NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

Kalnciema Street 11B, Rīga, LV-1048, Phone: +371 67335467
e-mail: info@stratcomcoe.org

INVITATION TO TENDER

FOR RESEARCH ON RUSSIAN AND CHINESE INFORMATION OPERATIONS

IN KENYA AND SOUTH AFRICA

To be supplied to the NATO Strategic Communications Centre of Excellence (NATO StratCom COE)

Revision	Version 1
Release Date	**29 April 2026**
Issuer	LtCol. Bonnie Golbeck, Staff Officer, NATO StratCom COE
Service providers Response date	**31 May 2026** submitted via e-mail to tender@stratcomcoe.org no later than 23:59 hrs (Eastern European Time zone: UTC +02:00).

Invitation to Tender for Research on Russian and Chinese Information Operations in Kenya and South Africa

You are kindly invited to submit a project proposal to provide research on **Russian and Chinese Information Operations in Kenya and South Africa** focused on the changing perceptions in the case study countries.

To simplify exchange of information regarding this Invitation to Tender (ITT) please nominate a Bid Manager and provide their contact details within your submission.

Please direct any questions regarding the ITT content or process to LtCol. Bonnie Golbeck in writing at Bonnie.Golbeck@stratcomcoe.org. You should not contact other NATO StratCom COE personnel unless asked to do so by the appointed NATO StratCom COE representative.

The NATO StratCom COE makes no obligations in any way to:

1. pay any service provider for an ITT response;
2. award the contract with the lowest price proposal or any service provider;
3. accept any ITT information received from service providers not covering the full set of requirements;
4. include service providers responding to this ITT, in any future invitations;
5. any other commitment to service providers whatsoever.

We look forward to receiving your response.

Yours sincerely,

Bonnie Golbeck, LtCol.

Staff Officer, Operational Support Branch

E-mail address: Bonnie.Golbeck@stratcomcoe.org

Whilst care and attention has been exercised in the preparation of this document, it remains subject to contract, and all warranties, whether expressed or implied by statute, law or otherwise, are hereby disclaimed and excluded.

These limitations are not intended to restrict continued business discussions between the NATO Strategic Communications Centre of Excellence (NATO StratCom COE) and service providers.

Any proposal received by the NATO StratCom COE is subject to contract with the NATO StratCom COE.

Reference A -- *Russian information operations outside of the Western information environment* (Revised version) https://stratcomcoe.org/publications/russian-information-operations-outside-of-the-western-information-environment-revised-version/316

Table of Contents

1. Introduction

1.1. The NATO Strategic Communications Centre of Excellence (NATO StratCom COE), based in Riga, Latvia, contributes to strategic communications capabilities within the NATO Alliance, Allied nations, and Partners. The NATO StratCom COE designs programmes to advance strategic communications doctrine development, harmonization and implementation, conducts research and experimentation to find practical solutions to existing challenges, identifies lessons from applied strategic communications during operations, and enhances training and education efforts and interoperability.

1.2. The NATO StratCom COE is running procurement to conduct research on **Russian and Chinese Information Operations in Kenya and South Africa** focused on the changing perceptions in these case study countries.

1.3. The contract will be awarded within four weeks after the announcement of the winner. The contract shall be completed by 26 February 2027.

2. Background

2.1. In its war against Ukraine, Russia's narratives are being spread and are already resonating in Latin America, Africa and Asia. Previous research efforts have identified detailed descriptions of the tactics, methods, and actors used by both Russia and China for framing the West and Western agendas to adversely influence perceptions in third nations.

2.2. NATO StratCom COE's ongoing research into Russian and Chinese narratives in third nations will now seek to use the identified narratives, themes, and tactics to develop a greater understanding of local perceptions of these narratives.

2.3. This project builds on the results of previous research by the NATO StratCom COE into the case study countries at Reference A in order to develop counter narrative options.

3. Requirements

3.1. The project aims to identify how Western nations could change perceptions around selected Russian and Chinese narratives, especially those related to the war in Ukraine, and the possible implications in the short to medium term (1-3 years), in the case study countries. This will be achieved through validation of the narratives and audiences previously identified in Reference A. Additionally, this will allow for the development of a methodology for audience research. The subsequent audience research will lead to a set of recommendations to counter selected Russian and Chinese narratives.

3.2. The report should serve as practical support to decision-makers and stakeholders of NATO member nations and partners on Russian and Chinese information influence operations and their effects.

3.3. The aim of report is <u>not</u> to establish causality or test effectiveness of Russian and Chinese information influence operations and audience perceptions, but to provide recommendations on how perceptions favouring Russian and/or Chinese false narratives might be changed.

3.4. The main output will be an analytical study (desk study and audience research) which will seek to answer the following research questions:

3.4.1. Desk Study concerning Russia's and China's narratives:

3.4.1.1. Are the narratives identified in *Russian information operations outside of the Western Information Environment* (Reference A) still valid?

3.4.1.2. Are the target audiences previously identified in Reference A still accurate?

3.4.1.3. Does a literature review identify any significant changes to the Reference A conclusions?

3.4.1.4. Using publicly available information, polls or data scraping, what is the current public opinion on these issues?

3.4.1.4.1. Data scraping for social media may be obtained at no cost through the NATO StratCom COE. Bids should include the desired social media networks, date ranges, and either a desire for post or posts and comments. The search would need to be limited to certain accounts or keywords. An expected volume should be indicated. Include a line item in the proposal for outside data procurement in case the NATO StratCom COE cannot meet the data needs. NATO StratCom COE data scraping availability will be announced with contract award.

3.4.1.4.2. AI/LLMs may be used to analyze data for trends and facilitate data analysis in local languages.

3.4.1.5. Which of the identified narratives and audiences lends themselves to further study through audience research as outlined in paragraph 3.4.2.?

3.4.1.5.1. Emphasis should be put on narratives related to Russia's war against Ukraine, and NATO in general.

3.4.1.5.2. Emphasis should be put on audiences that could be considered actors or stakeholders and not just the public at large where able.

3.4.2. Audience analysis on success and mitigation of narratives where public opinion favours Russian and/or Chinese views:

3.4.2.1. What methodology can be used to study successful techniques for changing the perceptions surrounding the chosen narratives?

3.4.2.2. Consider using key insight interviews as outlined in Annex A, and round table group methodology. Those selected for these interviews should be experts in the field and capable of discussing trends across society and not only their personal views.

3.4.3. Based on the finding of the desk study and the audience analysis, provide a set of applicable recommendations regarding:

3.4.3.1. Which Russian and/or Chinese narratives can be countered?

3.4.3.2. How to change audience perceptions around the studied narratives?

3.5. The deliverables include the following:

3.5.1. In cooperation with the NATO StratCom COE, develop a methodology to assess the stated research questions above. Methodological development should not start anew but focus on refining the methodologies used in Annex 1 to create the correct balance. All methodological developments shall be reviewed and approved by the NATO StratCom COE prior to execution.

3.5.2. Develop conclusions and recommendations.

3.5.3. Produce a report of up to 10,000 words (excluding references, footnotes/endnotes), to include an executive summary, relevant findings from the desk study, an overview of the research questions and methodologies, a summary of the analytical findings from audience research, and conclusions and recommendations.

3.5.4. Be prepared to deliver briefing(s) of the key findings of the research to cross-government stakeholders and civil society actors, as relevant, organized and funded by the NATO StratCom COE.

3.6. The research should be published by the NATO StratCom COE on its website and possibly in printed form.

3.7. NATO StratCom COE is looking to contract one service provider to implement all deliverables listed above. The service provider must provide all parts (paragraph 3.5.) of the research. The service provider is encouraged to partner or subcontract with experts and/or NGOs in the countries or regions covered by the report in order to analyse and interpret data, conduct interviews (as relevant), and disseminate the outputs.

3.8. The service provider is expected to actively solicit and integrate inputs by the NATO StratCom COE by applying a fully transparent and inclusive process throughout the project period. This may include overseeing additional contributors in order to ensure, in particular, the application of the common methodology and the overall coherence of the output.

3.9. The NATO StratCom COE suggests the employment of advanced information environment monitoring tools, which allow analysis in local languages.

3.10. The service provider is expected to participate in a review process of the submitted report and incorporate feedback from the NATO StratCom COE into the work, and offer suggestions and data for graphs, illustrations and supporting material for the final publication of the report.

3.11. The service provider is expected to submit the analytical study in academic English language, providing appropriate referencing, following the NATO StratCom COE style guide. The NATO StratCom COE is responsible for the final English language editing as necessary, the layout, and the printing of the publication as decided.

3.12. The service provider is expected to provide relevant data sets produced in the research process (for example, data collected through analytical tools, documents, publications, interviews, surveys, etc.).

3.13. The service provider is expected to facilitate the application of the methodology in further research, including by other stakeholders, and participate in a potential methodology review in 2027 as decided by the NATO StratCom COE.

4. Reporting (timings approximate)

4.1. Meet to clarify and confirm the approach, scope, research objectives and delivery process as soon as the tender has been awarded (via videoconference or other means).

4.2. Submit methodology for review and comments within one month of signing the contract.

4.3. Submit summary of literature review and top critical narratives in each country concerned based on initial data collection with a recommendation of which to select for further study and proposed methodology for audience research no later than **24 September, 2026**.

4.4. Initial draft of the report (including raw data) no later than **6 January 2027**.

4.5. Final report (including data sets) delivered for review and comments no later than **26 February 2027.**

4.6. NATO StratCom COE may request progress updates and chapter reviews throughout the project period.

5. Tender Submission

5.1. The tender submission should consist of:

5.1.1. A brief written proposal (up to 7 pages) for the delivery of the work specified in paragraphs 3.4 and 3.5 (see Section 3, Requirements). The proposal should be based on the methodology in Annex 1. It should outline a conceptual approach toward conducting the analysis of the case study countries to deliver the required results;

5.1.2. The proposal should include the desired social media networks, date ranges, and either a desire for post or posts and comments. The search would need to be limited to certain accounts or keywords. An expected volume should be indicated. Include a line item in the

proposal for outside data procurement in case the NATO StratCom COE cannot meet the data needs. NATO StratCom COE data scraping availability will be announced with contract award.

5.1.3. Describe the information environment analysis tools the service provider intends to use in producing the report, and include links to previous research using such tools if available.

5.1.4. A total budget for the full proposal and a budget breakdown, in EUROS (with VAT and without VAT; other tax must be clearly specified for each budget position, marked as zero where not applicable). Provide budget estimates for each output, indicating the costs for:

5.1.4.1. Methodology review;

5.1.4.2. Case studies of Kenya and South Africa– include individual breakdown per country and potentially a breakdown by different research methods chosen for desk study and audience research;

5.1.4.3. A separate line item for data collection in the event the NATO StratCom COE cannot scrape the data; and

5.1.4.4. Report production.

5.1.4.5. The budget should include milestones for suggested payments.

5.1.5. Copy of service provider's Certificate issued by the national Commercial Register or a National Register covering other types of legal entity (for example, civil society organisations). If that is not applicable (for example, the Service provider is an individual), please provide an explanatory statement and a different form of a document confirming your identity.

5.2. Evidence of previous relevant work experience from the last three years, e.g. links to publicly available sources.

5.3. Information regarding persons or entities that the service provider may choose to sub-contract for work on the Contract delivery (company or person's name, other relevant credentials, e.g. company registration number, website address, contacts, etc., and a short company profile or person's biography).

6. Timetable

General	
Deadline for submission	**31 May 2026 by 23:59 hrs** (Eastern European Time zone: UTC +02:00)
Contract implementation period	Upon agreement
Questions	Questions arising from this document should be addressed to LtCol. Bonnie Golbeck until **25 May 2026** at the latest.
Full contact details	LtCol. Bonnie Golbeck, Bonnie.Golbeck@stratcomcoe.org

7. Respondent Instructions

7.1. A written proposal is required that complies with the indicated requirements (see Section 5, Tender Submission). The proposal should be submitted electronically using an official email of the entity, in PDF format.

7.2. The file(s) should be submitted to: tender@stratcomcoe.org by 23:59 hrs Eastern European Time zone (UTC +2 hrs) on **31 May 2026**.

7.3. Submissions after the deadline will not be considered. Proposals must be submitted exclusively to the designated submission address. Any proposal sent to a different address will not be accepted or taken into consideration.

7.4. The service provider is expected to supply the required information or state clearly any reason for being unable to do so.

7.5. Any assumptions used in preparing responses should be clearly stated. Any appropriate supporting documents (brochures, demo videos, presentations) should be included.

7.6. If any of the requirements specified in Section 3 (Requirements) are not met, or if any of the requested documents in Section 5 (Tender Submission) are not submitted, the Contract Award Committee reserves the right to exclude the service provider from further participation in the procurement.

7.7. The Contract Award Committee reserves the right to reject any proposal that is considered abnormally low, including in cases where the service provider fails to provide a satisfactory justification for the proposed price upon request.

7.8. Questions relating to clarification of the ITT will only be accepted in writing to NATO StratCom COE representative. Likewise, all responses from the NATO StratCom COE will be written and may also be made available to other service providers (subject to confidentiality). In the event that any answer materially affects the ITT specification, an amendment of the original requirements will be sent to all service providers. The NATO StratCom COE will attempt to answer any questions within two working days of receipt of that request; otherwise it will respond within that timescale notifying the service provider of the estimated time to obtain the information.

7.9. The NATO StratCom COE reserves the right to modify the provisions of this ITT at any time prior to the scheduled date for written responses. Additional scope and requirements can be added. Notification of such changes will be provided to all service providers.

7.10. Should the service provider wish to propose a deviation from the specification please ensure that you clearly identify and highlight where appropriate in your response.

7.11. All information supplied in this tender to date, any further information supplied during the tender process will remain confidential and available only to the Contract Award Committee members.

7.12. The NATO StratCom COE reserves the right to cancel this procurement procedure at any time without awarding a contract.

8. Tender Assessments

8.1. Evaluation Criteria and Process. A set of evaluation criteria has been prepared by the NATO StratCom COE for the evaluation of every submission. At each stage an initial evaluation will consider whether or not every instruction and requirement contained within the ITT has been fulfilled.

8.2. Evaluation criteria is based on “best value”, an objective assessment by the Contract Awarding Committee as to who offers the best combination of price and service. The following is considered:

8.2.1. Cost and budget breakdown;

8.2.2. Quality of service provision (based on the evidence provided);

8.2.3. Previous experience with conducting similar projects; and

8.2.4. Level of compliance with the requirements, reporting and deliverables of the ITT.

8.3. The NATO StratCom COE will continuously assess all interactions with bidders throughout the procurement process, including compliance with the requirements of this ITT and the quality of submissions. The NATO StratCom COE reserves the right, at its sole discretion, to disqualify any bidder whose submission does not comply with the requirements set out in this ITT.

8.4. The NATO StratCom COE reserves the right to modify the scope of this tender, after receiving the bids, to include price estimates.

9. Decision Announcement to Participants

The NATO StratCom COE reserves the right to control the format and content of any such announcement, and to limit it in any way believed by the NATO StratCom COE to be appropriate (which includes the right to not provide any explanation).

10. Contract Details

Contractual and payment details are subject to negotiation with the selected service provider.

INVITATION TO TENDER
FOR RESEARCH ON RUSSIAN AND CHINESE INFORMATION OPERATIONS
IN KENYA AND SOUTH AFRICA

RESEARCH METHODOLOGY

The following text outlines the common methodology applied to the case studies conducted in 2023. For research purposes in 2026, it is expected that this methodology will be reviewed and subsequently applied to further case studies, consistent with the provisions of the Invitation to Tender to which this document is attached. In instances where parameters of research in 2026 differ from those of 2023, such as the selection of case studies or the Research Questions, the Invitation to Tender takes precedence.

The research took the recognised methodology of case study research, analysing "a phenomenon occurring in a bounded context".[1] These phenomena were significant themes within the selected countries. However, if other significant political ramifications were evident, the case studies highlighted these. This approach helped identify the most relevant thematic narratives to address the research questions. All results were validated through triangulation of various sources and methods including digital data collection and analysis; reviews and cross-referencing with existing research; and Key Insight Interviews (KIIs). Some direct quotes from the KIIs have been edited for correct grammar and better understanding.

The research used a mixed method exploratory sequential designed that was empirically driven and inductively based design[2], whereby, for each country, a literature review identified relevant case studies and informed the design of questions for the KIIs, which subsequently informed the quantitative examination of the relevant geographic and temporal digital space by providing on the ground perspective of critical timeframes and events.

This methodology was critically reviewed by the COE community of interest, including through an in-person workshop held in June 2023, and a period for comment and review later that month. After adjustments, the final methodology was submitted and approved in late June.

Research questions

A. Concerning Russia's information operations:

1. To which audiences is communication targeted?
2. Which Russian narratives resonate in the countries concerned?
3. What current and historical circumstances of those affected countries are likely to create a receptive environment to Russian narratives?
4. Who are the main actors of communication?
5. Can targeted operations be identified?
6. What tactics, techniques and procedures are used in these operations?
7. Are local media manipulated and instrumentalised and how?
8. What are the effects of these operations?

B. Concerning Western strategic communications:

1. Which narratives compatible with Western values and interests are working in the countries concerned?
2. Which are the most susceptible audiences?
3. Who are the actors of communication, and can be considered as potential allies?

[1] Huberman, M. and Miles, M. (1994). 'Data management and analysis methods', in *Handbook of qualitative research*, ed. by Norman K. Denzin and Yvonna S. Lincoln. Thousand Oaks, CA: Sage.
[2] Creswell, J. and Plano Clark, V.L. (2011). *Designing and Conducting Mixed Methods Research*. 2nd edn. Thousand Oaks, CA: Sage.

C. What are the short- and medium-term (1-3 years) ramifications for Western countries in terms of:

1. Voting in international bodies including the UN Security Council and UN General Assembly.
2. How have Russia and pro-Russian actors in the region framed the cost-of-living crisis in their favour?
3. How have Russia and pro-Russian actors in the region framed critical national issues in each country?
   a. Egypt – The cost-of-living crisis.
   b. Mali – Security and regime stability.
   c. Kenya – Traditional values and moral decay.
   d. South Africa – The emerging multipolar world order and South Africa's place within it.
   e. United Arab Emirates – Sanctions and unilateral Western economic measures.

Limitations

As specified in the proposal, the literature review and KIIs were largely conducted in English only. This initially limited the sample pool of potential interviewees to solely English speakers. However, given limitations on the number of English speakers in Mali, several interviews were conducted in French.

The data collection and analysis used translation software to translate online social media content in the dominant languages of the specific country. However, such translation might have missed certain nuances. Thus, it was highly unlikely that this software produced highly accurate results for large documents or interview transcription. This created an information gap that limited insight and foresight into the issues being studied under this methodology.

The methodology also had limited scope for on-the-ground research beyond KIIs, which limited the ability to monitor oral media beyond secondary source research. It was likely that this impacted the levels of insight into the select countries, all of which typically had limited independent funding in media and a rich oral tradition that translated to the contemporary information environment.

The data collection and analysis were unable to access closed messaging platforms (e.g., WhatsApp and Telegram). Preliminary secondary source research indicated that such platforms played a critical role in the sharing of information and the spread of disinformation in the selected countries. Being unable to monitor them left an information gap that could only be filled by on-the-ground researchers who could access these platforms or contact those on them directly.

The list of research questions was extensive. The resources allocated to this research did not allow for a definitive examination of all of the research questions. Although the desk research and KIIs attempted to address all of the research questions, qualitative reporting required a degree of inference regarding causality, making key assumptions. Where such inferences were made, they were made explicit in the research report.

Literature review

The literature review was conducted in English or used pre-translated sources only, to establish insight into Russian and Western relations with each country and historical grievances within them, existing information environments in each of the select countries, and Russian information operations. This provided important context to inform the research and identified critical information gaps. The literature review was also used to establish definitions that anchored analysis going forward.

In brief, definitions for this methodology are:

- **Information Influence Operations (IIOs):** The organised attempt by one or more actors to achieve a specific effect among a target audience, often using illegitimate and manipulative behaviour. IIOs draw on communicative tactics such as fabrication, false identities, malign rhetoric, symbolism, and technological advantages to exploit vulnerabilities in the information environment.[3] Can be applied at a strategic narrative level or a tactical targeted level.
- **Propaganda:** Information systematically disseminated by an organisation of actors with the purpose of influencing perceptions in favour of the actors' political narrative. Comes in the shades of **White, Grey and Black.** White is favourable facts. Grey is misleading information (or 'cherry-picked') or from a disguised source to increase its authenticity. Black is outright lies or falsehoods usually disseminated from a disguised source.[4]
- **Disinformation:** False or misleading information spread intentionally by an actor or actors to influence perceptions. Often but not always from a disguised source.[5]
- **Misinformation:** False or inaccurate information spread without malicious intent, although its effects can still be harmful. [6]
- **Malinformation:** Information based on fact but used out of context to mislead, harm, or manipulate.[7]
- **Conspiracy theory:** Information that attempts to explain the ultimate causes of significant social and political events and circumstances with claims of secret plots by two or more powerful actors.[8]

Through the literature review, the research methodology was refined through an extensive examination of the **'**Theory of Reflexive Control' (TORC, see below)[9], aspects of which form a core methodology for modern Russian information operations. Where such inferences were made, they were made explicit in the research report.

This enhanced our understanding of the Kremlin information tactics, techniques, and procedures (TTPs) and how they are scaled from specific events and social groupings all the way to a national or region-wide level.

The analysis of the TORC and Kremlin TTPs were further informed by existing research on Russian information operations. This included directly translated sources such as Messner's theory of 'subversion warfare', Panarin's theory of 'information warfare', and Dugin's theory of 'net-centric warfare.' It also included Western studies of Russian information warfare, including Thomas Rid's 'Active Measures' and previous research by the NATO StratCom COE.

Case studies

Case studies were selected to examine, and thus be representative or typical of specific phenomena, namely Russian IIOs. Case studies were chosen via literal replication logic, as in, they were selected to have similar results (with contextual variations) rather than similar study characteristics.[10]

[3] Pamment, J. and Smith, V. "Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online". NATO Stratcom CoE, July 19, 2022
[4] Guth, D.W. (2009) 'Black, white, and Shades of Gray: The Sixty-year debate over propaganda versus public diplomacy', in *Journal of Promotion Management*, 14(3–4), pp. 309–325. doi:10.1080/10496490802624083.
[5] Rich, M. and Kavanagh, J. (2018) 'Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life'. RAND
[6] NATO (2023). NATO's Approach to Countering Disinformation. NATO
[7] *Foreign influence operations and disinformation* (no date) cisa.gov. Available at: https://www.cisa.gov/topics/election-security#:~:text=Misinformation%20is%20false%2C%20but%20not,mislead%2C%20harm%2C%20or%20manipulate (Accessed: 01 May 2024).
[8] Douglas, K.M. et al. (2019) 'Understanding conspiracy theories' in *Political Psychology*, Vol. 40(1), pp. 3–35. doi:10.1111/pops.12568
[9] Vasara, A. (2020) "Theory of Reflexive Control: Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy". National Defence University, Helsinki
[10] Yin, R.K. (2009) *Case Study Research: Design and Methods*. 4th edn. SAGE

The selection of the proposed case study themes outlined in Table 1 has been based on initial discussions at the COE's workshop held in June 2023, secondary source research and digital analysis. With a focus on energy and food security-linked phenomena, we also prioritised themes where we may see the greatest likelihood of Russian information operations activity and competing narratives.

Table 1: Case Study themes

Country	**Themes**
Mali	Security and regime stability
Kenya	Traditional values and moral decay
Egypt	Cost of living crisis
South Africa	The multipolar world and South Africa's place in it
United Arab Emirates	Sanctions and unilateral Western economic measures

KIIs and qualitative analysis

The KIIs were conducted in English and French and then transcribed for subsequent thematic coding analysis (TCA).[11] They were limited to five per country, (due to time scarcity) unless exceptional circumstances. The selection criteria for potential interviewees included their recent, relevant academic or journalistic output, their political, security communications and/or media specialist knowledge, their local, cultural background and their recent proximity to the geographical area of study. The latter were included as we wished to maximise ground-truth via interviewees with deep and recent experience on the ground, rather than academics far removed from those circumstances, spatially and temporally.

All interviewees were informed of the scope of the research and their consent was requested. Further, their consent to be credited in the final research paper was established. However, for security reasons or otherwise, several interviewees wished to remain anonymous. This will be honoured and a list of those interviewees consenting to being named will be made available separately.

The KIIs were in the format of semi-structured questions over 45-60 minutes, conducted over VOIP systems (Teams, Zoom). Multi-case study protocol ensured that certain questions were common across all interviews, regardless of case study, with other questions designed for the specific case study context.

Digital data collection and analysis

Our approach has differed for each of the core social media platforms and associated large content and news providers that deliver content engagement. The commonality of cause has been combining the views and reach with their associated output in text, image and video formats across these platforms into a comparable dataset.

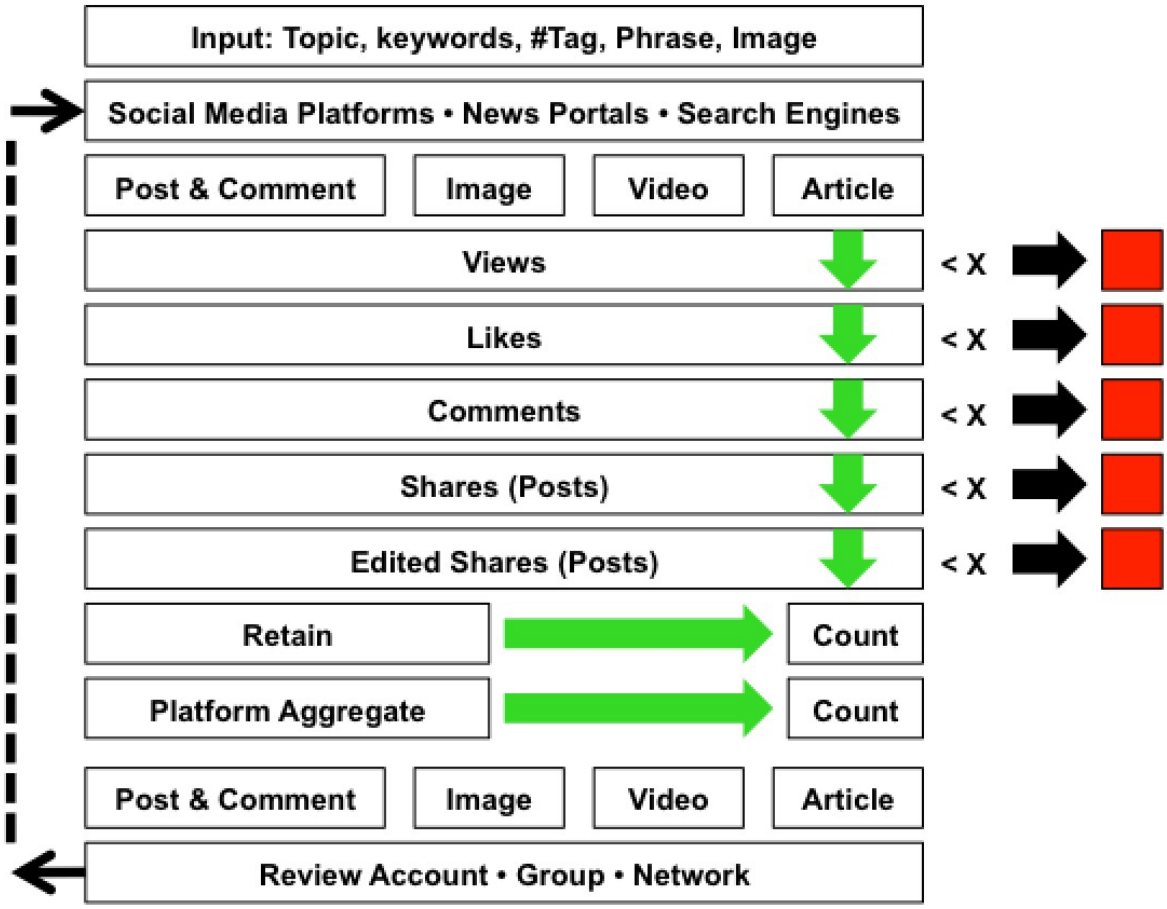
We focused on the time window of 1 January 2022 until 1 September 2023. This covers the build-up of the Ukraine conflict and covering 18 months of the war. All digital media was searched for within the date parameters. For relevance, we used the following parameters: Region, Country, City. Names, Keywords, #HashTags. Once this dataset was established, we sorted by Views, Shares (Posts), Comments and Likes. Our process involved seeking out the source-point and then cascading through the time stamps and collating accounts and organisations that participated in significant engagement.

[11] Saldana, J. (2021) *The Coding Manual for Qualitative Researchers*. SAGE

This has enabled us to centre the analysis around each of the five countries. Our approach uncovered that the largest content metric (be it text, image or video) was produced mostly outside of each country and amplified inside the country concerned. Unsurprisingly the largest media companies and social media 'influencers' from around the world featured heavily in source material prior to in-country engagement. This approach considers the larger diaspora and interested parties across the wider communities worldwide, as none of these analysed search terms remain isolated within the borderless internet. Material reviewed and analysed within the original source from outside of a country was discovered through the process of targeted search profile terms and subsequent engagement using the parameters described above.

The analysis of all material and the presentation of significant material was based on the following metrics; Views, Shares (posts), Re-edited Posts, Comments and Likes. This enabled us to filter out the material that might be seen as interesting, topical, or relevant, but which had no significance in volume and did not engage within the public space. Engagement was our first priority; once the material was extracted, we applied three core data visualisations: (i) Sentiment Analysis (ii) Word Cloud (iii) Emoticon Usage. Visually we have limited this to something that can be readily viewed and understood. We focused on short statements and questions that had garnered a motivational response (engagement) through Comments. These were collected and collated from sources that represented that question or statement. These were then custom analysed through bespoke software and output through a Word Cloud for the Top 100 words, and Parliament Graphs for the Top 10 Emoticons by volume per statement/question.

Figure 1 – Digital data scrape process



The approach we have taken has demonstrated that conversations coalesce around a topic that is often personal to the audience, resonates with the individual and is personality driven. Leaders not countries and their perceived collective personalities, drive the traffic and engagement—Putin before Russia, Zelensky before Ukraine. This played out in the keywords, hashtags and engagement.

Unsurprisingly humour and subversion receive the strongest engagement. Something that individual large-scale global influencers have understood and exploited to the maximum. The most effective social media asks the question, poses an opinion and often delivers the answer. Controversy drives traffic, 'clout' and, therefore, financial gain for all concerned. Outside of the region, media companies and social media influencers drive the conversations. Politically-motivated influencers from another geographical region can, and do, have both immense sway and are often used and amplified for nefarious purposes. The unintended consequences of an ideological viewpoint in one country is being utilised by regimes to support their own narrative elsewhere. This is another definition and an example of the 'useful idiot'. The social media platforms vary widely in their suppression of content, accounts of individuals and organisations. With rulesets operating for different countries, often based on national laws and operating requirements and, through other ideological and political policy reasons, are enforced by the source country, mostly driven by the US.

Parliament graphs have been used to display the percentage of Emoticon Usage as a response in-line or as a response to a question, statement or theme posed within social media. Using the full Emoji Unicode TF8 sets, Emoticons and Emojis have been pattern matched and merged to produce a consistent dataset to run. A simple counting metric was used to generate percentage usage for each Emoji within the analysed comments.

The comments were collected against questions or statements that resonated along the same line of enquiry. This data was collected from all the major social media platforms. The Parliament Graphs do not ensure any analysis of weighting that is used within the Sentiment Analysis, this is purely usage. It is clear to all that the standard three Emojis of; Grinning Face, Grinning Face with Smiling Eyes, Face with Tears of Joy, are used most heavily. These three represent the universal response to agreement and are often used in an ironic way to a statement. As such, contextualisation is important when analysing for Sentiment. It is also worth noting that both mobile devices and the tools provided by the social media companies to respond within a post use a frequently/most frequently used display for the Emoji used by the individual responding. This also generates a positive reinforcement loop for most frequently used Emojis. Therefore, it is worth reviewing the smaller percentages on each Parliament Graph to see more 'nuanced' responses to the questions and statements posed. We restricted the displayed datasets to the Top 10 for both display purposes and because the data often reduced dramatically to an equal weighted number of dozens of minor used Emoticons further down the usage list. The data analysed for each Question, Comment Group consisted of at least 1,000 individual post responses, with some receiving up to 100,000 responses.

RESEARCHING RUSSIAN IIOs: REFINING THE METHODOLOGY

Russian Information Influence Operations (IIOs) have become a growing topic of interest among policymakers, practitioners of information resilience, and the general public since the advent (and weaponisation) of social media and as part of the wider study of dis/mis/mal-information and Russian *gibridnaya voyna* (hybrid warfare). This growing interest in IIOs has yielded positive results in terms of increased resilience and awareness. But, it has also led to the term being redefined and politicised across Western literature. It is therefore necessary to define what we mean by 'IIOs.'

IIOs are defined by the NATO Strategic Communications Centre of Excellence (StratCom COE) as systematic campaigns by one or more actors to achieve a desired effect using a range of online and offline measures, often using illegitimate and manipulative behaviour 'drawing on communicative tactics such as fabrication, false identities, malign rhetoric, symbolism, and technological advantages to exploit vulnerabilities in the

information environment.'[12] However, this definition is not complete, as it implies that such operations exclusively utilise disinformation tactics (black propaganda). But states frequently utilise a blend of propaganda 'shades' (white, grey and black) in their operations. Therefore, this methodology has chosen to expand the definition to include factual information that is beneficial to the disseminator (white propaganda), while acknowledging it frequently comes from a disguised source, as well as misinformation (grey propaganda) and the desire to create a cumulative effect on attitudes and behaviours. IIOs can be applied at a strategic narrative level or a tactical targeted level.

IIOs seek to exploit vulnerabilities in the public information sphere. One of the most common vulnerabilities across the international community is the rise of conspiracy theories as everyday explainers for events.[13] This is particularly true in areas of lower media literacy and with lower levels of trust in government, which was a common factor to varying degrees among the selected countries of study. It was therefore appropriate for the methodology of this study to further define 'conspiracy theories.' By conducting a smaller literature review of several authoritative works on conspiracy theories and public consumptions of them, this methodology arrived at Douglas et. al.'s definition that they are 'information that attempts to explain the ultimate causes of significant social and political events and circumstances with claims of secret plots by two or more powerful actors.'[14]

ANALYSIS USING THE THEORY OF REFLEXIVE CONTROL (TORC)

The Kremlin has always assigned special importance to information-psychological operations[15] with reference to them in both the 2015 National Security Strategy and 2016 Information Security Concept.[16] According to former KGB Maj. Gen. Oleg Kalugin, information operations, rather than intelligence gathering, were the 'heart and soul of Soviet intelligence.'[17] Western information operations are continuously held as responsible for the Soviet Union's collapse by Russian observers,[18] and the so-called Gerasimov Doctrine cited information as a key component of full-spectrum warfare. While primarily a document on military strategy that focuses on measures outside of the traditional military spectrum as a complement to military operations (and therefore out of the scope of this report), it is nevertheless indicative of the centrality of IIOs in the Russian mindset. However, while Gerasimov's paper attracted much attention in the West, the prior resurgence in Information Warfare literature went remarkably unnoticed until the Crimea crisis of 2014. This report analysed three prominent Russian works on the subject highlighted in Fridman's authoritative work on Hybrid Warfare: Evgeny Messner's theory of Subversion Warfare, Igor Panarin's theory of Information Warfare, and Alexander Dugin's theory of Net-centric Warfare.[19]

In the twentieth century, Messner highlighted the shift in warfare from direct military force to manipulating a nation's will through propaganda. This required a blend of 'propaganda by deed', 'propaganda by word' and 'offensive' and 'defensive' propaganda.[20] He also coined the term 'psycho-reconnaissance' to understand the target's socio-cultural context for effective manipulation.[21] Messner also argued that peaceful and aggressive relations were inseparable, implying the necessity for ongoing IIOs.

---

[12] Pamment, J. and Smith, V. "Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online". NATO Stratcom CoE, July 19, 2022

[13] Uscinski, J., Enders, A., Klofstad, C., Seelig, M., Drochon, H., Premaratne, K., & Murthi, M. (2022). "Have beliefs in conspiracy theories increased over time?". *PloS one*, *17*(7), e0270429. https://doi.org/10.1371/journal.pone.0270429

[14] Douglas, K.M. et al. (2019) 'Understanding conspiracy theories', in *Political Psychology*, 40(S1), pp. 3–35.

[15] Abrams,S. (2016) **"**Beyond Propaganda: Soviet Active Measures in Putin's Russia" in Connections: The Quarterly Journal, 15(1), pp 5-31 and Fridman, O. "The Russian Perspective on Information Warfare: Conceptual Roots and Politicisation in Russian Academic, Political, and Public Discourse" Defence Strategic Communications Vol 2 (2017), NATO Stratcom CoE, and Krieg, A. (2023). *Subversion: The Strategic Weaponization of Narratives*. Georgetown University Press, p. 197

[16] Office of the President of the Russian Federation. "Doctrine of Information Security of the Russian Federation". December 5, 2016

[17] Office of the President of the Russian Federation. "Russian National Security Strategy". December 31, 2015

[18] Kello, L. (2017). *The Virtual Weapon and International Order*. Yale University Press.

[19] Fridman, O. (2018) *Russian Hybrid Warfare: Resurgence and politicisation*. Oxford University Press.

[20] Ibid, p. 61

[21] Ibid, p. 69

Though Messner's anti-communist views led to his work being overlooked in Soviet Russia, it has gained prominence in Putin's Russia, particularly in the context of modern IIO theory. His ideas resonate in the works of Dugin and Panarin, although the latter two take a more detailed approach to strategic influence.

Igor Panarin, a political scientist in the Russian Military Academy of Science, aligns with Messner by viewing the informational domain as a critical battleground throughout history.[22] But Panarin broadens the scope by defining three parallel stages of information warfare:

- 'Collection, aggregation and exchange of information on adversaries and allies for the purpose of conducting active actions.'[23]
- 'Infiltration of negative commentaries and disinformation into the informational domain of the adversary' as well as countering any attempt by the adversary to combat it or receive factual information.[24]
- Informational defence – blocking the adversary's attempts to do the same.

He views IIOs not only as a means to enhance national power, but also as a defensive strategy against perceived Western information warfare targeting Russia.[25] Moreover, Panarin argues that information warfare is not exclusive to the military domain; it extends across civilian economic, financial, and diplomatic spheres.

Panarin primarily emphasises exploiting various facets of national power to influence adversaries' decision-making processes through the manipulation of 'social objects', categorising them into groupings of 'large'– such as state-level social classes and professions; 'medium'– such as commercial industries, organisations and military units, and 'small' such as families, small military units, neighbourhoods, etc.

Similarly, Dugin argues that 'reality is secondary to the virtual' due to the fact 'reality itself only becomes real after reports about it appear in the informational dimension.'[26] He extends Messner and Panarin's theories by targeting not only institutional networks but also demographic groups. Dugin advocates for the manipulation of 'natural networks,' such as minorities, through 'agents of influence' and global systems like international institutions and media to propagate favourable narratives.

Fridman succinctly summarises that Dugin's net-centric warfare aims to influence networks to promote specific ideas for political goals. Dugin's theory was adopted to the Command and Control Research Group, which promoted it as a method of enhancing military combat power.[27] However, Dugin sees it as transcending military application, altering the world's political, economic, social, cultural, and anthropological landscape in the ongoing struggle between Eurasian and Atlantic cultures.

Ultimately, Messner's observations on modern warfare heavily influenced later thinkers like Dugin and Panarin, who expanded and detailed the strategies and stages of information warfare, encompassing its use for both offensive influence and defensive protection in the global geopolitical landscape that are evident in modern Kremlin IIOs.

Despite Russian assertions that the West is the original practitioner and even expert on information operations, study of the subject has only entered the popular public domain in the West relatively recently.[28]

[22] Ibid, p. 85
[23] Ibid, p. 86
[24] Ibid, p. 86
[25] Ibid, p. 89
[26] Ibid, p. 78
[27] Alberts D.S., Garstka, J.J. and Stein F.P. (2000), "Network Centric Warfare". DoD C4ISR Cooperative Research Program p.88.
[28] This surge in interest can largely be attributed to the 2014 Crimea crisis, Kremlin informational support of the Assad regime in Syria, and its interference in the 2016 US presidential election campaign. Consequently, recent literature on IIOs is consistently intertwined with literature on Kremlin IIOs.

One of the first things to note regarding Western literature on Russian information operations is an apparent focus on simplicity, or even a lack of strategy, especially in the internet age. Instead, most of the prominent literature focuses on the operational (campaign) and tactical level.

One of the most popular understandings of Russian IIOs (specifically its use of propaganda) is Paul and Matthews's 'Firehose of Falsehood' model, in which Kremlin propaganda is defined by its 'high number of channels and a shameless willingness to disseminate partial truths or outright fictions'. The benefit of this model is that the appearance of multiple sources endorsing the same argument is more persuasive than a single source, especially when within the target's social group. Likewise, repetitiveness creates an illusory effect of truth via a natural tendency by people to use frequency as a metric for truth when confronted with masses of information. Furthermore, removing the obstacle of establishing facts allows the Kremlin to create first impressions, which are resilient to change. Especially when presented through 'peripheral cues' like a professional format.[29]

An equally popular conception is that when confronted in its IIO activities or other malign operations, the Kremlin engages in a simple but effective formula of rebuttal, dubbed by Ben Nimmo as the '4 Ds':[30]

- Dismiss – either by denying the allegations on the ground or denigrating the accuser.
- Distort – misrepresenting information to align with the overarching narrative.
- Distract – launching counter accusations about separate topics to the one being discussed (often in the form of 'whataboutism').[31]
- Dismay – conveying the belief that any opposition to Russian objectives or that achieving objective truth is a hopeless endeavour.

Others have since added a fifth D: Divide – messages designed to create conflict between subgroups and widen divisions within a community.[32] This material is often presented in a manner as to gain an emotional reaction. Content that angers, disgusts, or shocks is more likely to be engaged with according to psychological literature.[33] Likewise, this material also focuses on an entertainment factor, which increases its chances of being shared and gaining positive interactions,[34] as well as achieving a lasting impression on viewers even if untrue.[35]

These narratives are typically disseminated via several methods:

1. **Front organisations:** A seemingly independent entity or group that conceals its true affiliations and aims, serving as a tool in propaganda campaigns. Typically, a front organisation presents itself as separate from the entity it represents or serves, often adopting a benign or relatable facade to gain trust and influence. These fronts are strategically created or manipulated by a controlling entity, such as a government or special interest group, to disseminate propaganda or advance specific agendas. Front organisations engage in activities that appear altruistic or aligned with community interests, allowing them to infiltrate social, cultural, or political spheres.

2. **Agents of influence:** Individuals strategically positioned to promote specific ideas, messages, or agendas within a target audience or society. Their role in propaganda campaigns involves subtly shaping public opinion or decision-making by spreading information, narratives, or ideologies that

[29] Paul, C. and Matthews, M. (2016) "The Russian "Firehose of Falsehood" Propaganda Model". RAND
[30] Corp. S. "Combatting Disinformation with the Four D's". Center for Academic Innovation, University of Michigan, March 8, 2022
[31] Cambridge Dictionary "whataboutism", Cambridge University, n.d.
[32] ADTAC Disinformation Inventory. "The 5D's (dismiss, distort, distract, dismay, divide)". ADTAC, n.d.
[33] Berger, J., & Milkman, K. L. (2012). What Makes Online Content Viral? In *Journal of Marketing Research*, 49(2), pp. 192-205.
[34] Ibid.
[35] Known as the sleeper effect. See Wadwha, P. "Beware of the Sleeper Effect" and Paul, C. and Matthews, M. (2016) "The Russian "Firehose of Falsehood" Propaganda Model". RAND, p.6

align with the propagandist's goals. These agents often exploit their credibility, connections, or authority in various domains, such as media, academia, politics, or social groups, to gain trust and influence over the targeted population. By appearing as independent sources or trusted figures, agents of influence can effectively sway opinions, provoke reactions, and foster an environment conducive to the propagandist's aims, all while maintaining a facade of impartiality or autonomy. These can include 'entrepreneurs of influence'[36] or 'useful idiots'[37] and cynics.[38]

3. **Information laundering:** *RT* and *Sputnik* play a critical role in this form of dissemination. Either by directly producing propaganda content that is then provided to local organisations free of charge or bringing in social media commentary (often linked to pro-Kremlin inauthentic networks) to legitimise a narrative.

4. With the advent of social media, the employment of **sockpuppet profiles** (fake accounts posing as an individual established to manipulate online discussions)[39] and **bot networks** (semi-automated or automated programs that use the normal functions of communications platforms to amplify an existing message)[40] also play an increasingly significant role in dissemination.

In Western literature, Kremlin IIOs are viewed as prioritising quantity over consistent quality messaging. Rid observes that Kremlin IIOs in the digital age have become more active, sacrificing control for increased output and relying on societies to spread propaganda.[41] Dr Rory Cormac emphasises the trade-offs between reach and deniability, highlighting the outsourcing and limited control in IIO strategies.[42] While this suggestion of a 'throw it out and see what sticks' approach to Kremlin IIOs is debatable, what is undenied in Western literature is these operations' effectiveness. The West faces challenges countering these threats while preserving free speech and determining the best deterrent strategy. In his book *Subversion,* Dr Andreas Krieg goes as far to say that 'Russia provides the most sophisticated case study for how states weaponise narratives in an effort to subvert the opponent's information-psychological stability'.[43] And even sceptics like Rid who suggest that usually the impacts of IIOs are overstated acknowledge that the perception of them is such that it helps 'expand and escalate that very threat and its potential'.[44]

Many scholars have successfully utilised these commonalities to create research frameworks for identifying Kremlin TTPs within IIOs. However, these commonly focus on vague outputs like 'winning the information war' or 'muddying the water' rather than the ultimate effects of influencing attitudes, behaviours and, ultimately, decision-making. These risk creating misconceptions that Kremlin IIOs are unguided or lack a strategic goal beyond 'chaos.' Considering our research questions focus not just on narratives but also on opinion and decisions to engage with Russian narratives over Western ones, we chose to use an existing Soviet concept (since revamped in modern Russian IIO strategies), which focuses on creating a cumulative impact on decision-making through information inputs: The Theory of Reflexive Control (TORC).[45]

[36] Defined as people who invest their own money or social capital to build influence abroad in hopes of being rewarded either financially or the reinforcement of their own narrative. See Laruelle, M and Limonier, K. "Beyond "hybrid warfare": a digital exploration of Russia's entrepreneurs of influence" in *Post-Soviet Affairs, Vol 37(4)*, July 17, 2021

[37] Defined in Oxford English dictionary as a person perceived as propagandizing for a cause—particularly a bad cause originating from a devious, ruthless source—without fully comprehending the cause's goals, and who is cynically being used by the cause's leaders. The term was often used during the Cold War to describe non-communists regarded as susceptible to communist propaganda and psychological manipulation.

[38] Differs from a useful idiot by not necessarily believing in the narrative they espouse. For example, Tucker Carlson, the Fox News pundit who has parroted Kremlin talking points, has been revealed in leaked communications to not believe the narratives he puts forward. See Rubin, O. "What Fox News hosts allegedly said privately versus on-air about false election fraud claims". ABC News, April 24, 2023

[39] Butts, M. "Bot, Troll or Sockpuppet and The Sharing Question". Medium, February 22, 2018

[40] RoBhat Labs. "Identifying Propaganda Bots on Twitter". Medium, October 31, 2017

[41] Rid, T. (2020). *Active measures: The Secret History of Disinformation and Political Warfare*. Profile Books. p. 7

[42] Cormac, R. (2022). *How To Stage a Coup: And Ten Other Lessons from the World of Secret Statecraft*. Atlantic Books. p. 77

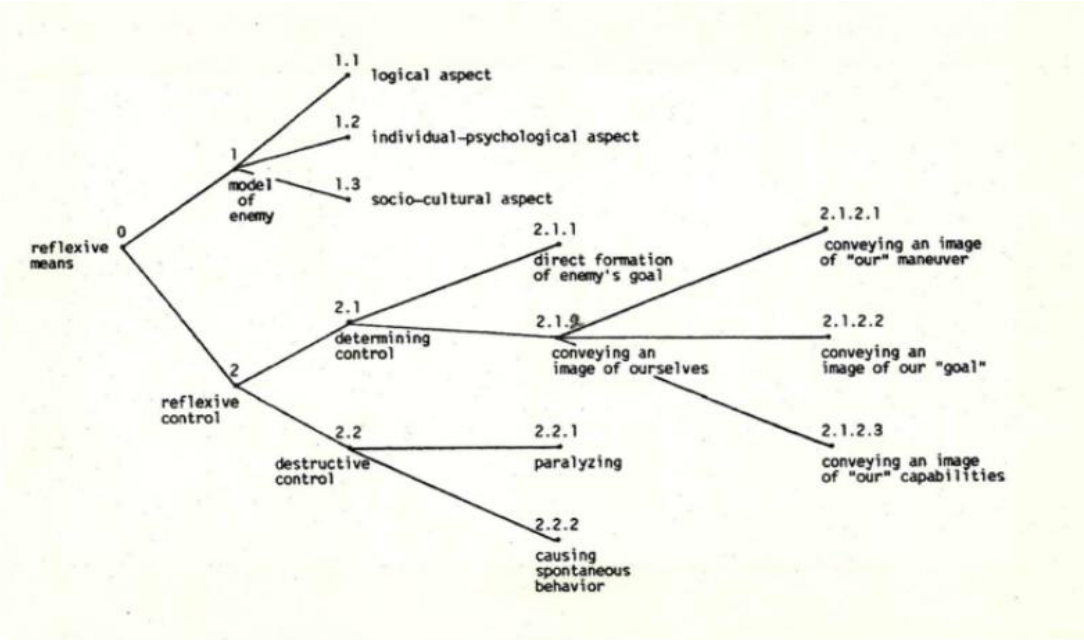
[43] Krieg, A. (2023). *Subversion: The Strategic Weaponization of Narratives*. Georgetown University Press.

[44] Rid, T. (2020). *Active measures: The Secret History of Disinformation and Political Warfare*. Profile Books p. 434

[45] Giles, K. and Seaboyer, A. (2019) "The Russian Information Warfare Construct". Defence Research and Development Canada, pp. 28-42

First established by Dr. Vladimir Lefebvre in the 1960s, and then built on by V. Druzhinin and D. Kontorov, the TORC is a methodical framework for shaping perceptions of target audiences via information inputs to create voluntary decision-making (a 'reflexive action') in the target (or 'agent') that is favourable to the practitioner.[46] It encompasses not only the logical processing of information (including information systems), but also psychological, emotional, and cultural frameworks within which decisions are made.[47]

Figure 2 – Original concept of the Theory of Reflexive Control



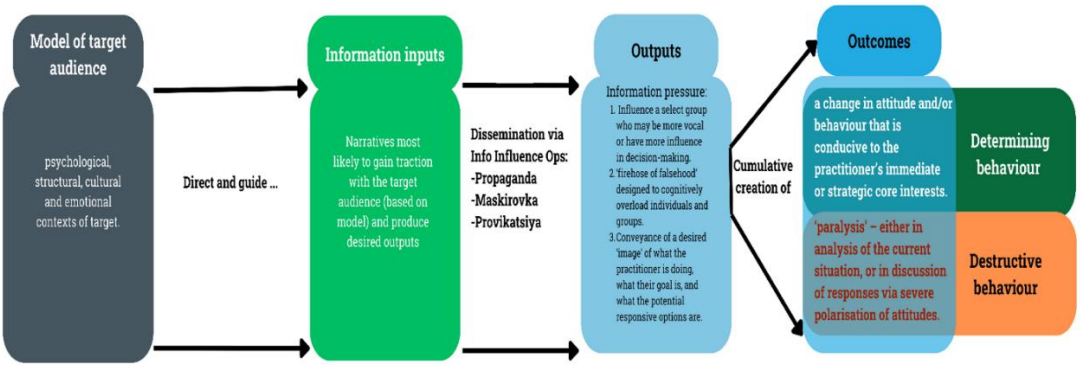
As detailed in the above diagram,[48] the TORC begins with a 'model of the enemy' – this is an overall profile of an individual, group or state that acts as the target audience (similar to Messner's concept of psycho-reconnaissance). It includes detailed psychological, structural, cultural, and emotional contexts in order to understand the best choices of information input to achieve the desired reflexive action. The information input chosen will then be determined by the desire to create a destructive action or determining action. Information inputs will target cultural, psychological and/or emotional issues and contain narratives most likely to gain traction with the target audience and produce desired outputs. These outputs can include information pressure, which can encompass: (1) tailored information or narratives designed for a select group that may be more vocal or have more influence in decision-making; (2) a 'firehose of falsehood'[49] designed to cognitively overload individuals and groups; or (3) conveyance of a desired 'image' of what the practitioner is doing, what their goal is, and what the potential responsive options are.

This process aims to achieve several behavioural outcomes: either those falling under 'determining action', such as a change in attitude and/or behaviour that is conducive to the practitioner's immediate or strategic core interests; or destructive actions, primarily 'paralysis,' either in analysis of the current situation, or in discussion of responses via severe polarisation of attitudes. The primary difference between determining and destructive actions should therefore be viewed as being based on the severity of the impact.

[46] Lefebvre, V.A. (trans. Lefebvre, V.D.) "Reflexive Control: The Soviet Concept of Influencing an Adversary's Decision Making Process" in *Science Applications,* 1984.
[47] Giles, K. and Seaboyer, A. (2019) "The Russian Information Warfare Construct". Defence Research and Development Canada, p. 2
[48] Davis, C. "Paper – Evolution of Russian Information Warfare". SOF News, May 5, 2023
[49] Paul, C. and Matthews, M. (2016) "The Russian "Firehose of Falsehood" Propaganda Model". RAND

The TORC was first analysed by Western practitioners in the 1980s.[50] Consequently, it can be broken down even further based on existing literature and technological changes in the 21st century. For instance, Kasapolgu rightly recognises the presence of *maskirovka* (masquerade, i.e., deception, such as the disguise of Russian special forces during the illegal annexation of Crimea in 2014),[51] but it can be legitimately argued that this is only one of three overlapping (and often concurrent) concepts underneath the umbrella of the TORC. In practitioner efforts to provide calculated informational inputs, it can engage not just in *maskirovka,* but also *provokatsiya*[52] (provocation, such as false-flag attacks and hoaxes), and *informatsiya voyna* (taken in this context as the application of white, grey and black propaganda to manipulate information systems and cognition). In the context of the 21st century, inputs and activities can constitute a range of online and offline activities, but heavily utilise social media.[53] A further benefit of the TORC is its flexibility of scale. As Kasapolgu highlights, the 'insidious merit' of the TORC is how it can be applied at an operational, tactical and/or strategic level.[54] But in a non-military context, this can be used to observe its usage at an individual/community, regional, and policymaking/national level. Therefore, this report adapts the existing framework to accommodate the larger scale and methods in which the TORC now operates (Figure 3).

Figure 3 – Theory of Reflexive Control research framework



APPLICABILITY TO RESEARCH METHODOLOGY

The TORC has been the subject of increased scrutiny in the West since the Crimea Crisis. But remarkably, it has rarely been used as a guiding framework to understand and analyse ongoing Russian IIOs. This is largely because it has traditionally been viewed through a military lens. But as Giles and Seaboyer attest, it is not a purely military discipline.[55] Indeed, it can be argued that according to Russia's own texts on information warfare, the TORC cannot be viewed as separate from non-military operations precisely because information warfare is considered both a peacetime and wartime activity. Therefore, it is entirely legitimate to adapt the TORC as a framework for analysing Kremlin IIOs. At the same time, this is not a foolproof framework. The entire point of IIOs and the TORC in the 21st century is to create changes that will not always be readily apparent. Nevertheless, by adopting the framework in our study, we were better able to understand the likely target of information inputs (in terms of historical, cultural, and psychological fault lines), the target audiences, and intended outputs and outcomes. This can also act as a further guide for measurements of a 'successful' IIO.

[50] Chotikul, D (1986) "The Soviet Theory of Reflexive Control in Historical and Psychocultural Perspective: A Preliminary Study". Naval Postgraduate School, Monterey
[51] Moore, C. "Russia And Disinformation: Maskirovka". Centre for Research and Evidence on Security Threats, March 18, 2019
[52] GlobalSecurity.org "FSB Operations" GlobalSecurity.org, n.d.
[53] Giles, K. and Seaboyer, A. (2019) "The Russian Information Warfare Construct". Defence Research and Development Canada, pp. 28-42
[54] Kasapolgu, C. "Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control". NATO Defence College, November 25, 2015, p.5
[55] Giles, K. and Seaboyer, A. (2019) "The Russian Information Warfare Construct". Defence Research and Development Canada, p. 10

There is significant debate as to how one measures the success of IIOs, or even if you can measure impact at all. According to Jamieson's study of the 2016 US presidential campaign, they were critical in getting Trump elected by shifting perceptions of Clinton and Trump.[56] Whereas Rid sees the overall impact as 'impossibly hard to measure by design'.[57]

In his seminal work on subversion, Dr Andreas Krieg focuses on 'mobilisation'–to what extent the attitudes, decisions and behaviours produce real action.[58] He suggests five levels of impact according to this metric ranging from 1 (low impact) to 5 (high impact):

1. Social media discourse among genuine users.
2. Offline civil-societal discourse involving conventional media.
3. Policy-relevant discourse between experts and policymakers.
4. Nonvirtual civil-societal mobilisation (e.g. protests and riots).
5. A strategic shift in policy making.

However, this cannot be applied to all systems at the same level. In democracies freedom of expression and assembly (and, therefore, protest) are guaranteed. But in more authoritarian systems, such as several of the selected countries in this study, the public space is tightly controlled, making public protests much less likely. Therefore, we settled on "reach" and "penetration" as metrics of success.

> **Reach** quantifies the total number of users exposed to a campaign, regardless of whether they are part of the target audience or not.
>
> **Penetration** specifically looks at the percentage of the target audience that has been reached, and how many have shared or engaged with that content, indicating the level of adoption or engagement within that group.

Both metrics are important to understanding the aimed impacts of IIOs in the 21st century. While reach indicates the potential reach and visibility of a campaign, penetration provides insights into the campaign's effectiveness in engaging and influencing the intended audience. In the context of our work this is especially important as the penetration is about mainstream media and influencers and how they respond and amplify material that may be misinformation or disinformation. This further fits within Russian concepts of IIOs[59] and the TORC. Although it is almost certain that any immediate destabilising actions would be welcomed by the Kremlin, multiple studies note that the Russian approach is marked by strategic patience with the aim of creating a fragmented information environment, which leads to the desired destructive reflexive actions of cynicism and apathy or withdrawal into bias-confirming sources. This leads to further polarisation and the desired strategic outcome of 'paralysis' or actions that are designed to align with the constructed 'images' the Kremlin projects. For instance, a favourable image of Russia leads to potential demonstrations supporting alignment with Russia or at least acquiescence to it. This is summarised by former KGB Chief Yuri Andropov's belief that exposure to disinformation was similar to cocaine: 'a little bit every so often won't hurt, but if you start to use it every day, you become a different man all together.'[60]

[56] Jamieson, K.H. (2018) *Cyberwar: How Russian Hackers and Trolls Helped Elect a President*. Oxford University Press
[57] Rid, T. (2020) *Active Measures: The Secret History of Disinformation and Political Warfare.* Farrar, Straus and Giroux
[58] Krieg, A. (2023). *Subversion: The Strategic Weaponization of Narratives*. Georgetown University Press, p. 137
[59] Ibid, p. 198
[60] Canadian Security Intelligence Service. (2018). "Russia, the West and the geopolitics of disinformation" in *Who Said What? The Security Challenges of Modern Disinformation*. CSIS