Building Resilience and Psychological Defence

An analytical framework for countering hybrid threats and foreign influence and interference

BJÖRN PALMERTZ, MIKAEL WEISSMANN, NIKLAS NILSSON & JOHAN ENGVALL
LUND UNIVERSITY PSYCHOLOGICAL DEFENCE RESEARCH INSTITUTE, WORKING PAPER 2024:1

Building Resilience and Psychological Defence

An analytical framework for countering hybrid threats and foreign influence and interference

Björn Palmertz, Lund University Psychological Defence Research Institute

Dr. Mikael Weissmann, Swedish Defence University

Dr. Niklas Nilsson, Swedish Defence University

Dr. Johan Engvall, Stockholm Centre for Eastern European Studies

About the Lund University Psychological Defence Research Institute

PDRI is an independent research institute based at the Department of Strategic Communication, Lund University. Its core funding is provided by the Swedish Psychological Defence Agency. In addition, PDRI receives funding from different sources to produce specific publications or develop research tracks.

About Psychological Defence Research Institute Working Papers

In this publication series, researchers connected to PDRI present short analyses or briefings on issues relevant to the public understanding of psychological defence. This includes work on the concept of psychological defence, its associated capabilities, the tactics, techniques and procedures used by threat actors, and the use of new technologies or new platforms to exert information influence.

Table of Contents

1 Introduction[1]

The need to develop resilience and psychological defence in the face of different forms of hybrid threats and malign foreign influence and interference is greater than ever. Russia's full-scale invasion of Ukraine on 24 February 2022 represents a watershed moment for European security. The overall security situation has become more volatile with uncertain future prospects both in Europe and globally. New threats, such as offensive cyber operations, influence campaigns and other types of related operations from state actors as well as non-state actors, further add to the complex security landscape. In response to the deteriorating security situation, NATO alliance members adopted a new strategic concept which states that "the Euro-Atlantic area is not at peace".

In this light, it has become increasingly obvious that a country's resilience and psychological defence capabilities must cover a broad spectrum of conflicts, including severe crises and war. This paper takes these complex and multifaceted types of threats as a point of departure in its attempt to outline an analytical framework for countering hybrid threats and foreign influence and interference. The ambition is then to operationalise this framework into a practical guide that can be used for identifying and analysing hybrid threats and foreign influence against democracies and their national interests.

To be able to build resilience and psychological defence, a shared analytical framework is needed, which provides a broader and more inclusive nation-state perspective than existing frameworks (see section 1.1 below). The framework outlined below is intended to be a starting point for analysis, usable for government and non-government actors alike. It aims to serve as a platform for addressing different dimensions of hybrid threats and malign foreign influence and interference. It also provides tools for comparing and analysing the dimensions within and across cases. The formation of responses to foreign interference should be seen as a process consisting of three distinct phases: 1) assessing situational awareness; 2) addressing defence and countermeasures; and 3) evaluating the state's system for countering foreign interference.

This framework serves as the basis for the development of a practical analytical guidebook that is built to be modular, where one can pick and choose depending on own needs and questions asked. It is also developed to be suitable for both more structured

analysis as well as less structured qualitative analysis. The guidebook is simplified into an analytical template that can be used as a readily available checklist for users.
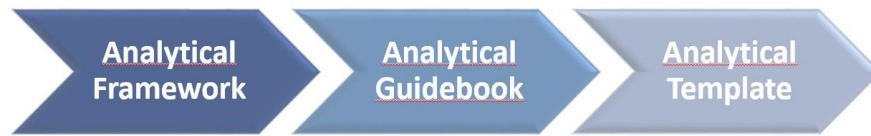

Figure 1: Overview of framework structure

It should be emphasised that both the framework and the guidebook represent a starting point, not a final answer to hybrid threats and malign foreign influence. The guidebook is intended to be developed and customised for the user's own needs and future developments in the complex and fast-developing reality we are all living in.

1.1 Examples of existing frameworks[2]

Since WWII a number of analysis frameworks or categorizations related to propaganda, influence operations and foreign interference have been developed. In 1939 the Institute of Propaganda Analysis at Columbia University classified propaganda according to seven identified techniques. Around the same time, they also published the "ABCs of Propaganda Analysis" offering advice on how to build a contextual understanding of propaganda, your own vulnerabilities as well as the actors involved in using it.[3] Another is SCAME analysis - a framework used by the US military and other countries psychological operations units which offers a simplified approach to structure identified influence activities.[4]

From a networked NGO perspective comes the open-source methodology used by Bellingcat when focusing on investigations regarding the war in Ukraine. It offers a set of standard operating procedures, providing practical steps for investigators to follow when searching for content online.[5] Another open-source framework is DISARM, launched in 2019; aimed at countering disinformation through sharing data & analysis and enabling more effective coordination of actions. It has many object types, including

---

[2] Worth bearing in mind is that intelligence agencies and other actors dealing in the collection and analysis of classified information very rarely publish their analysis methodology. This review is also limited to frameworks available in English.

[3] Institute for Propaganda Analysis (1939) The Fine Art of Propaganda. New York: Harcourt, Brace and Company.

[4] Headquarters, Department of the Army (2005) Tactical Psychological Operations - Tactics, Techniques, and Procedures. FM 3-05.302. Appendix D-2.

[5] Bellingcat & Global Legal Action Network (2022) Methodology for Online Open Source Investigations into Incidents Taking Place in Ukraine Since 24 February 2022.

tactic stages and techniques related to both manipulators and responses employed by defenders.[6]

When looking towards academia Jowett and O'Donnell's 2018 book Propaganda and Persuasion includes a 10-step plan of propaganda analysis. It provides a broad approach taking the propagandist, dissemination, target audience, counter activities and societal context into account. It is most suited to study propaganda occurrences from a long term rather than operational here-and-now perspective.[7]

Specifically developed for EU institutions and governments is the ABCDE framework published in 2020 which offers a shared and structured approach to break down the disinformation problem into smaller operative factors through looking at the actor, behaviour, content, degree, and effect.[8] It has also been adapted into the RESIST 2 Counter Disinformation Toolkit, developed for the UK government, and connecting it to other tools used by UK government communications such as the FACT and OASIS model.[9]

Additionally, Pamment & Smith has published a framework which serves as a point of departure for future work on the attribution of influence operations. It utilizes a matrix built on four types of evidence (technical, behavioural, contextual, and legal/ethical) and three sources of evidence (open source, proprietary source, and classified source).[10] Pamment has also developed a Capability Definition and Assessment Framework to systematically define countermeasures against disinformation, information influence, and foreign interference employed by societal actors. And explore how they could be assessed within a single coherent framework.[11]

These frameworks differ in aim from being focused on supporting analysis through categorizing components and techniques of malign influence activities, to offering a structured approach and shared terminology on how states or societal actors can build, use and evaluate counter influence capabilities. None, however are designed to enable an overarching view of threats and capabilities for the nation state in relation to hybrid threats and foreign interference, including its societal context and broad range of actors. That is what this framework attempts to do, offering a structure to nation state cross-threat

---

[6] https://www.disarm.foundation/framework

[7] Jowett, G. and O'Donnell V. (2018) Propaganda & Persuasion, 7th ed. Ch. 6 How to analyze propaganda. SAGE Publications.

[8] Pamment, J. (2020) The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework. Carnegie Endowment for International Peace.

[9] Pemment, J. (2021) RESIST 2 Counter Disinformation. UK Government Communication Service.

[10] Pamment, J. & Smith, V. (2022) Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online. NATO StratCom COE & Hybrid COE.

[11] Pamment, J. (2022) A Capability assessment framework for countering disinformation, information influence, and foreign interference. NATO StratCom COE.

and joint capability analysis useful when, for example, developing case studies at such a level of resolution.

1.2 Defining foreign interference

This paper focuses on how to understand and address different types of threats targeting democratic states. These threats are best understood as different forms of foreign interference, a term which will be used to capture the different forms of hybrid threats and malign foreign influence and interference that democracies are confronted with. The notion of "foreign interference" serves as a comprehensive umbrella term, encompassing the diverse array of tactics employed by foreign states and non-state actors to manipulate, disrupt, or influence the affairs of democracies.

Foreign influence and interference is here understood as being synonymous with what the EU External Action Service labels Foreign Information Manipulation and Interference (FIMI). FIMI is defined as:

> *a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.*[12]

For hybrid threats, the paper adopts the broad understanding developed by the Hybrid CoE, arguably the primary institution within the Western security framework assigned the responsibility of addressing hybrid threats:

> *The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution.*[13]

---

[12] The European External Action Service (EEAS), "Tackling Disinformation, Foreign Information Manipulation & Interference," 27 October 2021, https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en. (last accessed 22 January 2024)

Also see *1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a framework for networked defence*, February 2023.

[13] The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), "Hybrid threats as a concept", https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (last accessed 22 January 2024).

On the basis of this, hybrid threats include the following:

> *Coordinated and synchronized action that deliberately targets democratic states' and institutions' systemic vulnerabilities through a wide range of means.*
>
> *Activities that exploit the thresholds of detection and attribution, as well as the different interfaces (war-peace, internal-external security, local-state, and national-international).*
>
> *Activities aimed at influencing different forms of decision-making at the local (regional), state, or institutional level, and designed to further and/or fulfil the agent's strategic goals while undermining and/or hurting the target.*[14]

---

[14] Ibid.

2 Analytical framework for countering hybrid threats and malign foreign influence and interference

The potential threats posed by foreign interference are conceptually broad and comprise a state's international security environment, the interconnections between this international environment and the national domestic context, the existing vulnerabilities in this context, and the state's means for addressing antagonistic behaviour from external actors. We suggest that the formation of responses to foreign interference should proceed in three conceptually distinct phases, representing a cycle of

1) establishing situational awareness,

2) applying and adapting existing defences and countermeasures and developing new ones if needed, and

3) holistic evaluation of the state's system for countering foreign interference.

The process can be summarized as **Assess, Address and Evaluate**.

Assess refers to the double-sided mapping of external threats - denoting antagonistic actors that seek (or may seek) to exercise malign influence by various means, and the internal vulnerabilities that these actors seek to (or may seek to) target. It also includes the available defensive mechanisms.

Address denotes the state's existing capabilities for addressing the threats and vulnerabilities identified. This includes existing frameworks for national coordination of these efforts as well as international cooperation and existing legal and regulatory frameworks.

Evaluate, finally, refers to an integrated analysis, with a view to establishing a holistic understanding of the impact of threats and effectiveness of capabilities identified above. In turn, the assessment stage should serve as a basis for making informed decisions about the need for reinforcement, revision or change in the state's capacity and its methods of response.

Figure 2: Analytical framework for countering hybrid threats and foreign influence and interference

2.1 The six dimensions of foreign interference

When assessing foreign interference six key dimensions needs to be taken into account: **1. Threat Assessment, 2. Vulnerability Assessment, 3. Defense Mechanisms, 4. Coordination and Cooperation, 5. Legal and Policy Framework, 6. Impact and Effectiveness**. The first three belong to the Assess part of the analytical process, i.e., the assessment of the threat and one's own vulnerabilities, as well as what Defense Mechanisms that are in place/exists. Dimensions four and five, Coordination and Cooperation and Legal and Policy Framework, concern the frame in which the first three exists. This is the Address phase of the process. Lastly, dimension six covers the Evaluate phase, focusing on the combined impact and effectiveness of the first five.

2.1.1 Assess

Threat Assessment concerns the identification and analysis of who the threat actors are – direct or through proxy - and their tactics, techniques, and tools used when attempting to interfere with the country's affairs. Here, the time dimension needs to be considered, as the threat levels and patterns of interference may evolve over time. When assessing the threat, there is an inherent need to be forward-looking, asking whether there are any emerging or future threats that the country should anticipate and prepare for.

The second dimension, **Vulnerability Assessment** concerns the identification and analysis of a country's vulnerability to foreign interference, i.e., the underlying political, social, and economic factors that contribute to the country vulnerabilities. In this context, it is important to take each country's governance structure and democratic processes into account to analyse and understand their impact on vulnerability to foreign interference. Moreover, it is important to also include the role and impact of different kinds of societal

10

divisions or issues, as well as societal groups and organizations that deliberately or unwittingly are targeted and exploited by foreign actors to amplify discord and manipulate public opinions. Finally, the cyber dimension needs to be addressed as it is a critical component in a country's resilience and ability to counter hybrid threats. Thus, it needs to be assessed if, and, if so, how, a country's technological infrastructure and connectivity influence its vulnerability to cyber-based interference.

Having identified and analysed the threats and vulnerabilities, it is time to move on to the **Defence Mechanisms**. Here, the first step is to identify the existing strategies, policies, and institutions in place to defend a country against foreign interference. The subsequent step is to analyse the effectiveness of these mechanisms in detecting, preventing, and mitigating interference attempts. When conducting the analysis of defence mechanisms, it is also important to analyse if there are any gaps or weaknesses in the country's defence mechanisms, and, if so, what they are. In this context, it is worthwhile to also analyse how resilience is promoted in the population, including dimensions such as media literacy and critical thinking.

2.1.2 Address

Coordination and Cooperation is an important dimension for successful countering of complex problems such as hybrid threats and foreign influence and interference. Identifying and analysing structures and practices are complex tasks, not least since they tend to be unique depending on each country's context. However, areas that need to be addressed include how relevant government agencies, intelligence services, and law enforcement bodies are coordinated and whether joint national capabilities have been developed across the hybrid threat spectrum to identify, analyse and counter such activities. For example, is information sharing coordinated and are there cooperation and coordination between the response capability of the government leadership, intelligence, cyber defence and counter influence agencies, and other key societal actors? On the societal level, the role of civil society organizations, media outlets, and other non-state actors in supporting defence against foreign interference needs to be taken into account.

It is here also important to acknowledge that coordination and cooperation is not only a national affair, but includes international ties to countries and organizations. Thus, it needs to be explored whether there are collaborations and mechanisms in place for sharing intelligence, information and best-practices with international partners and allies, and if so to what extent they are effective.

Legal and Policy Framework is a crucial part, creating the frame for resilience and countering of hybrid threats and foreign interference. It is important to map and understand the kind of legal frameworks and regulations that exist to counter foreign interference and protect national security. What are they and how well do existing laws and policies address the evolving nature of foreign interference? This includes the technological dimensions, addressing whether they are able to account for the emerging technologies used by adversaries. Having addressed what exists, it is also important to

analyse the effectiveness of the implementation and enforcement of these legal and policy measures, and whether there are any legislative or policy gaps that need to be addressed.

2.1.3 Evaluate

Finally, **Impact and Effectiveness** need to be evaluated, being the goal of the other five dimensions. Here it needs to first be analysed what the impacts of foreign interference on the country's political stability, public opinion, and democratic processes are. Thereafter, focus shifts to response and lessons learned; how has the country responded to specific instances of foreign interference, and what lessons have been learned? Have existing defence mechanisms shown demonstrable effectiveness in countering foreign interference? Finally, it needs to be asked how the citizens perceive the effectiveness of defence measures and their confidence in the government's ability to protect against foreign interference.

3 Analytical guidebook

In this section the analytical framework outlined above is operationalised in an analytical guidebook. The guidebook follows the structure of the above outlined six-dimensional framework for assessing foreign interference: 1. Threat Assessment, 2. Vulnerability Assessment, 3. Defence Mechanisms, 4. Coordination and Cooperation, 5. Legal and Policy Framework, and 6. Impact and Effectiveness. The proposed framework outlines four questions to be asked for each dimension. In this way, it creates a structured guide for assessing foreign influence and interference and the defence against it in different countries across the spectrum between war and peace.

While all questions should be applied to the respective country, there is no need to force answers if a sufficient foundation cannot be found. Instead, having asked the question is sufficient to ensure that various dimensions have been taken into consideration. It should be acknowledged that since the guidebook is framed for democratic states' and institutions' vulnerabilities, there can be discrepancies when applied to less democratic states and institutions.

ANALYSE

1. **Threat Assessment**
   a) Who are the foreign states and actors of foreign interference targeting the country?
   b) What specific tactics, techniques, and tools do these actors use when attempting to interfere with the country's affairs?
   c) How have the threat levels and patterns of foreign interference evolved over time?
   d) Which emerging or future threats should the country anticipate and prepare for?

2. **Vulnerability Assessment**
   a) What are the underlying political, social, and economic factors that contribute to the country's vulnerability to foreign interference?
   b) How do the country's governance structure and democratic processes impact its vulnerability to foreign interference?
   c) Are there particular societal divisions or issues, or societal groups or organizations that deliberately or unwittingly are exploited by foreign actors to amplify discord and manipulate public opinion?
   d) How does the country's technological infrastructure and connectivity influence its vulnerability to foreign interference?

---

3. **Defence Mechanisms**

   a) What are the existing strategies, policies, and institutions in place to defend against foreign interference?

   b) How effectively do these defence mechanisms detect, prevent, and mitigate foreign interference attempts?

   c) Are there any gaps or weaknesses in the country's defence mechanisms that need to be addressed?

   d) How does the country promote media literacy, critical thinking, and resilience among its population to counter foreign interference?

ADDRESS

4. **Coordination and Cooperation**

   a) How are relevant government agencies, intelligence services, and law enforcement bodies coordinated to address foreign interference?

   b) Have joint national capabilities been developed across the hybrid threat spectrum to identify, analyse and counter such activities? (For example, information sharing and response capability between the government leadership, intelligence, cyber defence and counter influence agencies, or other key societal actors.)

   c) What role do civil society organizations, media outlets, and other non-state actors play in supporting defence against foreign interference?

   d) How does the country engage in international cooperation and exchange best practices, information and intelligence sharing with international partners and allies?

5. **Legal and Policy Framework**

   a) What legal frameworks and regulations exist to counter foreign interference and protect national security?

   b) How well do these laws and policies address the evolving nature of foreign interference and emerging technologies used by adversaries?

   c) Are there any legislative or policy gaps that need to be addressed to enhance defence against foreign interference?

   d) How effectively are these legal and policy measures enforced and implemented?

EVALUATE

6. **Impact and Effectiveness**

   a) What are the measurable impacts on the country's political stability, public opinion, and democratic processes taking into account second order and unintended effects of foreign interference?

   b) How has the country responded to specific instances of foreign interference, and what lessons have been learned?

   c) Have the defence mechanisms put in place shown demonstrable effectiveness in countering foreign interference?

   d) How do the country's citizens perceive the effectiveness of defence measures and their confidence in the government's ability?

4 Conclusions

Analysing hybrid threats and foreign interference is per definition integrated with many analytical areas and encompasses a wide variety of threats. This results in a need for frameworks that can facilitate the collation of various types of information. In addition, due to the broad nature of how influence can manifest itself from an opponent against a society, there is need for a structured and pedagogic approach that can be understood by a broad array of decision-makers. Since hybrid threats are oftentimes interconnected and simultaneously targeting several aspects of society, it is beneficial with an analytical framework that simplifies and makes it possible to identify important interrelated aspects in large and complex volumes of information.

Also important is that the framework is flexible and, to a certain degree, modular, since its application and the resolution needed in the different categories may differ slightly depending on what societal actor will make use of it, and what level they operate on. In addition, one can be sure that capable adversaries adapt and develop their means and methodologies continuously.

The analytical framework presented aims to add one avenue among many in terms of building resilience and psychological defence among democratic states confronted by hybrid threats and malign foreign influence and interference. To be practically useful, an analytical framework addressing hybrid threats and foreign interference should:

- Account for the diversity of threats and the many different potential domains threatened by adversaries.

- Have a structured approach, enhancing the pedagogical understanding of the issue among a broad array of decision-makers.

- Simplify reality and enable the practitioner to identify important interrelated aspects in large volumes of information.

- Allow for flexibility and modularity since its application may differ slightly depending on different categories of threats as well as the type of practitioners utilizing it.

Hence, these four points have been guiding the framework outlined in this report.

5 Analytical template

The analytical framework presents a number of questions in each of its six dimensions. These are not intended to be exhaustive but to serve as a structured starting point and direction from which the analyst can refine or formulate additional questions based on the specific threat environment and societal context they are investigating. In addition, the framework does not require the analysis of dimensions to be done in a certain order, as long as they all are addressed and conclusions documented.

Each analytical question will be considered through a three-step approach:

1) The first, **Analysis**, is focused on answering the initial question or addressing the problem statement. It involves gathering relevant data, information, and evidence to provide a thorough understanding of the situation. It is strongly recommended that you document the sources used in the analysis.

The analysis-step lays the foundation for the following steps.

2) The second, **Impact Assessment**, aims to weigh the current significance or impact of the aspect being investigated. This involves evaluating the implications of the findings on various stakeholders, processes, or objectives. It thereby adds context by considering the real-world consequences and relevance of the identified factors.

3) The third, **Proposed Action**, involves recommending specific steps or strategies to address the identified threats, vulnerabilities or opportunities. The proposed action should be based on a logical connection between the analysis and the desired outcomes, taking into account the potential impacts on the organization or project. This way the overarching analysis will be more useful for decision makers, and future implementation if such is deemed necessary.

The aim of the three-step approach is to ensure a holistic and logical progression from understanding the problem to assessing its significance and finally proposing actionable solutions. Therefore, the assessment within each dimension ends in a conclusion where key findings and their implications are summarized, adding and/or highlighting aspects that span several of the questions posed. In a similar manner, key proposed actions and how several of these may interrelate, as well as indicate overarching perspectives, should be added in the conclusion.

At the very end of the process, the six conclusions from the assessments of each dimension are developed into a combined conclusion, building on the entire work conducted within the analytical framework.

1. Threat Assessment	STEP 1 Analysis	STEP 2 Impact Assessment	STEP 3 Proposed Action
a) Who are the foreign states and actors of foreign interference targeting the country?			
b) What specific tactics, techniques, and tools do these actors use when attempting to interfere with the country's affairs?			
c) How have the threat levels and patterns of foreign interference evolved over time?			
d) Which emerging or future threats should the country anticipate and prepare for?			
CONCLUSIONS (Threat Assessment)			

2. Vulnerability Assessment	STEP 1 Analysis	STEP 2 Impact Assessment	STEP 3 Proposed Action
a) What are the underlying political, social, and economic factors that contribute to the country's vulnerability to foreign interference?			
b) How do the country's governance structure and democratic processes impact its vulnerability to foreign interference?			
c) Are there particular societal divisions or issues, or societal groups or organizations that deliberately or unwittingly are exploited by foreign actors to amplify discord and manipulate public opinion?			
d) How does the country's technological infrastructure and connectivity influence its vulnerability to foreign interference?			
CONCLUSIONS (Vulnerability Assessment)			

3. Defence Mechanisms	STEP 1 Analysis	STEP 2 Impact Assessment	STEP 3 Proposed Action
a) What are the existing strategies, policies, and institutions in place to defend against foreign interference?			
b) How effectively do these defence mechanisms detect, prevent, and mitigate foreign interference attempts?			
c) Are there any gaps or weaknesses in the country's defence mechanisms that need to be addressed?			
d) How does the country promote media literacy, critical thinking, and resilience among its population to counter foreign interference?			
CONCLUSIONS (Defence Mechanisms)			

4. Coordination and Cooperation	STEP 1 Analysis	STEP 2 Impact Assessment	STEP 3 Proposed Action
a) How are relevant government agencies, intelligence services, and law enforcement bodies coordinated to address foreign interference?			
b) Have joint national capabilities been developed across the hybrid threat spectrum to identify, analyse and counter such activities?[15]			
c) What role do civil society organizations, media outlets, and other non-state actors play in supporting defence against foreign interference?			
d) How does the country engage in international cooperation and exchange best practices, information and intelligence sharing with international partners and allies?			
CONCLUSIONS (Coordination and Cooperation)			

---

[15] For example, information sharing and response capability between the government leadership, intelligence, cyber defence and counter influence agencies, or other key societal actors.

5. Legal and Policy Framework	STEP 1 Analysis	STEP 2 Impact Assessment	STEP 3 Proposed Action
a) What legal frameworks and regulations exist to counter foreign interference and protect national security?			
b) How well do these laws and policies address the evolving nature of foreign interference and emerging technologies used by adversaries?			
c) Are there any legislative or policy gaps that need to be addressed to enhance defence against foreign interference?			
d) How effectively are these legal and policy measures enforced and implemented?			
CONCLUSIONS (Legal and Policy Framework)			
	STEP 1 Analysis	STEP 2 Impact Assessment	STEP 3 Proposed Action

6. Impact and Effectiveness	STEP 1 Analysis	STEP 2 Impact Assessment	STEP 3 Proposed Action
a) What are the measurable impacts on the country's political stability, public opinion, and democratic processes taking into account second order and unintended effects?			
b) How has the country responded to specific instances of foreign interference, and what lessons have been learned?			
c) Have the defence mechanisms put in place shown demonstrable effectiveness in countering foreign interference?			
d) How do the country's citizens perceive the effectiveness of defence measures and their confidence in the government's ability?			
CONCLUSIONS (Impact and Effectiveness)			