focuses on the amplification of bots or specific bot tactics such as bridging and the illegal harvesting of data.[52] The "tactics" category can also include the types and number of actors involved in information operations,[53] and the organization of cyber-troops and the formation of troll farms to amplify hate speech and micro-target specific groups such as dissidents and journalists.[54]

The "capabilities" category covers societal resilience to withstand the influence of IOs,[55] and the flexibility and adaptability of the state.[56] It also includes the overt and covert capabilities of the state,[57] and perceptions of ability, such as that of security forces.[58] It also encompasses an examination of the cost effectiveness of information operations or responses.[59]

---

[49] For example: Starbird (2020) examines tweet clusters, cluster activity, and other numeric characteristics of tweets.
[50] Lundberg (2020) have among their independent variables of interest: pronoun usage (messages that contain any pronoun), gender pronoun usage (masculine or feminine), and first-person pronoun usage.
[51] For example: Chang (2020) focuses on three levels of narratives, specifically international system, national, and issue narratives.
[52] Beskow & Carley (2022).
[53] For example: Flake (2020) examines the use of specific civil society actors such as NGOs, academia, and the Orthodox Church.
[54] For example: Bradshaw & Howard (2019).
[55] For example: Filipec (2019) measures countries' societal resilience to disinformation, operationalizing it as the mental capacity and ability of citizens to recognize and work more efficiently with manipulative information; Pamment and Agardh-Twetman (2019) code long-term resilience of states targeted by IOs. Long-term resilience includes communication preparedness where the government is capable of projecting its identity through strategic narratives, capacity building that focuses on developing whole-of-government coordination capabilities and establishing partnerships with other countries and the private sector/civil society, threat assessment or the ability to monitor and intercept influence operations, analysis of adversary networks domestically, and the ability to communicate with the adversary using one's own transnational networks of influence.
[56] For example: Iasiello (2017) investigates the role of adaptability in deploying information operations in their success. Specifically, the work probes how Russia reformed its IOs in the wake of Georgia's success in the international sphere, against the backdrop of the conflict with Georgia.
[57] For example: DiResta et al. (2020) examine how China's overt and covert capabilities have enhanced is information operations. Overt capabilities are resources dedicated to its news agency, Xinhua, and covert capabilities are resources invested in content farms and websites.
[58] For example: Clements (2014) has as independent variables of interest the ability of soldiers as well as (dis)information about their abilities (modeled as the difference between their true and alleged abilities).
[59] Allen & Moore (2018) assert that Russia's successful use of information operations is in part driven by the cost effectiveness of these operations. Cost effectiveness is a measure of capabilities broadly speaking because it captures the ease with which a state can employ IOs.

The "context" category relates to historical, geopolitical, as well as ideational, regional and international context that may influence the effectiveness of an IO or responses to an IO. Thus, this category also captures challenges and barriers states confront when implementing operations or crafting responses when adversaries use IOs against them. An article may study, for example, geographic and historical ties between countries.[60] This bucket also includes international context, such as the presence or absence of a legal framework regarding IOs,[61] uncertainty in the system,[62] characteristics of regional/international governance,[63] international rivalry and competition,[64] the changing military context,[65] or significant international phenomena and global events that operate in the background (i.e., the COVID pandemic).[66]

The category labeled "ideational and attitudinal elements" pertains to a range of independent variables that tap ideational characteristics that guide decisions about undertaking an IO or crafting responses to one. These encompass a country's foreign policy postures (such as hardline or moderate) in so far as postures impact how states carry out IO threats and attacks or responses to them. The category also encapsulates variables that tap public attitudes[67] or overall public sentiment,[68] such as levels of societal polarization, which are posited to affect decisions to pursue IOs and respond to them.[69]

Independent variables are coded as fitting the "institutions" bucket if they relate to a state's regime type,[70] domestic institutions,[71] qualitative features of institutions, such as the strength of the rule of law,[72] or the political economic regime (i.e., market liberalism).[73]

Finally, the "other" category pertains to factors that may impact individuals' consumption of information operation messaging. These may pertain, for example, to individuals' demographic characteristics[74] such

---

[60] For example: Čižik (2017) postulates that Russia's close ties with right wing parties and politicians in Eastern Europe affect the success of its IOs.
[61] For example: Hollis (2008) argues that existing international law likely prohibits IOs that involve violence or violent consequences in the physical space. Thus, the legal framework is the variable of interest that conditions states' responses to IOs.
[62] For example: Gorwa & Guilbeault (2020) examines the impact of uncertainty on IO effectiveness. Uncertainty is captured along several dimensions: Confusion about the structure of the system a bot is deployed in (social media platform, API, algorithmic, etc.); Confusion about the function or communication of the bot; Confusion about the usage of the bot (automate information, spread ideology, etc.).
[63] For example: Dowling (2022) examines the effects of digital area governance such as the digitization of systems like voting, petitions, online debate, etc.
[64] For example: Sukhankin (2019) focuses on increasing competition over the Arctic.
[65] For example: Haig & Hajdu (2017) model context as the changing operational environment for contemporary military operations.
[66] For example: Morejón et al. (2022) model the context of high vulnerability, as periods of global upheaval such as the COVID-19 pandemic or the Russian invasion of Ukraine.
[67] For example: Wang (2021).
[68] For example: Pan &Hagström (2021) focus on ontological security or how well integrated a state's sense of identity, continuity, and symbolic order is.
[69] For example: Bastos & Farkos (2019) develop a battery of survey items that capture a range of public attitudes, including populist sentiment, polarization, conspiracy-theorizing, and emotional charge.
[70] For example: Bradshaw & Howard (2018).
[71] For example: Caballero et al. (2020) focuses on the type of domestic actors involved in responses to info ops.
[72] For example: Lin & Kerr (2019) investigate the role of Western liberalism and open society in generating vulnerability to IOs.
[73] For example: Pan & Hagström (2021) investigate the role of neoliberal reforms/governmentality on Australia's use of IOs. Neoliberal governance is operationalized as the degree of market discipline, privatization, and disembeddedness of society from direct social control of economic processes and relations.
[74] For example: Hjorth & Adler-Nissen (2019) analyze the effects of age on the susceptibility to information operations.

as gender and age that in turn modulate the effectiveness of IOs by conditioning how individuals perceive IOs.

Table 11 breaks down the independent variables examined in the literature by category. The percentages represent the classification by independent variables or concepts identified. This breakdown is for an analysis of 233 unique independent variables analyzed across all empirical pieces. That is, review and theoretical articles were eliminated from this analysis. The analysis shows that the literature is heavily focused on "tactics" as explanatory variables. More than 70 percent of the scholarship on information operations is categorized as fitting this bucket.

The next prominent category is "context," comprising just over 10 percent of the literature. If we take these categories in conjunction, scholars are engaged with analyzing the tactics of information operations, as well as, to a lesser extent, the broader environment in which tactics are implemented, and which may condition their effectiveness. Seven percent of empirical findings pertain to "ideational and attitudinal factors" category, while the category of "capabilities" comprise 5.6 percent of the scholarship. Next, "domestic institutions" category comprises 3.4 percent of independent variables of interest. Finally, the residual "other" category, occupies the remaining 2.7 percent of scholarship.

Table 11: Causes Analyzed in the Literature on Information Operations: Breakdown of Independent Variables (IVs) by Category for Empirical Scholarship, for All IVs Identified

Distribution of Independent Variables Across Categories Independent Variable	% of Variable
Tactics	70.39
Example: Technical tactics such as the use of specific propaganda methods including computational propaganda and imitation of websites; construction of strategic narratives; organization of cyber troops, use of trolls/inauthentic accounts/bots.	
Capabilities	5.58
Example: Overt and covert material capabilities, perceived capabilities, resilience and adaptability of actors.	
Context	10.14
Example: Historic, geographic, and ideational context, including ties between countries, global background events and phenomena affecting info ops.	
Domestic Institutions	3.43
Example: Regime type, domestic mechanisms, systems of governance.	
Ideational and Attitudinal Elements	7.72
Foreign policy posture, public attitudes.	
Other	2.74
Example: Individual demographic traits, paradigms affecting info ops.	

Next, the report breaks down explanatory variables by category for articles that are concerned with states' responses to information operations and for articles that focus on states' use of information operations against adversaries. Following the same protocol described in reference to Tables 9 and 10, articles that covered both responses to and initiation of IOs were classified into mutually exhaustive categories based on the predominant research question and/or hypothesis and corresponding dependent variable. To reiterate, this ensures that the scholarship is classified into mutually exclusive categories that capture articles that either exclusively or predominantly focus on initiation or response. To refresh, the literature focused on states' responses to information operations launched against them is thinner in comparison to the literature that investigates the use of IOs by states. Accordingly, there are 19 total independent variables coded for states' responses to IOs, out of a total of 233 independent variables coded for *all* empirical pieces.

Table 12 shows that for works that concentrate on *state responses*, the most prominent category is "context," comprising 40 percent of the literature. That is, when it comes to how states respond to IOs targeting them, the historical, geographic, and ideational context is frequently advanced as a determinant of policies. Tactics emerge as the second-most dominant independent variable category. Twenty percent of studies have independent variables of interest classified as "tactics." The categories "domestic institutions" and "ideational elements" each come in at 16 percent within this body of scholarship. Clearly, structural (institutional) and intangible (ideational) variables are put forward as factors influencing states' responses to adversaries' use of information operations against them. "Capabilities" and "other" buckets each include 4 percent each of the independent variables coded.

Table 12: Independent Variables by Category for Empirical Literature on States' Responses to Information Operations, for All IVs Identified

Distribution of Independent Variables Across Categories for States' Responses to Information Operations	% of Variable
Independent Variable	
Tactics	20
Capabilities	4
Context	40
Domestic Institutions	16
Ideational and Attitudinal Elements	16
Other	4

Table 13 shifts focus to the scholarship on states' deployment of information operations against adversaries. Of 233 independent variables coded, this literature encompasses 214 variables, that is almost 92 percent of all variables of interest for empirical pieces. The "tactics" category emerges as the dominant category for this strain of the literature. Indeed, 78.6 percent of independent variables are classed as

falling under this heading. The next prominent category is "context," which makes up nearly 8 percent of variables. Note here the contrast between the two strands of scholarship, as evidenced by the comparison of the categorical breakdown in these two tables. Not only are the "tactics" and "context" categories reversed in terms of their order of prominence for these literatures—with tactics dominating studies on states' deployment of IOs, -- but also, there is a sharp drop-off from the percentage of variables classified as approaches to those classified as contextual in the latter literature. While context is still important, the literature is mostly preoccupied with examining the tactics that states use to deploy IOs against other states. Third, 5.47 percent of independent variables are coded as pertaining to capabilities. Next, the category, "ideational and attitudinal elements" stands at 6.47 percent while variables falling into the category of "domestic institutions" comprise only 1.5 percent of all variables for this subset of empirical literature.

Table 13: Independent Variable Breakdown by Category for States' Use of Information Operations, for All IVs Identified

Distribution of Independent Variables Across Categories for States' Use of Information Operations Independent Variable	% of Variable
Tactics	78.6
Capabilities	5.47
Context	7.96
Domestic Institutions	1.5
Ideational and Attitudinal Elements	6.47
Other	0

Turning to empirical pieces that focused on the largest independent variable category (tactics), and which is the key focus of this report, the next section examines the five most frequently analyzed tactics and discusses their effectiveness. In keeping with the previous sections of the report, the discussion proceeds separately for a) states' responses to adversaries' use of information operations and b) states' deployment of information operations against adversaries. Finally, as context is the prevailing category of interest only for studies that deal with states' responses to IOs, the report will follow with a discussion on how context affects effectiveness of responses.

Most Analyzed Tactics in the Context of Information Operations

The five most frequently analyzed tactics in the literature fall into the following categories: "cultural and societal manipulation," "disinformation and information warfare," "strategic narratives," "propaganda,"

and "social media manipulation."[75] There are a total of 75 independent variables that belong to the "tactics" category. Of these only five pertain to states' responses to IO attacks, and 70 pertain to states' uses of IOs against an adversary.

Table 14 below portrays the classification by each subcategory of tactic for all empirical pieces. Thirty-two percent of tactics under scrutiny pertain to the use of disinformation campaigns. These campaigns present efforts to spread deliberately false or misleading information to deceive an audience and influence public perception or behavior, often to achieve political, social, or economic objectives. Examples of tactics that would fall under the disinformation category would be the manipulation of information, deception and information control,[76] and information warfare.[77] The second most popular category, "social media manipulation," deals with the use of social media platforms such as Twitter to spread information and misinformation and influence public opinion. This bucket encompasses the micro-level aspects of messaging on social media, such as the length and lexicon of posts,[78] type of social media platform,[79] clustering,[80] and the thematic content, topic, or ideological disposition of the accounts deployed by the initiator. To expand on the latter, one study finds that the right vs left disposition of Russian-backed IRA accounts affect the thematic content of messages posted on Twitter.[81] This category also encompasses the use of bots and inauthentic accounts, fear mongering and incitement of hatred, and the broader use of existing societal polarization, for example between supporters of Republicans vs Democrats in the United States, or by inflaming racial tensions. Twenty three percent of tactics fall in the "social media manipulation" category.

The use of "strategic narratives" comprises a bit over 12 percent of tactics. This captures the use of strategic narratives,[82] and discourse, and specifically, the use of narratives on social media.[83] Tactics such as the exploitation of nostalgia, reliance on past narratives such as exemplified by Russia's use of Soviet narratives,[84] also qualify as fitting this label. Next, "cultural and social manipulation" is the fourth most-often utilized tactic, comprising approximately 10 percent of tactics studied in the literature. This subcategory includes the targeting or use of cultural elements or agents such as the targeting of a cultural

---

[75] Disinformation refers to deliberately false or misleading information spread with the intent to deceive, while propaganda is a broader concept that involves disseminating information—often biased or exaggerated—to promote a particular political cause or ideology. While both can manipulate public opinion, disinformation focuses specifically on falsehoods, whereas propaganda can include truthful content presented in a skewed or manipulative way.
[76] For example: Veljovski et al. (2017).
[77] For example: Jensen et al. (2020).
[78] For example: Lundberg et al (2020).
[79] DiResta et al. (2017) have as independent variables indicators that tap the type of actor sponsoring disinformation (dichotomous noting IRA or GRU), and the type of social media platform (categorical including Facebook, Twitter, Instagram).
[80] For example: Starbird (2020) examines the use of thematic clustering (Pro-Kurd or anti-Erdogan) and cluster activity measured through the number of accounts, number of tweets, percent retweets, percent with URL, and the tweets per accounts.
[81] For example: Golino (2022) examine how the ideological disposition of IRA accounts (left vs right) affect the variation in themes they promote in influence operations.
[82] For example: Veebel et al. (2022) define strategic narratives as instruments that draw on collective memory while also including other factors such as political agendas and ideological views that affect interpretation. The authors examine the role of strategic narratives that frame the West as corrupt and in decline, NATO as fragile, and liberal values as failing. These narratives assist Russia with obtaining strategic objectives, such as creating a rift between the U.S. and the EU.
[83] For example: Boyte (2017) studies the role of social media trolls in Russia's strategy of undermining Ukraine.
[84] For example: Kuzio (2019).

affairs ministry or cultural affairs department,[85] or the use of cultural artifacts such as literature and film,[86] the exploitation of religion, or the leveraging of dyadic cultural links.[87] It also pertains to societal exploitation such as if the state manipulates civil society actors including academia, NGOs, and the church.[88] Lastly, "propaganda" is the fifth most popular tactic, comprising 6.7 percent of tactics analyzed. Propaganda approaches include types of propaganda,[89] propaganda methodologies,[90] and online propaganda.[91]

Table 14 : The Five Most Common Tactics in Information Operations

Tactics Subcategories	% of Tactics
Cultural and Societal Manipulation	10.26
Disinformation	32.05
Propaganda	6.41
Social Media Manipulation	23.08
Strategic Narratives	12.82

Table 15 gives the disaggregation of subcategories of IO tactics in findings that pertain only to the studies on states' use of IOs against other states. This breakdown shows similar results to the full sample of empirical literature. "Disinformation" is the most often utilized tactic, at 31.5 percent. "Social media manipulation" comes next, at 24.7 percent. "Strategic narratives" again occupy the third spot, at almost 14 percent of tactics considered. "Cultural/social manipulation," at 13 percent is followed by the subcategory of "propaganda" at 6.85 percent.

[85] For example: Aldrich (2014) examines how the use of the Cultural Relations Department (CRD) shaped the British strategy of countering Soviet information operations.
[86] For example: Mälksoo (2020) examines the production and release of "The Soviet Story", as a militant Baltic memory project aiming to establish parity in East and West European memory of totalitarian crimes in the twentieth century. The author analyzes the role that film plays in creating a cultural front in the Russian-Baltic war by challenging conceptions of the Soviet legacy in East Europe.
[87] Veebel et al. (2022).
[88] For example: Flake (2020).
[89] For example: Bastos & Farkas (2019) focus on three classes of propaganda: black propaganda or disguised sources within the enemy population, gray or unidentifiable sources, and white or identifiable sources.
[90] For example: In their study on the use of propaganda against adversaries, Elswah and Alimardani (2021) distinguish between old and new propaganda methodology where the old methods are based on leading individuals to a predetermined outcome, in contrast to new methodology which hinges on the creation of distrust without pushing for specific views. Their measure, the "imitation of websites" is an example of old methodology of propaganda.
[91] For example: Darczewska (2014) studies how the use of online propaganda facilitated Russia's success in annexing Crimea, arguing that the use of propaganda allowed the Kremlin to cultivate support among the Russian-speaking population in Ukraine.

Table 15 : The Five Most Common Tactics in States' Uses of Information Operations

Tactics Subcategories	% of Tactics
Cultural and Societal Manipulation	9.59
Disinformation	31.51
Propaganda	6.85
Social Media Manipulation	24.66
Strategic Narratives	13.7

Table 16 lists the subcategories of tactics, only for the studies that concentrate on states' responses to information operations. When states respond to adversaries' use of IOs against them, they most frequently rely on the use of disinformation (40 percent) or strategic narratives (40 percent). Third, they also leverage cultural and societal manipulation tactics. As the table shows, however, none of the subcategories of tactics in states' responses were categorized as relating to propaganda, or social media manipulation.

Table 16 : The Five Most Common Tactics in States' Responses to Information Operations

Tactics Subcategories	% of Tactics
Cultural and Societal Manipulation	20
Disinformation	40
Propaganda	0
Social Media Manipulation	0
Strategic Narratives	40

The subsequent pages will consider how the two most prominent categories of independent variables, tactics and context, affect the effectiveness of state responses to an adversary's use of information operations and the effectiveness of state's use of information operations offensively. To recap, while the literature's focus on the impact of tactics figures prominently in studies on states' *initiation of* information operations against adversaries, the role of context figures prominently in studies on states' *responses to* information operations mounted against them. This section considers how distinct tactical subcategories affect the effectiveness of information operations, for both segments of the literature. As context figures as a prominent explanatory factor in analyzing states' responses to information operations, the report will continue by considering the role of context *only for states' responses.*

It is worth noting how "effectiveness" was coded. For each empirical article analyzed, the research team crafted a narrative summary of the core findings. For the purpose of this report, a success indicator was

created for articles that have outcome variables of interest that fall under the "effectiveness" bucket.[92] Success is coded as "Y" for studies that concluded that the approach had been effective,[93] has obtained the state's objective, or qualified the approach as a success.[94] "M" is coded for studies that indicated either moderate, partial/ limited success,[95] for qualified or modest achievement of objectives, or indicated that the results were conditional on other factors (e.g., domestic institutions and mechanisms).[96] Finally, "N" is coded for failure[97] or lack of success, for studies that acknowledged failure to meet objectives.[98]

The Effectiveness of Tactics Used by States as a Response to IOs: Key Findings

If we focus exclusively on studies of states' responses to IOs and explore the effectiveness of tactics, we are left with one study. The study focuses on the use of disinformation as a tactic. The latter is deemed successful against Russia's disinformation campaign during its invasion of Ukraine in February 2022. Specifically, the study finds that content curators, acting as fact-checkers on Twitter were able to mitigate the negative effects of Russia's disinformation.[99] The study concludes that fact-checkers have a significant role to play during contexts of high vulnerability. During the 2022 conflict, fact checkers responded quickly to the invasion and worked diligently to end the internationalization of hoaxes.

The Effectiveness of States' Use of Information Operations Against Adversaries: Key Findings

Turning to the effectiveness of tactics utilized when IOs are launched to attack or threaten adversaries, and beginning with the most popular tactic utilized, the report considers the effectiveness of disinformation (Table 17). Close to 63 percent of the time that this tactic has been studied within the context of threats and attacks involving IOs, it has been deemed successful. Further, it has been deemed moderately (or conditionally) successful an additional 18.75 percent of the time. Combined, the literature shows that disinformation is an effective tactic against adversaries; it was deemed successful 80 percent of the time it was analyzed. The findings show a lack of success (or failure) for nearly 18.75 percent of the cases studied by scholars.

To provide some substance to these patterns, in the "successful" category, researchers find that Russia's deployment of digital measures against Western democracies within the context of the Brexit referendum and the U.S. 2016 election could continue unimpeded due to the lack of awareness of threats from

---

[92] For the rest of the studies, the success indicator was coded as "U" for unknown or uncertain because these studies did not directly deal with the impact or effectiveness of approaches, but rather, for example, linked tactics to dependent variables other than "effectiveness," such as "strategic approaches."
[93] For example: Yang (2019) acknowledges the difficulties of measuring the effectiveness of Russia's reliance on IRA to exert reflexive control on behavior and views on targeted audience but references the polls conducted at the time of the elections as indicating increased divisiveness.
[94] For example: Ratiu & Munteanu (2018) qualifies Russia's hybrid warfare strategy as successful.
[95] For example: Jensen et al. (2020) qualify Russia's cyber warfare as having indirect and "subtle" effects.
[96] For example: Shackelford et al. (2020) investigate how states can counter the nefarious consequences of disinformation campaigns launched during electoral periods. It is coded as conditional because the authors imply that a multifaceted approach encompassing targeted reforms will be effective in limiting (not eliminating) the contagion of misinformation.
[97] For example: Templeman (2022).
[98] For example: Elswah & Alimardani (2021) find support for the idea that Iran's information operations against Arab states (mostly its rivals: Saudi Arabia, Bahrain, Lebanon, Egypt, and Algeria) have not been effective in influencing the public sphere.
[99] Morejon et al. (2022).

influence operations. The IO campaign escaped Western governments' attention and continued to sway the vote and create societal polarization.[100] To give an example of failure, one study shows, for example, that Russia's disinformation campaign sought to undermine public support for EU access in Ukraine but fell short of its aims.[101] The IO campaign failed because pro-Russian propaganda did not resonate with the public and the pro-Russian presence in Ukraine's political, cultural, and economic sphere was too small. Thus, even though Ukraine's president Viktor Yanukovych delayed the signing of the Association Agreement with the EU, protests erupted, showing that the IO was unable to influence public opinion on Ukraine's accession to the bloc. This example shows that resonance of an IO campaign with the target public can modulate its impact.

Researchers also find that geopolitical, cultural, and domestic factors blunted the success of disinformation campaigns. For instance, Russia's disinformation has been partially successful in the Middle East due to media censorship in the region.[102] Furthermore, other factors, such as ambivalent views about Russia in the region and the absence of cultural, historical, and other connections to Russia, as well as the lack of geographic proximity, all further undermine Russia's campaigns in the region.[103] In short, disinformation functions well if environmental factors, such as bilateral ties between the target and challenger/initiating state are strong and/or have geographic proximity. The tepid success of Russia's disinformation in the Middle East showcases how these factors can attenuate the impact of a disinformation campaign. Nevertheless, disinformation is a powerful tool because it is a versatile tactic, allowing states to adjust and finetune campaigns according to target audiences, to anticipate and sidestep barriers to penetrating target audiences, and because it can fit as a tool in a state's arsenal.[104]

The next popular tactical subcategory, "social media manipulation" was found to yield a successful outcome in 60 percent of cases, a partially successful outcome in another 20 percent of cases, and an unsuccessful outcome in 20 percent of cases. For example, a study of how the U.S. used messaging on Twitter to mobilize the Iranian public showed a lack of positive change in Iran during the 2009 protests.[105] The State Department sought to capitalize on the revolutionary nature of Twitter as a platform to rapidly transmit events to mobilize the Iranian public to engage in public diplomacy and push for regime change. However, the U.S. failed to effectively utilize Twitter to catalyze change due to widespread misunderstanding by Twitter users of the actual dynamics of Iran's security apparatus (i.e., the Iranian government's ability to hunt down protesters), which did not easily lend itself to regime change. The contrasting success case is a more recent study of the use of Twitter during the 2016 U.S. election; it is coded as a success because it shows that the platform facilitated wide reach and penetration of various ideological groups.[106] Social media manipulation is quite effective because it is dynamic, as new platforms offer new tools to spread misinformation; while the majority of studies focus on Twitter, the micro-tactics analyzed, such as the use of bots, inauthentic accounts, and troll farms provide fungible

[100] Silvestre (2022).
[101] Hosaka (2018).
[102] Karasik & Blank 2018 argue that prevalent media censorship in the Middle East allows governments to block Russian messaging that they oppose.
[103] For example: Karasik and Blank (2018) show how Russia has used its information warfare to project power and consolidate its influence in the Middle East.
[104] Polyakova et a.l (2016) show that Russia has successfully used disinformation to sow discord in the EU but calibrates its campaign to account for the lack of shared lingo-ethnic ties in Western Europe.
[105] Burns & Eltham (2019).
[106] Hindman & Barash (2018).

tools that can be applied across social media platforms. Furthermore, states can coordinate their disinformation campaigns across social media platforms, as researchers have found that states can use one platform as a testing ground to improve their tactical efficacy.[107]

Considering strategic narratives, the analysis shows that this tactic is quite effective. Two thirds of the findings are indicative of success. In this category, researchers find that Russia's strategic narratives allow it to create division between the EU and U.S. Thus, in a study of strategic narrative's effectiveness in establishing connections with target audiences, researchers find that Russia succeeded in fomenting populist sentiment and eroding support for liberal democracy.[108] Narratives are effective because they are adaptable and malleable, allowing states to craft new storylines about opponents depending on political objectives. They also allow states to combine visuals, text, and audio in their strategic storytelling; by doing so, states can redefine the image they cast about themselves or opponents to target audiences.[109]

Turning to the tactical subcategory of cultural and social manipulation, 60 percent of cases are coded as yielding successful outcomes, in addition to another 20 percent coded as mixed success. Twenty percent are coded as failed outcomes. The study of how Latvia used a documentary Soviet Story in the cultural front in the Baltics exemplifies the use of cultural manipulation to achieve specific objectives. In this case, the film's message that centered on the broader Eastern European hostility toward communism aimed to pressure politicians to condemn the crimes of totalitarian communist regimes but fell short of its goals because it made sweeping generalizations about European publics and did not leverage critical history well enough to credibly effectuate successful change in views about the Soviet legacy.[110]

Lastly, the tactical subcategory of propaganda has mixed results. The findings in the literature on states' use of IOs are evenly split between success and failure. Exemplifying success, one study finds that Russia's use of propaganda contributed to its success in annexing Crimea, especially by gaining support from Russian-speaking populations in Ukraine.[111] The key to the successful deployment of propaganda in this case was Russia's utilization of sociotechnical principles such as the principles of desired information, emotional agitation, clarity, through which Russia transmitted simple messages about Russophobia, and supposed obviousness, through which the Kremlin engineered political myths. Contrast this with a case of failure where antiquated techniques performed poorly. Along these lines, one study, for example, finds that Iran's use of propaganda against Arab rival states was deemed ineffective in undermining the public sphere in Arab states. Propaganda failed because it did not have sufficient reach of Iranian Twitter accounts. The failure was attributed to the reliance on old propaganda methodology, which aimed to goad audiences toward a predetermined direction rather than new propaganda methods that aim to create distrust without pushing for specific views.[112] These two contrasting cases show that propaganda holds promise if its methodology is updated and precise, if it effectively exploits limitations in cognition such as selective attention and cognitive miserliness. Russia succeeded in its use of simple messaging and clarity principles because people have limited mental faculties, often rely on shortcuts and heuristics,

---

[107] For example: Carter & Carter (2021) show that Reddit emerged as a trial platform, prior to the launch of these campaigns on Twitter.
[108] Veebel et al. (2022).
[109] For example: Van Noort (2020) argues that China successfully utilized visuals to sell its Belt and Road Initiative in its strategic narrative campaign to create an image of China as a cooperative power.
[110] Mälksoo (2020).
[111] Darczewska (2014).
[112] Elswah & Alimardani (2021).

leading clear, simple messages to have powerful impacts. In its deployment of propaganda, the Kremlin took advantage of influential figures in social media,[113] indicating that the availability of trusted figures in disseminating propaganda can also boost its effectiveness.

Table 17 : Effectiveness of Tactics Utilized in States' Use of Information Operations

Tactics Subcategories	% of cases where the tactic is successful	% of cases where the tactic is partially successful	% of cases where the tactic is a failure
Cultural and Societal Manipulation	60	20	20
Disinformation	62.5	18.75	18.75
Propaganda	50	0	50
Social Media Manipulation	60	20	20
Strategic Narratives	66.77	0	33.33

The Role of Context in States' Responses to and Offensive Use of IOs

Context is the second-most dominant category of interest as an independent variable for the empirical literature on information operations. It is the primary category of interest if we limit the analysis strictly to literature on states' response to information operations. The report identifies five general subcategories for variables that relate to context: "digital environment," "domestic environment," "dyadic ties," "ideational environment," and "international environment." All these variables can impact state responses to IOs and state use of IOs as an offensive tool.

The "digital environment" encompasses variables that tap the characteristics of the digital environment,[114] the properties of cyberspace,[115] or the milieu of digital communities.[116] The "domestic environment" subcategory incorporates variables that tap regime type and institutions, including electoral processes,[117] and the domestic legal system.[118] "Dyadic ties" pertains to geographic and historical ties between states[119] (typically vis-à-vis states that wield IOs, such as Russia or China) and/or cultural

[113]Darczewska (2014). In this case Russia relied on Dugin, a prominent geopolitical analyst with a large following. It also benefited from an extensive diaspora of ethnic Russians who could further spread and amplify the Kremlin's propaganda.
[114] For example: Fitzgerald & Brantley (2017) examine how the digital environment has influenced the evolution and success of IOs.
[115] For example: Deibert et al. (2012) explore how the properties of cyberspace have shaped the Russian cyber-campaign against Georgia during 2008 conflict.
[116] For example: Kargar & Rauchfleisch (2019) study the impact of digital hate-speech communities, and how membership in these communities shapes approaches to IOs.
[117] For example: Janda et al. (2017) have the existence of press freedoms and elections as two variables of interest pertaining to the domestic environment.
[118] For example: Notaker (2022) focuses on the role of domestic/legal frameworks, frameworks governing national security and/or citizens' rights.
[119] For example: Flake (2020); Šukyté (2017).

ties.[120] The "ideational environment" subcategory captures intangible ideational factors such as foreign policy postures and principles or strategic culture.[121] The "international environment" subcategory includes variables that pertain to global phenomena such as pivotal events (e.g., COVID pandemic),[122] regional circumstances,[123] international competition,[124] or global media and cyber context.[125]

If we consider the entirety of empirical findings on information operations where at least one independent variable is categorized as contextual, "domestic context" is the primary subcategory of interest, comprising almost 32 percent of independent variables. Scholarly interest is evenly split between the "digital environment," "dyadic ties," and the "international environment," each constituting 21 percent of independent variables, within the subset of empirical scholarship focused on context. Ideational environmental factors comprise the rest of the variables coded.

Decomposition of the subcategorization by scholarship that examines states' responses to IOs and scholarship that explores states' use of IOs unveils a contrasting dynamic. Table 18 displays the full breakdown. In the former literature, domestic environmental factors dominate whereas in the latter, digital environmental factors dominate, each comprising about a third of the literature. Evidently, research that explores states' use of IOs to attack or threaten adversaries pays greater attention to how the digital environment shapes the use and effects of information operations. In contrast, scholars pay greater heed to how domestic—institutional and electoral—factors affect the types and utility of responses countries craft in response to information operations. Domestic contextual variables still figure importantly in the literature on the use of information operations, comprising just over 23 percent of variables, but they are equally important as international environmental variables, again at just over 23 percent.

Table 18 : Contextual Independent Variables and Subcategories of Interest

Context Subcategories	Responses to info ops	Use of info ops
Digital context	16.67	30.77
Domestic context	33.32	23.08
Dyadic ties	16.67	15.38
Ideational Context	16.67	7.7
International context	16.67	23.08

[120] For example: Veebel et al. (2022) analyze how target states' cultural ties to Russia impact the effectiveness of Russia's strategic narrative campaigns.
[121] For example: Dumitrescu (2019).
[122] For example: Morejón-Llamas et al. (2022) focus on the global pandemic as a contextual factor.
[123] For example: Murinska et al. (2018) examine how local conditions, regional, and international context have influenced Russia's hybrid warfare in Latvia and Ukraine.
[124] For example: Sukhankin (2019) examines how an international environmental variable—increasing competition over the Arctic—has shaped Russian influence operations against Western allied countries, particularly Canada.
[125] For example: Hemment (2022) focuses on the hybridized and transnationally dialogic global media context in analyzing Russia's use of humor in its information operations.

The Role of Context in the Effectiveness of Responses to and Offensive Use of IOs: Key Findings

This section will distill the key insights on the role that context plays in the effectiveness of IOs launched by states, and in states' responses to IOs. It will also consider the role of context in prompting innovation in states' responses, insofar as innovation has fostered effectiveness.

Delving into the role that context played in the literature, there are several takeaways. First, considering states' responses to IOs, context figures as a delimiting factor, weakening states' responses to IOs and exposing them to the deleterious consequences of IOs. Bilateral ties with the challenger state stand out as the driver of this dynamic. Studies highlight how geographic proximity and historical ties with Russia amplify vulnerabilities and allow Russian information operations to continue full force. Along these lines, for example, scholars find that due to spatial proximity and the Soviet legacy, Russian propaganda has full access when spreading fake information in Estonia, Latvia and Lithuania as it seeks to divide the population, create a rift between minority groups, and present anti-EU narratives.[126] Additionally, Russia has succeeded in expanding influence in the Baltic and Eastern European states by targeting not only Russian speakers in Eastern Europe but also non-Russian speakers who are exposed to Russian-language propaganda.

Second, within the literature on states' responses to IOs, on a somewhat more positive note, context has sometimes propelled evolution in responses to IO threats. Researchers find that context can assist states in formulating and adapting their responses, particularly when context lends familiarity with the challenger. Along these lines for example, one study finds that familiarity with Russian history and culture makes Baltic countries more aware of Russia's propaganda tactics.[127] Thus, Baltic states have leveraged these connections to craft strong resistance policies, ranging from public discussions and educational investments related to critical thinking and propaganda, use of cultural artifacts to dilute the Soviet legacy, and laws that prohibit people from wearing hammer and sickle symbols and suspend Russian TV/online portals. Other scholars have also noted that target states can offset contextual restrictions through intelligence gathering, capitalizing on assets such as domestic regulation, adversarial will, and technology.[128] In summary, when it comes to states' responses to IOs, context has played a multifaceted role. While context can sometimes render target states inherently vulnerable, for example allowing challengers to exploit shared linguistic and ethnic ties, it can also equip targets with awareness, preparedness, and resilience. Context can also prompt innovation and adaptation, leading to proactive, and thus more effective responses to IO challenges.

When it comes to the role of context in states' use of IOs against adversaries, context is a reinforcing or amplifying factor in shaping IOs' effectiveness. Studies have shown that states can effectively leverage digital context. For example, the media environment following the Maidan Revolution in Ukraine in 2014 augmented the efficacy of Russia's information campaign against Latvia and Ukraine. Researchers assert that mass media facilitated the evolution of Russia's hybrid warfare, allowing Kremlin to innovate and conduct warfare in stages in Eastern Europe and the Baltics.[129] Media purposefully presented a

[126]Šukyté (2017).
[127] Šukyté (2017).
[128] Notaker (2022).
[129] Sandra et al. (2018).

unilaterally distorted "picture" of social disorder and collapse of the government machinery at the time and aggravated the pre-developed stereotypes and myths with respect to the fundamental incapability of the Ukrainians to have their state. As another example, the findings of another study show that interconnectedness through the Internet and social media enhanced Russia's ability to carry out disinformation and cyberwarfare in Central and Eastern Europe.[130]

To conclude, context has played contrasting roles for states' responses to IOs versus states' use of IOs to threaten or attack others. In the former case, context can put states at a disadvantage, allowing adversaries to exploit bilateral ties but also motivating target states to adapt and develop resilience against IO attacks. In the latter case, context can work to the state's advantage in magnifying the utility of IOs.

Research Gaps and Recommendations

The review of the literature on states' responses to adversaries' use of information operations and the nature of adversary's use of such operations points to several lacunae in scholarship as well as potential avenues for inquiry. These lacunae and attendant pathways for inquiry pertain to methodological, conceptual, and substantive issues. In the sections below, each is discussed in turn.

Methodological and Conceptual Issues

First, the literature on IOs would benefit from a rigorous, systematic conceptualization and corresponding measurement of effectiveness. As the literature stands, effectiveness is inadequately defined and operationalized. More specifically, the survey of the literature reveals that effectiveness is an umbrella concept that spans procedural outcomes; intermediate goals such as the continued, unimpeded operation of IOs; and end-goals such as inducing policy change from the target government. As such, there is a pressing need for precision and transparency in measuring and operationalizing effectiveness. One path forward here is to think more carefully about the dimensions of effectiveness, differentiating between intermediate and ultimate success in operations, and between efficiency and efficacy, to give two examples. A related recommendation is for scholars to develop a typology of effectiveness, which can in turn lend consistency in measuring effectiveness and establish a common vernacular for the scholarship on information operations. While doing so, scholars should outline the dimensions of an effective state response. For instance, among the studies that focused on states' responses and considered effectiveness as the outcome of interest, some conceptualized the lack of effectiveness as inadequacy,[131] while others directly assessed responses as ineffective.[132] This is a subtle, but crucial distinction in that inadequacy suggests gaps that can be redressed in the policy response whereas an ineffective qualification may

[130] Jacuch (2022).
[131] For example: Katerynych (2022) finds support for the idea that Ukraine's and Poland's doctrines on information security in response to Russian aggression are inadequate, based on perceptions from 46 journalists and editors in both countries.
[132] For example: Thornton & Karagiannis (2016) qualify Baltic states' responses to Russia's hybrid warfare as ineffective, attributing the ineffectiveness to liberal values which Russia is effectively able to weaponize.

demand a policy pivot. Furthermore, another important distinction in measuring effectiveness is between perceived success of responses and objective measures of success.[133]

A relatively recent study provides a good example of measuring impact, by carefully tying an information operation to changes in public attitudes. The study utilizes original survey data to uncover attitudes on domestic and foreign policy issues among Americans.[134] The authors then probe how exposure to RT or Russia Today influenced Americans' views on these issues. The study provides a guidepost because it leverages primary data (original survey of 944 Americans), has a clearly identifiable treatment (exposure to RT), and clearly defined outcome of interest (change in views on issues). The study is transparent and clear about how it conceptualizes and measures effectiveness of propaganda: as a change in public opinion in a target democracy (the U.S.). Moreover, the article postulates a theoretically driven argument rooted in working knowledge of the stability of public attitudes. The authors derive from the literature the suppositions that opinions on foreign affairs are more malleable because individuals are less knowledgeable about foreign policy issues, and that contrarily, opinions about partisan domestic issues tend to be more stable. This leads to a theoretically informed analysis of the survey data, leading to sophisticated, and generalizable insights about how propaganda by foreign adversaries (Russia in this case) can shape public opinion in democracies. Thus, scholars should follow in the footsteps of this study in conducting studies that are replicable and generalizable with a clear use of effectiveness as a measurable concept.

Second, a related shortcoming of the literature is that it has not paid careful heed to causal mapping of independent variables to and linking independent variables related to the information operation explicitly to outcomes. This is most acute when considering effectiveness as an outcome. While the literature has made strides in discussing how tactics relate to effectiveness, there has not been much effort paid to why, or under what conditions certain tactics work. For example, scholars have examined the effectiveness of IRA accounts in infiltrating political dialogue in Germany, probing how effective IRA accounts were in blending in and adapting to events in German politics.[135] While this represents an excellent study in digging deeper into how micro-tactics such as narrative switching or fishing-for-followers work, the study is more informative on how the IRA utilized specific tactics on social media but does not tell us why these tactics worked. There needs to be more focused consideration of whether a variable functions as a proximate, modifying, or intermediate cause of operational success. Related to this, scholarship has made headway in showing how states utilize IOs in tandem with conventional warfare methods. However, scholarship can offer more clarity on the causal contribution of IOs to outcomes. For example, scholars have documented how Russia effectively combines IO tactics such as propaganda and cyberattacks with military activities to reassert control over Ukraine and sow chaos in Eastern Europe, but they have not articulated the extent to which IOs contribute to overall effectiveness.[136]

---

[133] For example: Katerynych's (2022) measure focused on perceptions of success. The measure is based on survey responses from editors and journalists in Ukraine and Poland, and other, objective measures of success, such as the potential deterrence of the attacking power.
[134] Carter & Carter (2021).
[135] Dawson & Innes (2019).
[136] Mölder & Sazonov (2018).

Third, the survey of the literature reveals a significant paucity in data-driven work, in part stemming from the scarcity of cross-sectional and/or longitudinal datasets on information operations. A welcome exception is the Online Political Influence Dataset.[137] The dataset covers both foreign and domestic influence efforts, tracking their progress, and codifying their features. Beyond offering the first-of-its-kind dataset on the covert use of social media, the dataset is instructive in how it develops clear, systematic guidelines for identifying information operations, pruning cases, for example, that lack an identifiable political goal, or are not undertaken by a state actor. As the dataset is relatively new, there is fertile ground for applications in the study of information operations utilizing its measures. For example, scholars can investigate how various features of influence campaigns tie to their success.

This discussion also points to a need for an analogous dataset on states' responses to IOs. Such a dataset would follow in the footsteps of the Online Political Influence Dataset by measuring the tactics states pursue in responding to IO threats and challenges, the levers of power the tactics focus on, and recording outcomes. The provision of a dataset on states' responses will contribute to a more precise understanding of the effectiveness of states' responses to IOs.

Fourth, methodological innovations whereby scholars use sophisticated methods to capture the unique elements of messaging on social media are gaining traction among scholars, but these types of studies are still in the minority. Thus, there is a need to more fully make use of these innovations. Examples of methodological innovations include research that captures the impact of visual imagery and video design on the success of an information operation.[138] Other studies delve deeper into the content of messaging, for example, through sentiment and text analysis.[139]

Researchers can also apply conventional statistical methods to the study of IOs. Time-series tools can be harnessed by scholars to uncover temporal dependence and longitudinal trends in the way that states use IOs. One study that has carefully applied time series methods to the study of IRA's activity on three platforms, Facebook, Twitter, and Reddit, from 2015 to 2017 is a case in point.[140] Using Vector Autoregression (VAR) and Granger causality tests, the author shows temporal interconnectedness across social media platforms. Importantly, Granger causality tests allow the author to tease out the direction of causal impact, showing that activities on Reddit caused Twitter activity but not vice versa, and suggesting that activities on Reddit may have served as a testing ground for those on Twitter. Examples of other fruitful methodological applications include the use of network mapping and statistical network analysis. Network modeling should be used more often by scholars because it allows an analysis of clustering and synchronization, which can yield insights on both interdependence across accounts and information flow in social media by identifying influential sources and the links between influential accounts and others on social media.[141] Newer work has also utilized simulations and dynamic modeling to unveil underpinning themes. One study,[142] for example uses Monte Carlo simulations and Dynamic Exploratory Graph

[137] Martin et al. (2023).
[138] Bastos et al. (2021)
[139] Alieva et al. (2022) utilize digital content analysis, Bot hunting to identify bots, and social text analysis to identify networks on social media.
[140] Lukito (2020).
[141] Dawson & Innes (2019) apply these tools to ascertain whether different accounts are controlled by the same author.
[142] Golino et al. (2022).

Analysis to estimate the latent structure of topics published on Twitter accounts. Studies that apply dynamic approaches are in the minority, suggesting another empirical gap that holds promise.

Theoretical and Substantive Issues

Some of the methodological issues covered above have implications for theoretical and substantive gaps in the literature. I enumerate them below.

First, current scholarship places more emphasis on explaining strategic approaches or goals as an outcome rather than explaining effectiveness. While undoubtedly, the focus on approaches/goals provides valuable insights into how states pursue IOs as part of a broader strategic gameplan, whether that is to obtain concessions from target states, expand their sphere of influence, or undermine trust in the target population's faith in democracy, this focus comes at the expense of conceptual development on effectiveness. As such, this is a call for more studies that examine effectiveness as a dependent variable.

Second, there is disproportionate focus on North America and Eastern Europe in the literature on information operations. While this interest is unsurprising given that political developments in these regions have catapulted information campaigns into the limelight, it also draws into sharp relief the scarcity of work focused on other regions. The insights gleaned from existing work can be partially extrapolated to studying IOs in other theaters, with the possibility of amending insights based on region-specific dynamics.

Third, limited attention has been devoted to contextualizing information operations against the broader backdrop of global events or geostrategic phenomena. Thus, the interrelationship between traditional security concepts such as rivalries, geostrategic competition, international crises and IOs remains obscure even though such phenomena have implications for how and when states use IOs to attack adversaries and how states respond to their enemies' use of IOs as an attack. There are a handful of exceptions in the surveyed literature. For example, one study considers China's IOs against the backdrop of the global pandemic, analyzing China's messaging on *Global Times*, and documenting the newspaper's thematic focus on Trump's exploitation of COVID-19 to divert attention away from his leadership failures.[143] Within the state responses literature, another study considers COVID-19 and Russia' invasion of Ukraine as creating windows of high vulnerability, which in turn complicate content moderators' efforts to curate responses to disinformation.[144] While these studies do focus on a global phenomenon to analyze IOs, they do so by viewing the global pandemic as context, rather than variable. Scholars need to integrate global developments into dynamic models of IOs.

A model to follow is the work of Lukito (2020), which explores how interstate dynamics, such as the occurrence of threats in one context can influence when, against and by whom IOs are carried out. While Lukito's analysis does not find that dyadic hostility significantly affects the probability of observing an information operation, it does suggest that IOs could be viewed as a component of a hybrid strategy.

Fourth, while much ink has been spilled on identifying the perpetrators and targets of IOs, we know much less about the timing of these operations. There are, however, a few studies that shed light on

[143] Wilbur (2021).
[144] Morejón-Llamas et al. (2022).

strategic election interference. One such study[145] considers the strategic timing of IOs, for example, around elections (e.g., the 2016 U.S. presidential elections) as a trigger for an IO. Another study[146] differentiates between different types of election interference: interference targeting voting infrastructure and turnout; interference targeting the information environment surrounding elections; and interference built around long-term efforts to erode public trust in government institutions. Crucially, the study also sheds light on target selection by demonstrating that the strategic interests of the attacker are likely associated with different types of election interference.[147] Scholars should follow in the footsteps of this line of inquiry by examining target selection more broadly and explore the strategic timing of IOs. This amounts to answering who gets targeted and when. One way to pursue this line of inquiry would be to expand beyond election interference and identify other windows of vulnerability around other domestic pivotal events, such as sporting competitions. Another path forward would be to outline how the strategic interests of attacker states (e.g., Russia, China) influence target choice.

Fifth, there is a notable gap in examining why some states respond to IOs while others do not. The review of the findings suggests that scholarship on the lack of responses is rather sparse. Scholarship needs to identify the factors that delay or derail effective responses to IO threats. A few studies that document a lack of response on the part of targeted states offer clues on why states may fail to delay a response or fail to mount one altogether.[148] For example, one work[149] examines Russia's use of information operations in Eastern Europe (Hungary, Poland, Slovakia, and the Czech Republic). The study find that Russia has benefited from individuals who are loyal supporters of Putin, those who have business ties with Russia, and right-wing parties that receive financial support from Russia. Additionally, politicians' ties to the Kremlin led to deliberate inaction in some of these states. These findings indicate that the attacker's successful infiltration via financial ties and exploitation of political sympathizers may partially explain inaction on the part of the target state. Other researchers have attributed inaction to the lack of awareness on the part of targeted states that they were being targeted by an IO. They argue that Russia's IO about Brexit jeopardized the British electoral process, as the government remained unaware of a possible IO and subsequently denied the existence of an IO threat. Scholars should also elucidate policies that can mitigate a failure to respond, such as increased preparedness, intelligence gathering, and vigilance.

Sixth, more attention needs to be placed on cases where states outsource information operations to third parties, such as private military companies or mercenaries. Despite growing scholarly interest in mercenaries and private organizations in military conflict,[150] there is scant knowledge of their role in information warfare. Among the extracted empirical articles, only one study has proceeded in this direction, examining how disinformation strategies and narratives vary when they are conducted by state-affiliated entities as opposed to when they are relegated to third parties.[151] The study compared the disinformation strategies of the IRA and the GRU, showing that digital mercenaries utilize more custom-

[145] Lukito (2020).
[146] Hanson et al. (2019).
[147] Thus, Hanson et al. (2019) argue that China's focus has been exclusively on the Indo-Pacific region while Russia has focused on Europe and the Americas.
[148] Čižik (2017); Silvestre et al. (2018).
[149] Čižik (2017).
[150] Akcinaroglu & Radziszewski (2020).
[151] DiResta et al (2022).

tailored, precise techniques, which brought more dividends in terms of engagement than did disinformation tactics that relied on broader language. The conclusions are concerning in showing the cunning and sophistication of digital mercenaries who can harness cutting-edge techniques such as clickbait and attention-grabbing language and syntax (e.g., exclamation points, ellipses, the use of second-person pronouns), in an explicit effort to gain more traction and engagement from social media consumers.

Finally, a noteworthy report[152] lays the groundwork for another promising avenue to explore systems approaches to information operations. In contrast to the dominant paradigm of linear, siloed analysis of information operations, systems analysis takes a holistic perspective to understanding how the building blocks of IOs cohere together. It is particularly well-suited to understanding interconnectedness across social media platforms or among tactics, feedback loops that either counterbalance IOs (e.g., through responses to IOs) or enhance and accelerate them. Furthermore, systems approaches can be adapted separately to analyze IOs wielded by democratic, open systems, and IOs wielded by closed, authoritarian systems. Additionally, a systems approach better equips states with the toolkit for anticipatory policy-formulation. While interest has been most keenly on retroactive responses to IOs, there is a pressing need to shift to developing proactive approaches to IOs.

[152] Brooker (2021).

References

Akcinaroglu, S., & Radziszewski, E. (2020). Private Militaries and the Security Industry in Civil Wars: Competition and Market Accountability. *Oxford University Press.*

Aldrich, R. (2003). Putting Culture Into the Cold War: The Cultural Relations Department (CRD) and British Covert Information Warfare. *Intelligence and National Security*, 18(2), 109-133.

Alieva, I., Moffitt, J.D., & Carley, K.M. (2022). How Disinformation Operations Against Russian Opposition Leader Alexei Navalny Influence the International Audience on Twitter. *Social Network Analysis and Mining*, 12(1), 80.

Allen, T.S., & Moore, A.J. (2018). Victory Without Casualties: Russia's Information Operations. *The US Army War College Quarterly: Parameters*, 48(1), 8.

Arayankalam, J. (2020). Disinformation as a Strategic Weapon: Roles of Societal Polarization, Government's Cybersecurity Capability, and the Rule of Law. *ICIS 2020 Proceedings*, 1-17.

Arif, A., Stewart, L.G., & Starbird, K. (2018). Acting the Part: Examining Information Operations Within #BlackLivesMatter Discourse. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), 1-27.

Bastos, M., & Farkas, J. (2019). "Donald Trump Is My President!": The Internet Research Agency Propaganda Machine. *Social Media & Society*, 5(3), 2056305119865466.

Bastos, M., Mercea, D., & Goveia, F. (2023). Guy Next Door and Implausibly Attractive Young Women: The Visual Frames of Social Media Propaganda. *New Media & Society*, 25(8), 2014-2033.

Beskow, D.M., & Carley, K.M. (2020). Characterization and Comparison of Russian and Chinese Disinformation Campaigns. *Disinformation, Misinformation, and Fake News in Social Media: Emerging Research Challenges and Opportunities*, 63-81.

Bodine-Baron, E.A., Helmus, T.C., Radin, A., & Treyger, E. (2018). Countering Russian Social Media Influence. *Santa Monica: Rand Corporation.*

Boyte, K.J. (2017). An Analysis of the Social-Media Technology Tactics and Narratives Used to Control Perception in the Propaganda War Over Ukraine. *Journal of Information Warfare*, 16(1), 88-111.

Bradshaw, S., & Henle, A. (2021). The Gender Dimensions of Foreign Influence Operations. *International Journal of Communication*, 15, 23.

Bradshaw, S., & Howard, P. N. (2018). The Global Organization of Social Media Disinformation Campaigns. *Journal of International Affairs*, 71(1.5), 23-32.

Bradshaw, S., & Howard, P. N. (2019). The Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation. Oxford Internet Institute.

Brooker, C. (2021). The Effectiveness of Influence Activities in Information Warfare (Doctoral dissertation, UNSW Sydney).

Burns, A., & Eltham, B. (2009). Twitter Free Iran: An Evaluation of Twitter's Role in Public Diplomacy and Information Operations in Iran's 2009 Election Crisis.

Caballero, W. N., Lunday, B. J., Deckro, R. F., & Pachter, M. N. (2020). Informing National Security Policy by Modeling Adversarial Inducement and Its Governance. *Socio-Economic Planning Sciences,* 69, 100709.

Carter, E.B., & Carter, B.L. (2021). Questioning More: RT Outward-Facing Propaganda and the Post-West World Order. *Security Studies*, 30(1), 49-78.

Chang, Y.Y. (2021). The Post-Pandemic World: Between Constitutionalized and Authoritarian Orders–China's Narrative-Power Play in the Pandemic Era. *Journal of Chinese Political Science*, 26(1), 27-65.

Chong, A. (2014). Information Warfare? The Case for an Asian Perspective on Information Operations. *Armed Forces & Society*, 40(4), 599-624.

Čižik, T. (2017). Russian Information Warfare in Central Europe. *Information Warfare–New Security Challenge for Europe*. Bratislava: Centre for European and North Atlantic Affairs, 8-34.

Clements, M.T. (2014). Shock and Awe: The Effects of Disinformation in Military Confrontation. *Policy Studies*, 35(3), 211-220.

Darczewska, J. (2014). Anatomia Rosyjskiej Wojny Informacyjnej. Operacja Krymska—Studium Przypadku. *OSW Ośrodek Studiów Wschodnich im. Marka Karpia.*

Darley, W.M. (2006). Clausewitz's Theory of War and Information Operations. *Joint Force Quarterly*, 40, 73.

Dawson, A., & Innes, M. (2019). How Russia's Internet Research Agency Built Its Disinformation Campaign. *The Political Quarterly*, 90(2), 245-256.

Deibert, R.J., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War. *Security Dialogue*, 43(1), 3-24.

DiResta, R., Grossman, S., & Siegel, A. (2022). In-House vs. Outsourced Trolls: How Digital Mercenaries Shape State Influence Strategies. *Political Communication*, 39(2), 222-253.

Dolan, C.J. (2022). Hybrid Warfare in the Western Balkans: How Structural Vulnerability Attracts Maligned Powers and Hostile Influence. *SEEU Review*, 17(1), 3-25.

Doody, S. (2023). Government Responses to Asymmetric Threats: The State of the Literature on Counterinsurgency from 2002 to 2022—The Information Lever of Power. *START Report*, July, 2023. https://www.start.umd.edu/sites/default/files/publications/local_attachments/SEANFINALINFO_REPORT.pdf

Dowling, M.E. (2022). Foreign Interference and Digital Democracy: Is Digital Era Governance Putting Australia at Risk? *Australian Journal of Political Science*, 57(2), 113-128.

Dowse, A., & Bachmann, S.D. (2022). Information Warfare: Methods to Counter Disinformation. *Defense & Security Analysis*, 38(4), 453-469.

Dumitrescu, L. (2018). The Role of Strategic Narratives in Information Warfare. *Romanian Review of Political Sciences & International Relations*, 15(1), 34-44.

Elswah, M., & Alimardani, M. (2021). Propaganda Chimera: Unpacking the Iranian Perception Information Operations in the Arab World. *Open Information Science*, 5(1), 163-174.

Feng, J. (2022). Chinese Domestic Media Campaigns: Propaganda and Public Opinion in the Digital Age. *Beijing University Press.*

Filipec, O. (2019). Towards a Disinformation Resilient Society? The Experience of the Czech Republic. *Cosmopolitan Civil Societies: An Interdisciplinary Journal*, 11(1), 1-26.

Fitzgerald, C.W., & Brantly, A.F. (2017). Subverting Reality: The Role of Propaganda in 21st Century Intelligence. *International Journal of Intelligence and Counterintelligence*, 30(2), 215-240.

Flake, L. (2020). Russia and Information Warfare: A Whole-of-Society Approach. *Lithuanian Annual Strategic Review*, 18(1), 163-175.

François, C., Nimmo, B., & Eib, C.S. (2019). The IRA Copy Pasta Campaign: Russian Accounts Posing as Americans on Instagram Targeted Both Sides of Polarizing Issues.

Freelon, D., & Wells, C. (2020). Disinformation as Political Communication. *Political Communication*, 37(2), 145-156.

Golino, H., Christensen, A.P., Moulder, R., Kim, S., & Boker, S.M. (2022). Modeling Latent Topics in Social Media Using Dynamic Exploratory Graph Analysis: The Case of the Right-Wing and Left-Wing Trolls in the 2016 US Elections. *Psychometrika*, 1-32.

Gorwa, R., & Guilbeault, D. (2020). Unpacking the Social Media Bot: A Typology to Guide Research and Policy. *Policy & Internet*, 12(2), 225-248.

Greenberg, N. (2021). American Spring: How Russian State Media Translate American Protests for an Arab Audience. *International Journal of Communication*, 15, 22.

Haig, Z., & Hajdu, V. (2017). New Ways in the Cognitive Dimension of Information Operations. *Land Forces Academy Review*, 22(2), 94-102.

Hanson, F., O'Connor, S., Walker, M., & Courtois, L. (2019). Hacking Democracies: Cataloguing Cyber-Enabled Attacks on Elections. ASPI Policy Brief Report No. 16/2019, 1-36.

Harris, K. (2020). Russia's Fifth Column: The Influence of the Night Wolves Motorcycle Club. *Studies in Conflict & Terrorism*, 43(4), 259-273.

Hellman, M., & Wagnsson, C. (2017). How Can European States Respond to Russian Information Warfare? An Analytical Framework. *European Security*, 26(2), 153-170.

Hemment, J. (2022). Satirical Strikes and Deadpanning Diplomats: Stiob as Geopolitical Performance in Russia–US Relations. *PoLar: Political and Legal Anthropology Review*, 45(2), 201-223.

Hindman, M., & Barash, V. (2018). Disinformation "Fake News" and Influence Campaigns on Twitter. *Knight Foundation*. Knight Foundation, October.

Hjorth, F., & Adler-Nissen, R. (2019). Ideological Asymmetry in the Reach of Pro-Russian Digital Disinformation to United States Audiences. *Journal of Communication*, 69(2), 168-192.

Hollis, D. (2018). The Influence of War; The War for Influence. *Temp. Int'l & Comp. LJ*, 32, 31.

Hosaka, S. (2018). The Kremlin's Active Measures Failed in 2013: That's When Russia Remembered Its Last Resort—Crimea. *Demokratizatsiya: The Journal of Post-Soviet Democratization*, 26(3), 321-364.

Howard, P.N., Ganesh, B., Liotsiou, D., Kelly, J., & François, C. (2018). The IRA, Social Media, and Political Polarization in the United States 2012-2018.

Iasiello, E.J. (2017). Russia's Improved Information Operations: From Georgia to Crimea. *The US Army War College Quarterly: Parameters*, 47(2), 7.

Jacuch, A. (2022). The Blurred Lines of Peace and War: An Analysis of Information Operations Used by the Russian Federation in CEE1. *The Journal of Slavic Military Studies*, 35(2), 157-180.

Janda, J., Víchová, V., Richter, M., Sharibzhanov, I., & Fišer, J. (2017). Overview of Countermeasures by the EU28 to the Kremlin's Subversion Operations. *European Values*.

Jensen, B., Valeriano, B., & Maness, R. (2020). Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist. In *Military Strategy in the 21st Century*, 58-80. Routledge: London, UK.

Karasik, T., & Blank, S. (2018). Russia in the Middle East: Implications and Policy Recommendations. *The Jamestown Foundation*, November.

Kargar, S., & Rauchfleisch, A. (2019). State-Aligned Trolling in Iran and the Double-Edged Affordances of Instagram. *New Media & Society*, 21(7), 1506-1527.

Katerynych, P. (2022). Comparative Analysis of the Information Security Environment in Ukraine and Poland (Survey of Journalists and Editors). *Communication & Society*, 35(4), 37-53.

Kuzio, T. (2019). Old Wine in a New Bottle: Russia's Modernization of Traditional Soviet Information Warfare and Active Policies Against Ukraine and Ukrainians. *The Journal of Slavic Military Studies*, 32(4), 485-506.

Larson, E.V., Darilek, R.E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L.H., & Thurston, C.Q. (2009). Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities.

Lin, H., & Kerr, J. (2021). On Cyber-Enabled Information Warfare and Information Operations. *The Oxford Handbook of Cyber Security*, 251.

Lukito, J. (2020). Coordinating a Multi-Platform Disinformation Campaign: Internet Research Agency Activity on Three US Social Media Platforms 2015 to 2017. *Political Communication*, 37(2), 238-255.

Lundberg, J., & Laitinen, M. (2020). Twitter Trolls: A Linguistic Profile of Anti-Democratic Discourse. *Language Sciences*, 79, 101268.

Makarychev, A., & Yatsyk, A. (2021). Europe's Frontline of Information Wars: Russophone Communities in Estonia and Germany. *National Identities*, 23(3), 221-238.

Mälksoo, M. (2020). A Baltic Struggle for a "European Memory": The Militant Mnemopolitics of the Soviet Story. In *The Holocaust/Genocide Template in Eastern Europe* (pp. 48-62). Routledge: London, UK.

Martin, D.A., Shapiro, J.N., & Ilhardt, J.G. (2023). Introducing the Online Political Influence Efforts Dataset. *Journal of Peace Research*, 60(5), 868-876.

Mölder, H., & Sazonov, V. (2018). Information Warfare as the Hobbesian Concept of Modern Times: The Principles, Techniques, and Tools of Russian Information Operations in the Donbass. *The Journal of Slavic Military Studies*, 31(3), 308-328.

Morabito, D. (2021). National Security and the Third-Road Threat: Toward a Comprehensive Theory of Information Warfare. *Air & Space Power Journal*, 35(3), 19-39.

Morejón-Llamas, N., Martín-Ramallal, P., & Micaletto-Belda, J.P. (2022). Twitter Content Curation as an Antidote to Hybrid Warfare During Russia's Invasion of Ukraine. *Profesional de la Información*, 31(3).

Murinska, S., Aleksandrova, O., & Dodonov, R. (2018). Information Warfare: Future Challenges of Latvia and Ukraine. *Skhid*, 5(157), 66-72.

Notaker, H. (2022). In the Blind Spot: Influence Operations and Sub-Threshold Situational Awareness in Norway. *Journal of Strategic Studies*, 46(3), 595-623.

Pamment, J., & Agardh-Twetman, H. (2019). Can There Be a Deterrence Strategy for Influence Operations? *Journal of Information Warfare*, 18(3), 123-135.

Pan, C., & Hagström, L. (2021). Ontological (In)Security and Neoliberal Governmentality: Explaining Australia's China Emergency. *Australian Journal of Politics & History*, 67(3-4), 454-473.

Polyakova, A., Laruelle, M., Meister, S., & Barnett, N. (2016). The Kremlin's Trojan Horses: Russian Influence in France, Germany, and the United Kingdom. Washington D.C: Atlantic Council.

Radziszewski, E., Doody, S., Pate, A., Bouziani, S., & Room, M. (2023). Government Responses to Asymmetric Threats: The State of the Literature on Counterinsurgency From 2002 to 2022. *START Report*, January 2023. https://www.start.umd.edu/publication/government-responses-asymmetric-threats-state-literature-counterinsurgency-2002-2022-2.

Raymond, G.V. (2020). Religion as a Tool of Influence. *Contemporary Southeast Asia*, 42(3), 346-371.

Rațiu, A., & Muntenau, A. (2018). Hybrid Warfare and the Russian Federation Informational Strategy to Influence Civilian Population in Ukraine. *Land Forces Academy Review*, 23(3), 192-200.

Sander, B. (2019). Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections. *Chinese Journal of International Law*, 18(1), 1-56.

Sandra, M., Olena, A., & Roman, D. (2018). Information Warfare: Future Challenges of Latvia and Ukraine. *Skhid*, 157(5).

Sartonen, M., Huhtinen, A.M., & Lehto, M. (2016). Rhizomatic Target Audiences of the Cyber Domain. *Journal of Information Warfare*, 15(4), 1-13.

Shackelford, S.J., Raymond, A., Stemler, A., & Loyle, C. (2020). Defending Democracy: Taking Stock of the Global Fight Against Digital Repression, Disinformation, and Election Insecurity. *Wash. & Lee L. Rev.*, 77, 1747.

Silvestre, R. (2022). Protection of Democratic Processes and Electoral Acts From Russian Digital Active Measures: 2016 as a Reference Year. *Janus. Net e-Journal of International Relations*, 13, 19-35.

Starbird, K. (2020). Information Operations and Online Activism Within "NATO" Discourse. In *Three Tweets to Midnight: Effects of the Global Information Ecosystem on the Risk of Nuclear Conflict* (pp. 79-111).

Sukhankin, S. (2019). The Western Alliance in the Face of the Russian (Dis)Information Machine: Where Does Canada Stand? *The School of Public Policy Publications, University of Calgary*, 12.

Šukyté, D. (2017). Russian Information Warfare in the Baltic States and Possibilities to Resist. In *Information Warfare–New Security Challenge for Europe* (pp. 116-138). Bratislava: Centre for European and North Atlantic Affairs.

Templeman, K. (2020). How Taiwan Stands Up to China. *Journal of Democracy*, 31(3), 85-99.

Thornton, R., & Karagiannis, M. (2016). The Russian Threat to the Baltic States: The Problems of Shaping Local Defense Mechanisms. *The Journal of Slavic Military Studies*, 29(3), 331-351.

Van Niekerk, B., & Maharaj, M.S. (2011). The Information Warfare Life Cycle Model. *South African Journal of Information Management*, 13(1), 1-9.

Van Noort, C. (2020). Strategic Narratives, Visuality, and Infrastructure in the Digital Age: The Case of China's Maritime Silk Road Initiative. *Cambridge Review of International Affairs*, 33(5), 734-751.

Veebel, V., Ploom, I., & Sazonov, V. (2021). Russian Information Warfare in Estonia and Estonian Countermeasures. *Lithuanian Annual Strategic Review*, 19(1).

Veljovski, G., Taneski, N., & Dojchinovski, M. (2017). The Danger of "Hybrid Warfare" From a Sophisticated Adversary: The Russian "Hybridity" in the Ukrainian Conflict. *Defense & Security Analysis*, 33(4), 292-307.

Wang, F.Y. (2021). Barking Without Biting: Understanding Chinese Media Campaigns During Foreign Policy Disputes. *Security Studies*, 30(4), 517-549.

Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking. *Strasbourg: Council of Europe*.

Watanabe, K. (2017). The Spread of the Kremlin's Narratives by a Western News Agency During the Ukraine Crisis. *The Journal of International Communication*, 23(1), 138-158.

Weedon, J., Nuland, W., & Stamos, A. (2017). Information Operations and Facebook. Retrieved from Facebook: https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

Wilbur, D. S. (2021). Enlisting Propaganda for Agenda Building." *Journal of Information Warfare* 20(1), 82-95.

Winkler, J.R. (2009). Information Warfare in World War I. *The Journal of Military History*, 73(3), 845-867.

Yang, A. (2019). Reflexive Control and Cognitive Vulnerability in the 2016 US Presidential Election. *Journal of Information Warfare*, 18(3), 99-122.

Zannettou, S., Caulfield, T., Bradlyn, B., De Cristofaro, E., Stringhini, G., & Blackburn, J. (2020). Characterizing the Use of Images in State-Sponsored Information Warfare Operations by Russian Trolls on Twitter. In *Proceedings of the International AAAI Conference on Web and Social Media*, 14, 774-785.

Appendix A: Literature Extraction Guide

Extraction Manual for Information Operations Database

Identification Variables:

All the relevant literature sources were transferred to a collaborative Zotero library, an open-source reference management software. Each bibliographic entry in Zotero was assigned a unique system-generated key and contained a PDF copy of the publication. Additionally, each Zotero entry contains metadata about each publication, such as the author, year of publication, type of publication, among other features. The bibliography forms the basis for identification variables. Initially, each piece of literature has a single line entry. However, additional lines are added as needed, duplicating the identification variables listed, in order to properly reflect the number of research questions and associated hypotheses in the publication.

Extractor (Extractor Name): Text entry. Enter your name to "claim" the work for extraction.

Key: Alphanumeric. Unique ID linked to Zotero.

Publication Type: Text. From Zotero.

Publication Year: YYYY. From Zotero

Author: Text. From Zotero

Publication Title: Text. From Zotero

Research Questions & Hypotheses

1. **RQ** (Research Question): Text entry.
    - Record the research question from the publication
    - If there are multiple research questions, add additional rows(s) for each question.
    - If there are no research questions explicitly stated, but one or more research questions can be inferred, enter the inferred research question followed by the text (inferred). If the publication is a review article (Y is coded for REVIEWARTICLE) and there is no research question, enter -99.

2. **H** (Hypothesis): Text entry.
    - Record the hypothesis associated with the research question.
    - If there are multiple hypotheses but they are "mirrors" (i.e., the same relationship is hypothesized to be both negative and positive, based on different theoretical considerations), enter as a single hypothesis.
    - If no hypotheses are explicitly stated, but one or more can be inferred, enter the inferred hypotheses followed by the text, (inferred). If the publication is a review article (Y is coded for REVIEWARTICLE) or a theoretical piece (Y is coded for THEORYONLY) and there is no hypothesis, enter -99.

Variables

What variables (qualitative or quantitative) are included in the analysis to test the hypothesis? If you are inferring variables, enter -99 for the fields below and follow instructions in the "Inferred Variables" section.

3. **VARDEP** (Dependent variable): text entry. Brief description of the variable and proxy variables that might be used to capture it.
4. **VARIND** (Independent variable): text entry. Brief description of the variable and proxy variables that might be used to capture it.
5. *Coded but not included in the portal database:*
6. **VARCON** (Control variables): text entry. Brief description of the variable(s) and proxy variable(s) that might be used to capture it. If there are no control variables, enter -99.

Inferred Variables

For articles that don't specifically mention their variables and you need to infer them based on the article's core focus, enter text and follow the same rules as above. If you did not infer any variables, enter -99 for each field.

7. **VARDEPINFER** (see rules above for VARDEP)
    - Inferred dependent variable(s).
8. **VARINDEPINFER** (see rules above for VARIND)
    - Inferred independent variable(s).
9. *Coded but not included in the portal database:* **VARCONINFER** (see rules above for VARCON)
    - Inferred control variable(s). Use syntax for **INDV** above.

Methodological Information

10. *Coded but not included in the portal database:* **DATA:** text entry. Enter any data sets used (for QUAN or quantitative pieces), including which variables relate to each data set.
11. **THEORYONLY**: Is the item only theoretical and without empirical tests? Y/N
12. **REVIEWARTICLE**: Is the publication a review article? Y/N
13. **FINDING:** text entry. For empirical pieces only (Y is coded for QUAL, QUANT, or MATHMOD variables). Provide explanation of key findings related to the hypothesis and/or research

questions. Be sure to note the finding as it relates to independent variables that are tested. If the piece is not empirical, enter -99.

14. **THEORYEXPLANATION:** text entry. For theoretical pieces only (Y is coded for THEORYONLY). Provide a brief description of key ideas about the phenomena that are explained, cause and effect relationships. If the piece is not theoretical, enter -99.

15. **REVIEWSUMMARY:** text entry. For review articles only (Y is coded for REVIEWARTICLE). Provide a brief description of key insights from the review. If the piece is not a review article, enter -99.

Method of analysis: For empirical pieces, what method(s) are used to test the hypothesis being coded?

16. **QUAL** (Qualitative): Y/N

17. **QUALDES** (Qualitative Method Description): Text entry for specific method(s).

18. **QUAN** (Quantitative): Y/N

19. **QUANDES** (Quantitative Method Description): Text entry for specific method(s)

20. **MATHMOD** (Formal mathematical modeling): Y/N

21. **MATHMODDES** (Formal mathematical modeling description): Text entry for specific method(s)

Temporal coverage

22. **START (**Start Year): YYYY entry. For pieces with no stated temporal focus, enter -99.

23. **END** (End Year): YYYY entry. For pieces with no stated temporal focus, enter -99.

Geographic Coverage

24. **GEOSCOPE** Scope of geographic coverage: where the attack is taking place and/or where the response to attack is taking place:

1. Subnational in a single country
2. Single Country
3. Two Countries (in cases where there is attack and counter response)
4. Multiple countries in a single region (defined as DOD region)
5. Multiple countries in multiple regions (defined as DOD region)
6. Global

-99. No specific geographic focus (e.g., in some theoretical and review pieces)

25. **UNGEO** (UN Geographic Subregion): Y/N for each region coverage, where the attack is taking place and/or where the response to attack is taking place:

015 Northern Africa (Algeria, Egypt, Libya, Morocco, Sudan, Tunisia, Western Sahara)

014 Eastern Africa (British India Ocean Territory, Burundi, Comoros, Djibouti, Eritrea, Ethiopia, French Southern Territories, Kenya, Madagascar, Malawi, Mauritius, Mayotte, Mozambique, Reunion, Rwanda, Seychelles, Somalia, South Sudan, Uganda, Tanzania, Zambia, Zimbabwe)

017 Middle Africa (Angola, Cameroon, Central African Republic, Chad, Congo, DRC, Equatorial Guinea, Gabon, Sao Tome and Principe)

018 Southern Africa (Botswana, Eswatini, Lesotho, Namibia, South Africa)

011 Western Africa (Benin, Burkina Faso, Cabo Verde, Cote d'Ivoire, Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Mauritania, Niger, Nigeria, Saint Helena, Senegal, Sierra Leone, Togo)

029 Caribbean (Anguilla, Antigua and Barbuda, Aruba, Bahamas, Barbados, Bonaire, Sint Eustatius and Saba, British Virgin Islands, Cayman Islands, Cuba, Curacao, Dominica, Dominican Republic, Grenada, Guadeloupe, Haiti, Jamaica, Martinique, Montserrat, Puerto Rico, Saint Barthelemy, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Sint Maarten, Trinidad and Tobago, Turks and Caicos Islands, U.S. Virgin Islands)

013 Central America (Belize, Costa Rica, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, Panama)

005 South America (Argentina, Bolivia, Bouvet Island, Brazil, Chile, Colombia, Ecuador, Falkland Islands, French Guiana, Guyana, Paraguay, Peru, South Georgia and the South Sandwich Islands, Suriname, Uruguay, Venezuela)

021 Northern America (Bermuda, Canada, Greenland, Saint Pierre and Miquelon, United States of America)

010 Antarctica

143 Central Asia (Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan)

030 Eastern Asia (China, China-Hong Kong, China-Macao, North Korea, Japan, Mongolia, South Korea)

035 Southeastern Asia (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar/Burma, Philippines, Singapore, Thailand, Timor-Leste, Vietnam)

034 Southern Asia (Afghanistan, Bangladesh, Bhutan, India, Iran, Maldives, Nepal, Pakistan, Sri Lanka)

145 Western Asia (Armenia, Azerbaijan, Bahrain, Cyprus, Georgia, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia, Palestine, Syria, Turkey, UAE, Yemen)

151 Eastern Europe (Belarus, Bulgaria, Czech Republic, Hungary, Poland, Moldova, Romania, Russia, Slovakia, Ukraine)

154 Northern Europe (Aland Islands, Channel Islands, Denmark, Estonia, Faroe Islands, Finland, Iceland, Ireland, Isle of Man, Latvia, Lithuania, Norway, Svalbard and Jan Mayen Islands, Sweden, UK)

039 Southern Europe (Albania, Andorra, Bosnia and Herzegovina, Croatia, Gibraltar, Greece, Holy See, Italy, Kosovo, Malta, Montenegro, North Macedonia, Portugal, San Marino, Serbia, Slovenia, Spain)

155 Western Europe (Austria, Belgium, France, Germany, Liechtenstein, Monaco, Netherlands, Switzerland)

009 Oceania (American Samoa, Australia, Christmas Island, Cocos Islands, Cook Islands, Fiji, French Polynesia, Guam, Heard and McDonalds Islands, Kiribati, Marshall Islands, Micronesia, Nauru, New Caledonia, New Zealand, Niue, Norfolk Island, Northern Mariana Islands, Palau, Papua New Guinea, Pitcairn, Samoa, Solomon Islands, Tokelau, Tonga, Tuvalu, Vanuatu, Wallis and Futuna Islands, U.S. Minor Outlying Islands)

-99 No specific geographic focus (e.g., in some theoretical and policy publications)

26. **DODGEO** (DOD Combatant Command AOR): Y/N for each region coverage, where the attack is taking place and/or where the response to attack is taking place:

1. **AFRICOM** (Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Cote d'Ivoire, Djibouti, DRC, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea Bissau, Kenya, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Republic of the Congo, Rwanda, Sao Tome and Principe, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, Sudan, Tanzania, Togo, Tunisia, Uganda, Zambia, Zimbabwe)
2. **CENTCOM** (Egypt, Israel, Jordan, Syria, Iraq, Kuwait, Saudi Arabia, Bahrain, Qatar, United Arab Emirates, Oman, Yemen, Iran, Turkmenistan, Lebanon, Uzbekistan, Kazakhstan, Kyrgyzstan, Tajikistan, Afghanistan, and Pakistan)
3. **EUCOM** (Albania, Germany, Montenegro, Andorra, Greece, Netherlands, Armenia, Holy See (the Vatican), Norway, Austria, Hungary, Poland, Azerbaijan, Iceland, Portugal, Belarus, Ireland, Romania, Belgium, Russia, Bosnia and Herzegovina, Italy, San Marino, Bulgaria, Kosovo, Serbia, Croatia, Latvia, Slovakia, Cyprus, Lichtenstein, Slovenia, Czech Republic, Lithuania, Spain, Denmark, Luxembourg, Sweden, Estonia, Macedonia, Switzerland, Finland, Malta, Turkey, France, Moldova, Ukraine, Georgia, Monaco, United Kingdom)
4. **INDOPACOM** (American Samoa, Australia, Bangladesh, Bhutan, Brunei, Cambodia, China, Christmas Island, Cocos Islands, Cook Islands, Fiji, French Polynesia, Guam, Heard and McDonalds Islands, Hawaii, India, Indonesia, Japan, Kiribati, Laos, Malaysia, Maldives, Marshall Islands, Micronesia, Mongolia, Myanmar, Nauru, Nepal, New

Caledonia, New Zealand, Niue, Norfolk Island, North Korea, Northern Mariana Islands, Palau, Papua New Guinea, Pitcairn, Samoa, Singapore, Solomon Islands, South Korea, Sri Lanka, Thailand, Timore-Leste, Tokelau, Tonga, Tuvalu, Vanuatu, Vietnam, Wallis and Futuna Islands, U.S. Minor Outlying Islands, Philippines)

5. **NORTHCOM** (continental United States, Alaska, Bahamas, Bermuda, Canada, Mexico, Puerto Rico, Turks and Caicos)
6. **SOUTHCOM** (Antigua and Barbuda, Argentina, Barbados, Belize, Bolivia, Brazil, British Virgin Islands, Cayman Islands, Chile, Colombia, Costa Rica, Cuba, Dominica, Dominican Republic, Ecuador, El Salvador, Falkland Islands, Grenada, Guadeloupe, Guatemala, Guyana, Haiti, Honduras, Jamaica, Martinique, Netherlands Antilles, Nicaragua, Panama, Paraguay, Peru, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, Trinidad and Tobago, Uruguay, U.S. Virgin Islands, Venezuela)

   -99 No specific geographic focus (e.g., in some theoretical and policy publications)

If there are five or fewer countries included in the analysis of where the attack is taking place and/or where the response to attack is taking place, please enter the relevant COW country code (list starts on next page) for each included country.

27. **COUN1**

28. **COUN2**

29. **COUN3**

30. **COUN4**

31. **COUN5**

StateNme	CCode	StateNme	CCode	StateNme	CCode
Afghanistan	700	Grenada	55	Panama	95
Albania	339	Guatemala	90	Papal States	327
Algeria	615	Guinea	438	Papua New Guinea	910
Andorra	232	Guinea-Bissau	404	Paraguay	150
Angola	540	Guyana	110	Parma	335
Antigua & Barbuda	58	Haiti	41	Peru	135
Argentina	160	Hanover	240	Philippines	840
Armenia	371	Hesse Electoral	273	Poland	290
Australia	900	Hesse Grand Ducal	275	Portugal	235
Austria	305	Honduras	91	Qatar	694
Austria-Hungary	300	Hungary	310	Republic of Vietnam	817
Azerbaijan	373	Iceland	395	Romania	360
Baden	267	India	750	Russia	365
Bahamas	31	Indonesia	850	Rwanda	517
Bahrain	692	Iran	630	Samoa	990
Bangladesh	771	Iraq	645	San Marino	331
Barbados	53	Ireland	205	Sao Tome and Principe	403
Bavaria	245	Israel	666	Saudi Arabia	670
Belarus	370	Italy	325	Saxony	269
Belgium	211	Ivory Coast	437	Senegal	433
Belize	80	Jamaica	51	Seychelles	591
Benin	434	Japan	740	Sierra Leone	451
Bhutan	760	Jordan	663	Singapore	830
Bolivia	145	Kazakhstan	705	Slovakia	317
Bosnia and Herzegovina	346	Kenya	501	Slovenia	349
Botswana	571	Kiribati	946	Solomon Islands	940
Brazil	140	Korea	730	Somalia	520
Brunei	835	Kosovo	347	South Africa	560
Bulgaria	355	Kuwait	690	South Korea	732
Burkina Faso	439	Kyrgyzstan	703	South Sudan	626
Burundi	516	Laos	812	Spain	230
Cambodia	811	Latvia	367	Sri Lanka	780
Cameroon	471	Lebanon	660	St. Kitts and Nevis	60
Canada	20	Lesotho	570	St. Lucia	56
Cape Verde	402	Liberia	450	St. Vincent & Grenadines	57
Central African Republic	482	Libya	620	Sudan	625
Chad	483	Liechtenstein	223	Suriname	115

Chile	155	Lithuania	368	Swaziland	572
China	710	Luxembourg	212	Sweden	380
Colombia	100	Luxembourg	212	Switzerland	225
Comoros	581	Macedonia	343	Syria	652
Congo	484	Madagascar	580	Taiwan	713
Costa Rica	94	Malawi	553	Tajikistan	702
Croatia	344	Malaysia	820	Tanzania	510
Cuba	40	Maldives	781	Thailand	800
Cyprus	352	Mali	432	Togo	461
Czech Republic	316	Malta	338	Tonga	955
Czechoslovakia	315	Marshall Islands	983	Trinidad and Tobago	52
Dem Republic of the Congo	490	Mauritania	435	Tunisia	616
Denmark	390	Mauritius	590	Turkey	640
Djibouti	522	Mecklenburg Schwerin	280	Turkmenistan	701
Dominica	54	Mexico	70	Tuscany	337
Dominican Republic	42	Modena	332	Tuvalu	947
East Timor	860	Moldova	359	Two Sicilies	329
Ecuador	130	Monaco	221	Uganda	500
Egypt	651	Mongolia	712	Ukraine	369
El Salvador	92	Montenegro	341	United Arab Emirates	696
Equatorial Guinea	411	Morocco	600	United Kingdom	200
Eritrea	531	Mozambique	541	USA	2
Estonia	366	Myanmar	775	Uruguay	165
Ethiopia	530	Namibia	565	Uzbekistan	704
Federated States of Micronesia	987	Nauru	970	Vanuatu	935
Fiji	950	Nepal	790	Venezuela	101
Finland	375	Netherlands	210	Vietnam	816
France	220	New Zealand	920	Wuerttemburg	271
Gabon	481	Nicaragua	93	Yemen	679
Gambia	420	Niger	436	Yemen Arab Republic	678
Georgia	372	Nigeria	475	Yemen People's Republic	680
German Democratic Republic	265	North Korea	731	Yugoslavia	345
German Federal Republic	260	Norway	385	Zambia	551
Germany	255	Oman	698	Zanzibar	511
Ghana	452	Pakistan	770	Zimbabwe	552
Greece	350	Palau	986		

Type of Information Operation

Type of Information Operation. Differentiation between threat/attack initiation and response to threat/attack. Classification based on the article's core focus.

32. **STATERESP** (State response to info op threat/attack): Y/N.
33. **ATTACKERTHREAT** (State initiation of info op threat/attack): Y/N.

Focus of info ops threat/attack:

34. **MILSTATEATTACK** (Military of the state that is threatened/attacked): Y/N
35. **POLSTATEATTACK**(Political/Legal institutions of the state that is threatened/attacked): Y/N
36. **ECONSTATEATTACK** (Economic institutions of the state that is threatened/attacked): Y/N
37. **GENATTACK** (General population of the state that is threatened/attacked): Y/N

Focus of the response to info ops threat/attack:

38. **MILSTATERESP** (Military of the state that is responding): Y/N
39. **MILADVERRESP** (Military of the attacker): Y/N
40. **POLSTATERESP** (Political/Legal institutions of the state that is responding): Y/N
41. **POLADVERRESP** (Political/Legal institutions of the attacker): Y/N
42. **ECONSTATERESP** (Economic institutions of the state that is responding): Y/N
43. **ECONADVERRESP** (Economic institutions of the attacker): Y/N
44. **GENSTATERESP** (General population of the state that is responding): Y/N
45. **GENADVERRESP** (General population of the attacker): Y/N
46. **NORESP** (No response: article explicitly focuses on the state undertaking no response to threat/attack): Y/N

National Lever of Power

Indicate how state(s) respond to attacker's use of information operations (only if the piece is coded Yes for STATERESP).

47. **D** (Diplomatic, the use of negotiation and dialogue and resulting treaties or policies to advance interests): Y/N

48. **DDES** (Description of diplomatic tactics): Text entry

49. **In** (Information, the deployment of information and narrative to shape events, strategies, and perceptions to advance interests): Y/N

50. **INDES** (Description of information tactics): Text

51. **M** (Military, the coercive application or threat of force in order to compel): Y/N

52. **MDES** (Description of military tactics): Text

53. **E** (Economic, the use of economic instruments and policies, including macroeconomic policy, trade policy, and foreign aid, to advance interests): Y/N

54. **EDES** (Description of economic tactics): Text

55. **F** (Financial, involving the use of financial systems, either formal or informal, and typically the denial of access to such systems, to advance interests): Y/N

56. **FDES** (Description of financial tactics): Text

57. **I** (Intelligence, the conversion of diverse data related to the environment, future capabilities and intention, and relevant actors into coherent information to allow decision advantage to advance interests): Y/N

58. **IDES** (Description of intelligence tactics): Text

59. **L** (Law Enforcement, the use of international, foreign, or domestic legal frameworks and their enforcement to advance interests): Y/N

60. **LDES** (Description of law enforcement tactics): Text

61. **DEV** (Development, activities designed to enhance the capacity of the recipient, typically but not exclusively the economic capacity): Y/N

62. **DEVDES** (Description of development tactics): Text

63. **GOV** (Governance, activities designed to enhance the efficacy and legitimacy of institutions): Y/N

64. **GOVDES** (Description of governance tactics): Text

National Consortium for the Study of Terrorism and Responses to Terrorism (START)
University of Maryland, College Park, MD 20740
infostart@umd.edu
www.start.umd.edu