ISBN 978-9934-619-60-1

Enhancing Organisational Capability: A Tailored Approach with Red Team vs Blue Team Adapted Workshops

A workshop methodology for developing increased capability against information influence operations

PREPARED AND PUBLISHED BY THE
NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

ISBN: 978-9934-619-60-1

Author: Sara Sörensen
Contributors: Sara Carlstein, Andreas Edevald
Content editing: Merle Anne Read
Design: Una Grants

Riga, March 2024

NATO STRATCOM COE
11b Kalnciema iela,
Riga, LV1048, Latvia
stratcomcoe.org
@stratcomcoe

Enhancing Organisational Capability: A Tailored Approach with Red Team vs Blue Team Adapted Workshops

A workshop methodology for developing increased capability against information influence operations

Executive summary

The purpose of the report is to present a method for exploring an actor's possibilities for countermeasures and capabilities against information influence operations (IIO). Using specific scenario conditions, the method assists in creating a discussion on what capabilities are needed and how organisations can develop these capabilities based on available resources. The method involves conducting workshops using a red team versus blue team exercise which has been adapted to generate a gap analysis for countermeasures in countering IIO. The report provides guidance on preparing for a workshop aimed at identifying vulnerabilities in an organisation's information environment and developing effective strategies to mitigate the consequences of IIO.

The workshops create a common problem understanding from a scenario and challenges chosen beforehand. The end result is an analysis that includes existing capabilities in the organisation, a reflection on how to develop capability activities and functions further, and prioritising between these. The report concludes that the workshop method is a useful tool for risk assessment and preparedness planning, and can be used for decision-making and operational development.

While countering IIO is often a national-level responsibility, we argue that all parts of society can be affected by IIO and should develop capabilities to counter disinformation. Therefore, the selected workshop method can be adapted to work on a local, regional, or national level.

Contents

Introduction

All parts of society are affected when a foreign threat actor uses information influence operations (IIO) to damage trust, divide and polarise groups, and fuel suspicion to create a more vulnerable society. Therefore, for all parts of society it is essential to develop an operational capability to identify and counter disinformation.

Capability in countering IIO should be based on the threat towards an actor's vulnerabilities and possible consequences for the actor's responsibilities in society. Since actors in different parts of society have different responsibilities and functions, capability in countermeasures will wary. Nevertheless, professionals need to understand that all parts of society can participate to some extent in limiting mis- and disinformation, and true resilience is built with a whole of society approach. Only then can societal resilience be achieved on a larger scale.

This report presents a method to explore an actor's possibilities for countermeasures and capabilities in specific scenario conditions, and how they can develop these capabilities based on available resources. Depending on an actor's responsibilities, scenarios can be adapted to their specific context and set up with different personnel and timelines. The workshop and finished analysis can assist in organisational decision-making, capability and resource prioritisation and problem-solving.

The report first looks at how the method is structured and how the scenario and challenges were built. It then explains the factors involved in planning a workshop for exploring current capabilities and identifying gaps that feeds into organisational decisions in capability development, such as the timing, participants, scenario, challenges, and role of the moderator. This is followed by a review of the implementation of the different phases of the workshop, including the workshop goals, the focus for team discussions, and the general structure. The report then suggests a structure for analysing the results and presents examples from the workshops that were conducted, to demonstrate the potential results from a workshop. The report concludes with general recommendations arising out of the workshops tested with Swedish actors.

Method development

The method presented and content of this report were produced in cooperation with the Swedish Psychological Defence Agency (MPF) and the Nordic Baltic Eight Group (NB8).

Scenario building

Capability building scenarios can be used in risk assessments which prioritise anticipated vulnerabilities and threats and can assist in planning preparedness. Different types of scenarios can answer different questions and can be used to reflect on different aspects regarding threats and risks. The scenario and challenges used in the workshops conducted for this report were created with the help of the NB8, which is coordinated by the NATO Strategic Communications Centre of Excellence. At a meeting in Reykjavik in November 2022 the NB8 group, consisting of representatives from the Nordic and Baltic countries, workshopped scenario descriptions and possible challenges. The aim was to create a contextual exploratory scenario whose analysis can assist in establishing the fundamentals for achieving certain goals in an exercise or workshop.

The use of scenarios in exercises and workshops requires them to be seen as credible by the participants. The exploratory approach also allows various specific challenges to be included. These challenges should be linked to relevant topics for the actors and can be combined to create a relevant scenario.[1]

Three workshops

To test the workshop method, three workshops at the local, regional, and national level were planned and conducted together with the MPF. Sweden was therefore the example nation, but the method can of course be applied to other nations. Testing the method at different societal levels contributed to analysing whether the selected method was suited to different actors and could be used to find reasonable levels of capability in countering IIO regarding their responsibilities. The workshops, called PSYCAP 2023, were held in Sweden and run with a Municipal and a County Administration Board, and a Swedish National agency.

The workshop method— red team vs blue team adapted method

The workshop had several inspirational methodologic standpoints. The basic concept of the workshop was a red team vs blue team exercise, but with additional discussion elements to create a gap analysis.

Red team vs blue team is a common group exercise, especially in cybersecurity. The goal of the red team is to attack an organisation's defences. The blue team defends against and responds to the red team's attacks.

The exercise is modelled on military training and in this report has been adapted to also function as a workshop to assess what countermeasures may need to be developed in countering IIO. The method enables participants to create a common problem understanding from a scenario that can be chosen beforehand.

For this workshop it was also relevant to include an element of development discussions to create a gap analysis. Gap analyses are used to identify the current state of an activity or organisation and what the ideal situation might be, and to clarify what is needed to fill the gap between the two. The method presented is a simplified version that can be done with experts and stakeholders over a single day. In short, the workshop method creates an analysis based on reflections from a variety of perspectives.

The end result of the workshop is an analysis that takes into account the organisation's existing capabilities, solution-oriented reflection on how to develop capability activities and functions further, and prioritising between countermeasures and capabilities. The workshop differs from regular exercises where the participants' main focus is on practice. Here the objective is primarily for participants to use their input to generate an analysis for continued development.

Part I—Planning a workshop for capability development

Preparations and planning

Before conducting this workshop there are some aspects to carefully consider.

Deciding on the objective: The purpose of this kind of workshop is to identify vulnerabilities in the organisation and develop effective strategies and countermeasures to mitigate the risk of IIO. This helps organisations to prepare for potential attacks and improve their overall resilience to information warfare.

Scenario and challenges: Decide on a scenario to use and specific challenges for the participants to discuss. The main scenario sets the context for what the world looks like during the workshop discussions, such as greater unrest in the region or increased cyberattacks (*see Annex 1*).

The challenges that the participants are to discuss in teams are short descriptions of specific events, such as a disinformation campaign aimed at their organisation, an event that might affect their work with regard to strategic communication, or one that calls for direct action to avoid negative effects on their work performance. The most important point is that the challenges are relevant, credible, and not impossible to solve. The main description should include a threat that is relatable for the organisation to take action against or that needs countermeasures (*for inspiration see Annex 2*).

Time: The workshop will take approximately eight hours to conduct, either in one session or over two half-days. Plan accordingly with location, and create a schedule and list of participants. The workshop can be made shorter or longer depending on how many challenges are presented to the participants to work with.

Remember that after the workshop has been completed the analysis has to be carried out. The data has to be documented and structured accordingly to be analysed. The analysis also has to be presented to both the participants and the leadership responsible for decision-making and prioritising the suggestions made during the workshop.

Participants: Participants and their expertise and knowledge base are important. Depending on who is participating, the focus of the workshop can create either a wide or narrow range of areas for capability development. For example, if only communicators are attending the workshop, then the focus for countermeasures will most likely concentrate on communication. Before inviting the participants be clear in your mind about whether the workshop's end results should have a wide or narrow focus.

It is also appropriate to reflect on participants' previous knowledge level. It may be worth providing particular information or making it a requirement that participants have experience of the subject from earlier engagements. Otherwise, include a lecture prior to the workshop.

For maximum efficiency in the discussions there should be no more than sixteen participants, eight in each group. The total number of participants in a single group can be smaller. The participants should be personnel from the organisation that have an in-depth understanding of their roles in the organisation and of the organisation itself. For the workshops conducted for this report the participants were communicators, crisis management and civil defence analysists, and IT and security staff.

The participants in the workshop were members of either the blue or the red team.

- The blue team represents the defenders trying to prevent or counter the IIO. The blue team will need a problem-solving mindset and they will defend against the red team. The blue team's objective is to try to find options for mitigating and countering the actions of the red team and to develop effective countermeasures. Various tools such as media analysis, social media monitoring, partnerships, and sentiment analysis could be used to detect and counter these activities.

- The red team represents an adversary attempting an attack on the blue team and creates challenges for the blue team during the workshop. The red team in our workshops was not told which specific actor it represented (Russia, China, or Islamic extremists), only that it was a malicious actor with reasonable resources, so that they don't over exaggerate what they can do. The red team might use various techniques such as social engineering, fake news, disinformation campaigns, and other propaganda tactics to influence public opinion.

Depending on the participation, the moderator can decide if the participants should be in the red team for the entire workshop or if the groups should switch roles during the different challenges, depending on the circumstances. It is then important to remind them about their different mindsets: problem-solving or attacking.

Questions during the challenges: Specific questions to be asked during the workshop can be planned ahead of time for each challenge, such as; when would participants believe that they would recognise the threat, who would be their partners in coordinating the situation, and so on. The questions would depend on what challenges were being discussed or what the moderator would wish the blue team to focus on with regard to countermeasures. The questions could also be adapted to the participants' expertise and according to whether the focus was on specific capabilities or was from a wide perspective.

Moderators: The moderator plays a crucial role in ensuring that the workshop is productive and effective, and meets its objectives. Moderators facilitate the discussion, encourage participation, manage time, and

ensure that the activities are focused on and relevant to the objectives of the workshop. For approximately sixteen participants there should be at least two moderators, but preferably three.

The main moderator is responsible for:

- setting the agenda for the workshop, based on the goals and objectives of the session. The moderator communicates the agenda to the participants before the workshop starts.

- the introduction of the workshop topic. The moderator provides any necessary background scenario and chosen challenges.

- time management. The moderator is responsible for keeping track of time and ensuring that the workshop stays on schedule. They may use tools such as timers or agendas to do so and ensure that all topics are covered.

- summarising discussions. At the end of the workshop, the moderator summarises the key points of the discussion and recaps any decisions made or actions agreed upon.

- collecting feedback. The moderator may collect feedback from the participants to evaluate the effectiveness of the workshop and identify areas for improvement.

It is useful to have one assisting moderator for each team, red and blue. Their responsibilities include:

- encouraging participation. The assisting moderator may encourage input from all participants, especially those who are quieter or less involved.

- facilitating discussions. The assisting moderator may facilitate group activities during the workshop, ensuring that everyone participates, that the activities stay focused on the objectives of the workshop, and that it stays productive. The moderator should prepare a paper with questions to help and guide the groups during their conversations. The questions could be a part of the planning of the scenarios and challenges. Suitable questions could be about what existing capabilities they have in anticipating, recognising, adapting, and learning, when they believe they would react to the challenges, and if they have partners they would contact.

- conflict management. If conflicts arise between the participants during the workshop, the moderator may intervene to manage the conflict and bring the discussion back to a productive focus.

Documentation: Workshop documentation is a shared responsibility of the moderators. The main moderator focuses on observing and documenting when the challenges discussion starts. The assisting moderators document on the whiteboard what is being suggested as solutions, continued threats and questions from both the red and the blue team, and any questions raised during the workshop.

All this should then be placed in a structured order to make analysis easier. We suggest that the main moderator documents the discussions and whiteboard reflections either digitally or on paper while the workshop proceeds.

Workshop assessment: Besides the analysis there could be an additional assessment being made, focusing on assessing what the participants thought about the concept of the workshop. Did the challenges focus on the right things? Was the scenario believable? Is this a good way for the organisation to perform this kind of analysis? Creating an assessment document for the participants to fill in after the workshop helps to gather their reflections that can be taken into consideration for future work.

Part II—Implementation of the workshop

Workshop method and structure

The workshop starts with a clear introduction of the goals for the day, the agenda and the general structure for the discussions, and the mindset for the participants (Figure 2). Introduce the participants and assign them to the red or blue team for the duration of the workshop. Most often, participants will focus more on the parts that are relevant for their role later in the exercise.

Even if participants have been given a lecture before the workshop, it is relevant to go over IIO threats and capabilities a second time. After this, the moderator introduces the main scenario, setting the tone for what the world is like in the fictional situation. Then the moderator presents the specific challenges that each group will face and takes any questions the group might have before the start, to make sure everybody understands the situation and what is going to happen next.

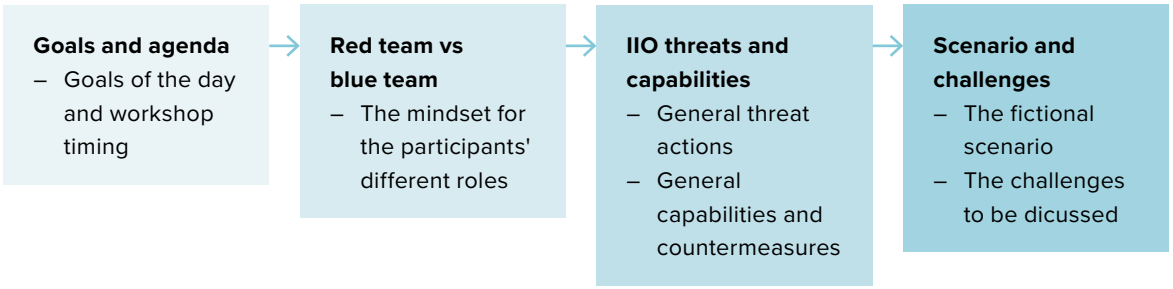

Figure 2. Suggested structure of the introduction for the workshop. Assigning participants their roles upfront helps direct their focus towards the relevant aspects.

Supporting documents

Before starting the discussions, go through the supporting documents the participants can use. For the workshops conducted in Sweden in November 2023, the participants had a lecture from the MPF and used the *Countering Information Influence Activities* handbook as an assisting document throughout the workshop.

Discussion phases for the challenges

Phase 1: Now the challenges can be presented one at a time (Figure 3). The workshop revolves around challenges that describe a situation where an actor has to react to a threat. The challenges should be expressed as simply as possible, whether written on the whiteboard or given out as a handout. Challenges are something that the moderator has chosen beforehand and adapted to the organisation and is therefore the "start-state" of the blue team discussions.

Phase 2: The blue team starts by proposing its approach to the situation. The moderators should keep guiding questions in mind and use them to steer the conversation appropriately if the participants get stuck. The main question to be addressed is:

- What actions can be taken to address the situation and how can the organisation's resources be leveraged to achieve success?

Phase 3: After the blue team has proposed its solutions, the red team reflects on potential reasons why the blue team's efforts may not succeed, or creates counteractions to the blue team's actions. The key question to be addressed is:

- What factors could impede the success of the blue team's actions, or what actions could be taken by a threat actor to prevent the blue team's efforts?

This phase indicates why it is so important for the red team participants to have in-depth understanding of the organisation, so that they can question or even counter the blue team's efforts with reasonable awareness of whether the blue team's endeavours would work.

Phase 4: The blue team is then given one more opportunity to respond to the red team's actions, and the discussion concludes with an examination of what the blue team would have done differently in their initial move, armed with the knowledge gained from the red team's response.

This process generates multiple actions and counteractions, and prompts reflections on why certain approaches may not be successful in a given scenario. By looking back, the blue team gains insight into what it could have done differently, which can inform its future strategies. The process is repeated for each challenge that has been selected.

Keep in mind: Although the participants in the discussion have the freedom to explore their own ideas and approaches for countering the situation, the moderator should prepare specific questions to ask as the conversation progresses. These questions should prompt the participants to reflect on their activities related to anticipating, recognising, adapting, and learning. This approach helps to ensure that the discussion is structured and productive, while also enabling the participants to explore their own strategies.

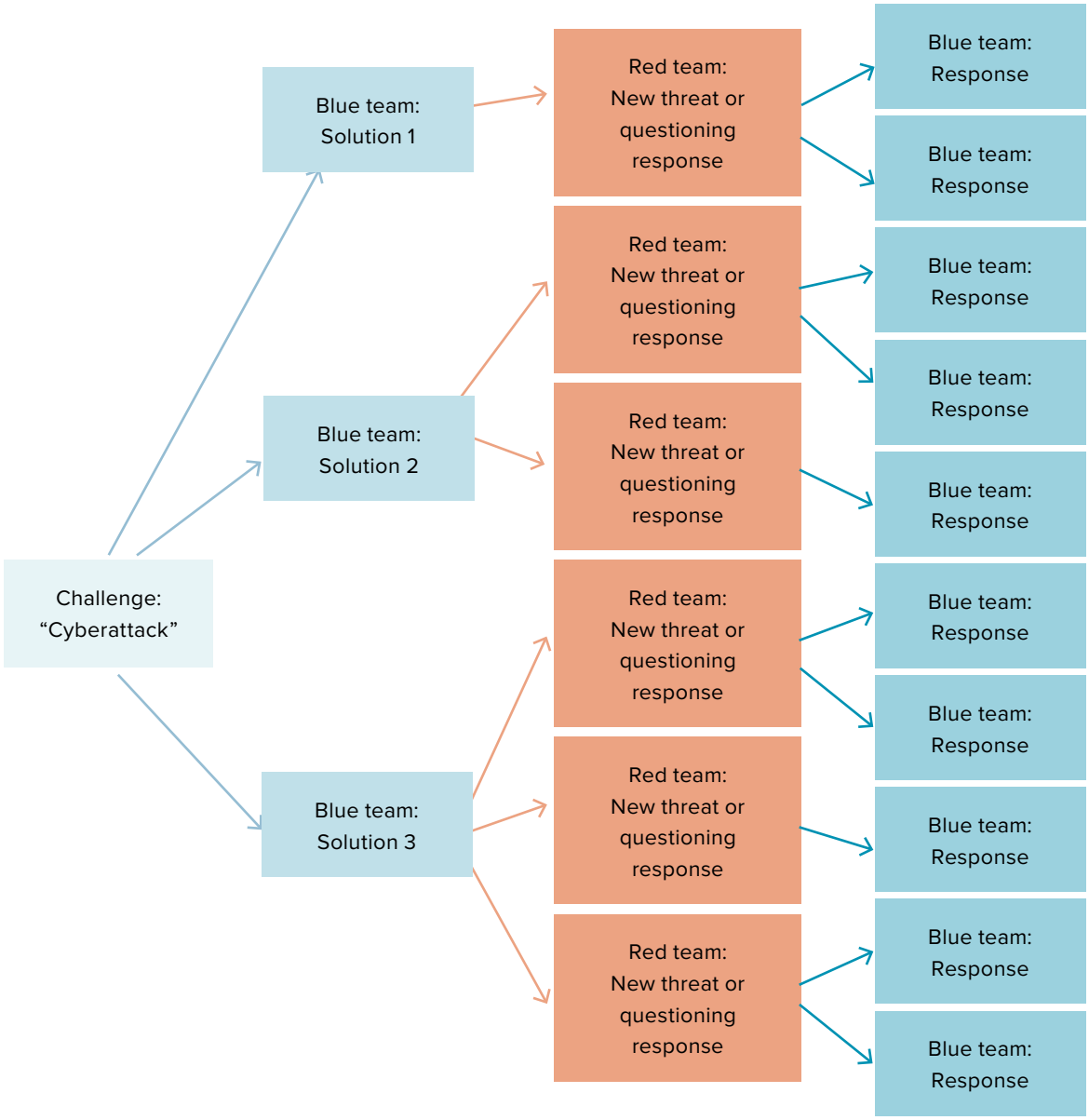

Figure 3. This flowchart demonstrates the team discussions and how they typically progress. Additionally, it serves as a method for organising discussions on a whiteboard to facilitate documentation and analysis.

Group discussions and prioritisation

Phase 5: When the blue team vs red team exercise is considered finished, the discussion for the gap analysis can start. The group endeavours to prioritise the different capabilities identified during the workshop and suggest possible areas for development. The aim is to clarify the necessary resources needed for such development. The identified capabilities are marked according to the following criteria:

- Activities that the actor can currently perform and that meet their needs (marked with green stickers).
- Activities that the actor can currently perform but they wish to develop further (marked with yellow stickers).
- Activities that the actor cannot perform currently (marked with red stickers).

The yellow and red capabilities are then discussed in more detail, including the following questions:

- How can these capabilities be further developed, and what resources are needed for the actor to perform these capabilities (e.g. more staff, bigger budget, certain tools)?
- Which of these capabilities should the actor prioritise for development in the near future, and which ones can wait? What would have the greatest impact on their general capability?

If there is time left:

- Was there any activity in the supporting handout document that was not used, but that you consider should be prioritised? Argue for why that is.

Part III—Workshop analysis

Understanding capability through organisational structure

There is a lot to be said about capability building, but for this workshop and generating analysis afterwards there are two relevant perspectives. First is the threat perspective, which can be seen from a growing scale. Capabilities and activities will have to become more advanced as the threat gets more comprehensive. This indicates that plans for capability development should be based on the expected threat level. Therefore, scenarios and challenges need to be adapted according to an actor's threat perception or their risk analysis. The type of threat which the target institution might face depends on the threat actor's aims of influencing the target audience in a larger society. This is where a point of contact from the organisation that is participating in the workshop becomes important.

There is also an organisational perspective, which focuses on understanding capabilities based on an organisation's functional structure in order to create resilience, such as being able to map out what kind of capabilities a specific actor might need and what kind of function they fulfil. Becker's functions for resilience provide a framework for understanding these working sets of activities, which can be

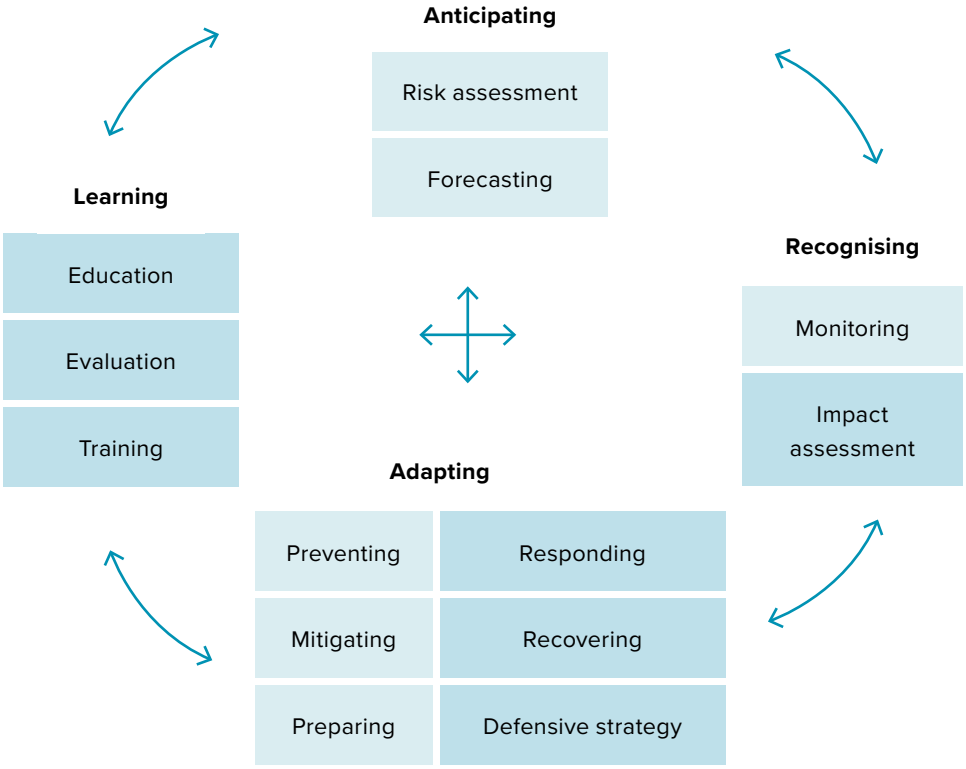

Figure 4. Becker's resilience system showing where the activities to counter IIO can be placed based on their purpose. The blue areas are reactive functions and the white areas are proactive functions. In this picture, Education and Training have been added to Becker's framework.

Anticipating disinformation requires proactive capabilities and activities such as risk and threat assessments, forecasting, contingency planning, and policy development to increase preparedness.

Recognising disinformation requires both proactive and reactive functions, including monitoring capabilities and documentation to create indications for recognition. Reactive functions include impact assessment and investigation into negative impacts on public discourse. To recognise disinformation campaigns, organisations can monitor social media and set up systems for reporting suspicious activity.

Adapting includes both proactive and reactive functions. Proactively, organisations can prevent and mitigate disinformation by increasing media literacy, creating public awarenes s, and developing partnerships. They can also prepare for potential threats by establishing partnerships and publishing relevant analysis. Reactively, organisations can respond to disinformation by using counter-branding, fact checking, debunking, and counter-messaging. Recovery may involve publishing analysis, conducting post-incident reviews, and developing strategies to rebuild trust and repair damage to reputation or public trust.

Learning is mainly a reactive function done over time in response to events or specific activities. To improve continuously, organisations can conduct regular research and analysis, implement training programmes, create evaluation structures, and share best practices with others, feeding back into the cycle, leading back to “Anticipation”.

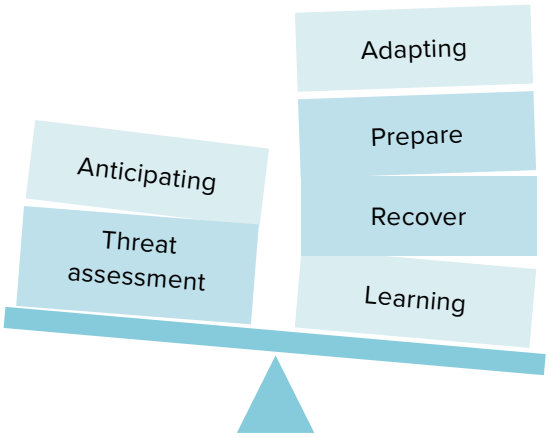

Figure 5. Examples of capabilities in different functions. The tipping scale illustrates where some functions might be lacking and therefore create an imbalance in an organisation’s resilience.

conceptualised at different levels of abstraction (Figure 4).[2] The main idea is that an organisation requires capabilities in all functions to operate effectively and be resilient to threats (Figure 5). Having capabilities in only one function or a few will result in an imbalance in the organisation’s resilience, since the functions are interconnected to one another.

Analysis

The most time-consuming aspect of the workshop is reviewing the documented results to provide a well-structured analysis for decision-makers to prioritise resources for capability development. A possible structure for the analysis phase is to start by giving a short description of the workshop and its objectives. Then continue by presenting each challenge, building on the countermeasures identified and the obstacles that the red team presented towards using these capabilities, indicating the gaps. Subsequently, the analysis should suggest the potential development possibilities for capabilities that were marked as needing continued development, with comments based on the prioritisation discussions conducted during the workshop (*for inspiration see Annex 3*).

In our test workshops, all three levels—local, regional, and national—were given the same challenges, only slightly adapted to fit their organisations' responsibilities and work in society. The results were shared with the participating organisations separately and will not be presented in this report, since they could indicate weaknesses in the organisations' capabilities. Instead the conclusions describe the overall capabilities that were discussed in the groups. The results from the workshops are presented in summary form below to demonstrate the potential outcomes from conducting a workshop.

Example of results from the workshops

I. Introduction

Three workshops were conducted with the Psychological Defence Agency in Sweden at local, regional, and national level between 7 and 9 November 2023. There was a point of contact (PoC) with the actors so that the scenario and challenges could be adapted to target their specific responsibilities in society. The PoC was also important in the dividing of the group to make sure that similar expertise was represented in both the red and blue teams.

In these workshops, each actor had representation solely from their individual organisation. This approach was chosen with the aim of identifying development opportunities within each organisation and concentrating on the capabilities of the participants, fostering discussions with those most directly affected. The objective was both to get the participants to reflect on their vulnerabilities and identify their current capabilities in identifying and countering IIO, and to generate a gap analysis based on their discussions.

II. Challenges and countermeasures

All three organisations were faced with the same challenges, just slightly modified to fit their responsibilities.

Cyberattack

The first challenge described a cyberattack that involved someone infiltrating the organisation's IT systems and uploading a new copy of the entire digital folder structure, as well as deleting and adding a large number of documents. Meanwhile, an investigation into the situation was under way, news starts to spread in the traditional media about leaked documents revealing that a manager within the organisation had misused large sums of

money or had otherwise been acting corruptly. Hacking and leaking documents often carry symbolic value as they can expose injustices that are otherwise concealed from the public. The narrative for the challenge was that all levels of society are corrupt, and public institutions cannot be trusted.

Deep fake

The second challenge continued with the same narrative of distrust in public institutions and corruption. This time a deep fake of the prime minister of Sweden was circulated on social media, announcing in a press conference that the organisation was part of a corruption scandal. Subsequently, there was a surge of hatred and threats towards the organisation and its staff, leading to sabotage against some of the organisation's facilities.

Nuclear incident

Challenge three described an international nuclear incident that could potentially spread some radioactivity to northern Europe, but with smaller particles that would not cause significant impact. False experts disseminated misinformation claiming that the authorities were lying to the public to avoid causing panic. This created a substantial information demand among the population, who were trying to find factual recommendations and advice, which is challenging when truth is mixed with lies and disinformation.

Blue team

The blue teams' responses generally involved initiating or continuing an impact assessment and internal investigation to understand how the challenge affected their organisation and determine the necessary steps forward. The crisis management group typically acted promptly to establish a comprehensive situational overview of the event. This not only facilitated extended national coordination and cooperation, acknowledged as essential to managing the situation, but also supported external communication efforts.

Recognising the need for effective external communication, most teams conducted target audience analyses, identifying their limitations in reaching specific societal groups. To address this, they initiated citizen dialogues to alleviate concerns and respond to questions from the most affected groups. Simultaneously, internal communication efforts intensified, providing tailored information to various groups of experts and employees.

All three organisations maintained information environment monitoring, but the challenges prompted a need for a more extensive and focused approach. The emphasis shifted towards a broader search for information to better address the evolving situation.

Red team

The red teams were very specific with their continued actions, focusing particularly on vulnerabilities that their organisation would struggle with. They searched for weaknesses that could be exploited by malicious actors in their organisation's digital infrastructure. The red teams employed a combination of sophisticated hacking techniques, social engineering tactics, and simulated cyberattacks to emulate real-world threats. They also explored the organisation's physical security measures, employee awareness, and overall resilience to potential breaches. They focused on the human element, recognising that employees could unknowingly become channels for cyber threats. They conducted simulated phishing campaigns, testing the organisation's susceptibility to social engineering attacks. These exercises helped identify areas where additional training and awareness programmes were needed to fortify the human firewall.

The red teams' understanding of the organisation's unique challenges allowed them to tailor their assessments of the specific threats the organisation faced, such as attempts to interfere with internal investigation and national cooperation, as well as continuing to spread false claims about the organisation to a specific audience that was already vulnerable to disinformation.

III. Existing capabilities

It is evident that the preparedness of the organisations on all levels is robust in national and regional coordination and cooperation. The actors recognised the significance of creating collaborative partnerships at all levels, ensuring a synchronised response that leverages collective resources and expertise to effectively address a range of challenges. This is possible due to the general coordination and cooperation structure integrated in the Swedish system of total defence.

Notably, the organisations demonstrate a high level of proficiency in crisis communication, particularly in the realm of external communication. Through planning and audience analysis, the organisations design targeted messages that resonate with various stakeholders. This capability positions them well to manage public perception, disseminate accurate information, and cultivate support during times of crisis.

A key strength lies in the establishment of agile crisis management groups within the organisations. These teams display a commendable ability to swiftly assimilate evolving situations, create a comprehensive situational picture, and formulate strategic responses. Their agility helps guide the organisations through crises and minimise potential impacts.

Furthermore, the organisations put a strong emphasis on information environment monitoring. This capability allows them to navigate through large amounts of information, extract valuable insights, and make informed decisions.

IV. Development possibilities

Evidently, even if the organisation had information environment monitoring capability, it was challenging to cover monitoring specific platforms and content that was audio or video based and convert that audio or video to written text. Participants recognised the need for specialised competence and expertise to interpret unfolding events and anticipate potential threats. The discussion also emphasised the importance of national support in monitoring, acknowledging the benefits of a collective approach to enhancing situational awareness.

The communication plans component prompted reflections on tailoring messages for specific target audiences and employees. Deliberations included considerations of time allocation for debunking misinformation and social media monitoring. Organisations grappled with questions of narrative focus, contemplating the optimal balance between reactive measures and proactive storytelling.

In identifying resources needed for capability improvement, participants acknowledged the significance of allocating dedicated staff, budgetary provisions, and advanced tools. Discerning that information environment monitoring and communication plans demand specialised skills, organisations expressed a commitment to investing in training and recruitment.

V. Conclusion

Anticipating

Anticipating a threat is based on having a perception of risk and being able to make forecasts for possible future risks. All the participating organisations have a statutory obligation to carry out risk and vulnerability analyses where IIO should be included. This can contribute to creating an organisational understanding of what effect IIO might have on their organisation and the risks entailed.

Forecasting, on the other hand, is more difficult to do that requires a multidimensional approach. It is difficult for organisations with limited resources to have both the time and expertise to facilitate it. In our workshops it was clear that only one of the participating organisations would have the working structure to do this.

Recognising

In order to recognise a threat in the area of IIO, it is essential to be able to make an impact assessment in connection with an event and to continuously monitor the information environment. The organisations' experience of this is extensive. Their information environment monitoring is proficient, and they have the capability to scale up to create a consequence assessment based on what has happened. The main challenge, however, is being able to follow what happens on platforms that are mostly in other languages and media (of all forms) that a specific target audience might consume. Here they need to make their own assessment and analysis of which platforms they should be on and monitor, and what joint information environment monitoring capability would look like, how it would function, and with whom.

Adapting

A crucial aspect of preparation involves the establishment of crisis management groups, dedicated teams equipped to handle crisis response and management. Additionally, fostering national and regional cooperation and coordination emerged as a key strategy, enabling a more unified and collaborative approach to challenges.

The preventive focus meant organisations should invest in robust IT security measures to prevent information breaches. Simultaneously, engaging in open dialogue with citizens emerged as a proactive strategy to address concerns and tackle misinformation at its source.

In the realm of mitigation, organisations should focus on building their own narrative and brand strength to counter negative impacts. Promoting media literacy was another cornerstone, aiming to enhance public understanding and critical evaluation of the information encountered. General preparedness, viewed as a holistic measure, was recognised for its potential mitigating effect on a range of challenges.

When responding to challenges, organisations highlighted the importance of timely and accurate dissemination of external information. Active debunking, or countering misinformation with a fact-based response, was identified as a critical component. Target audience analysis, the nuanced understanding of diverse audience needs, and effective communication in various languages were also emphasised.

In terms of defensive strategy, organisations emphasised the importance of crafting narratives that defend against threats and react to events. Clear guidelines and rules for the use of different communication channels were identified as essential, along with communication efforts that may necessitate debunking, powerful moderation, and trust-building measures.

While the majority of efforts concentrated on adaptive functions, there was less focus on recovering capabilities. Building trust emerged as a crucial aspect of recovery campaigns, coupled with work recovery efforts post-incident.

Learning

Evaluative measures involve carrying out assessments and investigations not only to understand past events but also to enhance practical skills through practice and training. All the organisations have the capacity to do evaluations and investigations after events have occurred and to hold regular education and training sessions for staff, ranging from role-specific to group training sessions. Some additional education might be necessary for some competency areas, as well as joint training on organisational structure with a focus on IIO events.

Part IV—Conclusions and recommendations

Overall, the workshops indicate that the methodology is well suited to generate useful results for participating organisations. The discussions on the challenges allowed practitioners and analysts to discuss their vulnerabilities and capabilities regarding IIO and also to reflect and agree upon what they want and need to improve.

The methodology creates a structure of thinking that the participants were quick to adopt, and the objectives and their roles were easy to understand. Initially it was assumed that, at the local level, municipalities would have more difficulty adopting the mindset of countering IIO, since this was not a usual aspect of their everyday functions. However, this idea rapidly proved to be wrong, since the challenges were altered in such a way that IIO risked affecting their areas of responsibilities. This can be achieved if the moderator has taken the time to get to know the organisation and has a PoC from the organisation that will do the workshops to get insight into how to alter the challenges based on their work. The scenario and challenges were difficult but not impossible to manage, and they created a situation that motivated the participants to act.

It is important for the participants to be open-minded during the workshop. It isn't always easy to discuss what isn't working or to admit that your role has limitations or even flaws. It can be difficult to create a safe environment where everyone can be open and exchange opinions. During the workshops, it was clear that most of the participants went into the room with a peer-to-peer learning mindset. Of course, groups where this kind of environment is achievable cannot always be expected. When difficulties arise, it is important to have a moderator who can lead the groups by asking questions and challenge the participants' statements.

The number of challenges can be adjusted. After two challenges, it was clear that the organisations' countermeasures were already exhausted and identified. However, going through an additional round created a data saturation point, which is useful for determining the stage at which collecting additional data no longer provides new insights or information.

Overall the workshops were successful in fostering collaboration and problem-solving, and emphasised the need for ongoing refinement based on participant feedback.

Annex 1: Scenario

The political tensions between Russia, Belarus, Iran, China, and the NATO countries have increased. Iran is openly sending weapons in support of the Russian war and aggression against Ukraine. Belarus has sent troops for some time to aid Russia. NATO has sent troops to Ukraine to defend the lines that the Ukrainians have been able to hold so far against Belarus, but not yet against Russian troops. In the last couple of weeks the Russian air force has violated airspace over the Baltics and Poland. Chinese rhetoric towards Taiwan has hardened and for some time security specialists have expected an attack in the near future.

Russia is severely economically destabilised. People in the country are badly affected, but Russia is trying to handle this by increasing payments to the poorest. The EU economy is still stable and approximately the same as over the last five years.

A series of hidden cyberattacks and physical sabotage has targeted social functions where someone tries to cover their tracks and/or direct suspicions elsewhere. The attacks seem to have been aimed mainly at local supply systems and private actors and companies, rather than towards strategic goals. After some time they start to focus on infrastructure disruptions, which then happen repeatedly.

There is an increase in advanced data breaches. The periodic disruptions to the electricity supply, as well as to data and telecom systems, contribute to increased disruptions in other supply systems and social functions. It is difficult to manage and coordinate operations, and access to electronic control systems is limited. The problems are amplified by cross-border effects.

The spread of propaganda via internet activists and alternative media conveys a skewed image of your country. Information influence operations, which primarily utilise the information infrastructure of open societies in terms of social media and blogs, as well as indirect TV (YouTube news channels), radio, and newspapers, have a negative impact on public trust in authorities and politicians.

The impact on society's functionality is so far fairly limited, but concern is still spreading among the public. People's perceived insecurity is increasing and leads to indirect effects such as anxiety and confusion as to what is actually happening and who is responsible.

Annex 2: Challenges

Demonstrations

Over the past year people have become frustrated about inflation and increased costs of food, fuel, and energy. This has led to tougher rhetoric regarding the situation on social media and in the international news media. Both propaganda media and traditional media are sharing harsh rhetoric articles about the country's situation. A closed group on a social media platform has planned a demonstration outside your workplace, which is seen as representative of the public sector. A large crowd gathers, chanting that you are responsible for the situation in which society finds itself. There is a concern that this might become more violent.

Narratives: The state has failed since it can't mitigate the crisis. If you don't support the government there is no freedom of speech. The government's foreign policy is detrimental to the country.

Techniques: False information is spread in closed social media groups. Websites, blogs, and YouTube channels that function as alternative media outlets spread dis- and misinformation using 'experts' and correct information, but use the latter in malicious contexts. Organisations that call themselves NGOs also add to these narratives.

Public demonstrations

Legitimate demonstrations are symbolic actions used to promote a certain political issue or position. They are an important element of the democratic dialogue. Hostile actors, however, may orchestrate demonstrations to falsely give the impression of strong support or dislike of a particular issue (also known as astroturfing).

Echo chambers

Organic sub-groups in which people communicate primarily with others who hold similar opinions and beliefs are called echo chambers; they exist both online and in real life. For example, people with similar opinions are likely to read the same newspapers and socialise with each other, and therefore may be rarely exposed to ideologically different opinions. This can be exploited online to spread targeted information to specific groups.

Bots

Bots are computer programs that perform automated tasks, such as sharing certain types of information on social media or answering FAQs on customer service platforms. They can also be used to emphasise particular messages online, to spam discussion forums and comments, to like and share posts on social media, and to implement cyberattacks.

Bandwagon effect

People who feel they belong to the majority are more likely to voice their opinions. Bots can boost the number of likes, comments, and shares of a social media post to give the impression of social acceptance. This appeals to the cognitive need for belonging and facilitates further engagement from actual human users.

Questions

- What functions and capability do you have to **anticipate** threats?
- What functions and capability do you have to **recognise** events?
  - Monitoring or assessing: What kind of information would you most likely find with the methods that you use? How do you use the information you collect or become aware of?
- What functions and capability can you use to **adapt** to the situation?
  - What can you do about the narratives and technics used?
- How do you **learn** from what has happened?

Cyber incident

The cyberattacks that have happened recently have also affected your organisation. Following a breach the information stored in common map structures has been rearranged and newly reuploaded. As far as you can tell there are several files and documents missing as well as new ones added. Your organisation has not yet managed to complete an inventory of all the documents. At the same time news is breaking about documents being leaked and published by your institution. The main story is how your chief executive has been swindling money.

Narratives: All levels of society are corrupt. You can't trust public offices and government agencies.

Techniques: By hacking your network someone has made it reasonable to question if your systems are secure and if you are now compromised. This undermines confidence in the particular system or the body responsible for it. Leaking the stolen information carries symbolic weight as leakers traditionally reveal injustices and cover-ups unknown to the public.

Phishing

Phishing is a technique that tricks users into revealing their passwords or other sensitive information online. Phishing involves automated spamming of emails that look legitimate but actually lead to fake websites that harvest any personal information entered. Spear phishing is a more sophisticated type of phishing used to access information on secure computer systems.

Hacking

Hacking involves acquiring unauthorised access to a computer or a network and is a crime.

As an information influence activity, hacking can serve as a symbolic act where the intrusion itself is secondary. The actual objective is to arouse suspicion that a system is insecure or compromised, in order to undermine confidence in the system in question or a body responsible for the same.

Forgeries

Fabricating official documents is an effective way of making disinformation appear authentic. For example, fake letterheads, stamps, and signatures can be used to produce forged documentation.

Leaks

Leaking can consists of releasing information that has been obtained by illegitimate means. This carries symbolic weight as leakers traditionally reveal injustices and cover-ups unknown to the public. However, when used as an information influence activity, leaked information is taken out of context and is used to discredit actors and distort the information environment. Leaked information is sometimes obtained through hacking or theft.

Questions:

- What functions and capability do you have to **anticipate** threats?
- What functions and capability do you have to **recognise** events?
  - When would you have discovered the breach?
- What functions and capability can you use to **adapt** to the situation?
  - What do you do to handle the leak while you confirm which documents are false and which ones are real?
- How do you **learn** from what has happened?

Increased hybrid threats and social distress

Since NATO sent troops to the Ukrainian border and air violations and cyberattacks have taken place repeatedly, a wide discussion has emerged among the public that it might be the first signs of an invasion towards your own country. However, the state agencies say that they do not see that as a possibility in the near future. Nevertheless, misinformation and disinformation about the risks of being a part of NATO are causing some people concern and the country's contribution to NATO is being questioned. Discussions mostly take place on social media and in closed groups. The level of alert, amid concern about the possibility of a new war starting, is rapidly increasing across the country and causing indirect effects such as anxiety and confusion among the public as to what is actually happening and who is responsible.

Narratives: NATO is a threat to the national interests of Country X. Country X's army is underdeveloped/incompetent. Country X is an irrelevant state. NATO is not going to help Country X. Mobilised citizens will be cannon fodder.

Techniques: Social media and bots are used to spread ideas and arguments presenting skewed images of the country and its work with NATO. In particular TikTok, Instagram, and marginal media (websites, blogs, YouTube channels) spread a large amount of distorted messages.

Misappropriation

Misappropriation is the use of factually correct content presented on an unrelated matter to frame an issue, event, or person in a deceptive way. For example, a false news article might use pictures from an unrelated event as proof of something's existence.

Hijacking and straw man arguments

An example of hijacking is taking over an existing debate and changing its purpose or topic. This is particularly effective when applied to hashtags and memes, and may also be used to disrupt events or countercultural social movements.

A straw man argument is used to discredit an adversary by attributing positions or arguments to them that they do not agree with and then arguing against those positions.

Bots

Bots are computer programs that perform automated tasks, such as sharing certain types of information on social media or answering FAQs on customer service platforms. They can also be used to emphasise particular messages online, to spam discussion forums and comments, to like and share posts on social media, and to implement cyberattacks.

Fake media

Disinformation can also be circulated by creating fake media platforms that look like, or that have a web address similar to, a real news site. It is relatively easy and inexpensive to create a fake website online that looks almost identical to a real website but publishes very different content.

Questions

- What functions and capability do you have to **anticipate** threats?
- What functions and capability do you have to **recognise** events?
- What functions and capability can you use to **adapt** to the situation?
- How do you **learn** from what has happened?

China activates the united front against Taiwanese interests

The EU has reacted by condemning China's hardened rhetoric towards Taiwan. China has amplified existing narratives in South American and African countries' social media and news about how the West is proclaiming a Western colonial rhetoric. This eventually starts to show up in your country as well. The narratives suggest that China has a moral right and duty to protect its territory and population. They portray your country as a US puppet state that is trying to deny China's right to retrieve its territory. This follows with denying diplomatic visas and access to diplomats traveling to China. Breaking news has emerged stating that an executive connected to your organisation has been arrested for espionage and China will take economic action against businesses in your country.

Questions

- What functions and capability do you have to **anticipate** threats?
- What functions and capability do you have to **recognise** events?
- What functions and capability can you use to **adapt** to the situation?
- How do you **learn** from what has happened?

Narratives: Country X is a racist and/or Sinophobe country. Country X does not follow its own constitution. Country X is hypocritical. Country X has a Cold War mentality. China is misunderstood: it needs to defend its territorial integrity.

Techniques: China purchases advertisements and places news articles in well-known newspapers proclaiming their good intentions and how their actions benefit everyone economically. Social media is flooded with arguments positive towards China with no understanding of why their actions should be condemned.

Whataboutism

Whataboutism attempts to deflect criticism by drawing false parallels with similar yet irrelevant phenomena.

Gish gallop

The Gish gallop aims to overwhelm an opponent with a flood of arguments, facts, and sources, many of which are spurious or unrelated to the issue at hand.

Dark ads

Messages tailored to an individual's psychographic profile are considered dark ads. Data gleaned from social media and other sources can be organised into a database of individuals with similar ideological opinions and personality traits. Advertisements that are only shown to certain individuals can include messages that appeal to their psychological leanings and encourage certain behaviours.

Radioactive leak

There are reports of an explosion at a nuclear power plant in Ukraine, which has led to radioactive pollution of the surrounding area. Experts say that some radioactivity (radioactive cloud movement) could be expected to spread to northern Europe, depending on the wind. However, in comparison with the Chernobyl nuclear disaster, only small radioactive particles will likely be detected that would not affect humans in a long term. People start to panic and speculate despite the experts' assessment.

Individuals that claim to be experts are interviewed on alternative media (mostly on YouTube channels) saying that the consequences will be devastating for your country, and that we cannot be sure that politicians would tell us the complete truth, to avoid panic. Some traditional media accidentally publish some of these false claims. People hoard iodine tablets and protective equipment, making it difficult for actors and authorities to purchase them for work for which they are required.

Narratives: Everyone will be affected. You can protect yourself. You are safe if you follow these steps (irrational protection measures). Politicians are lying to us.

Techniques: False experts are being used and broadcast on social media platforms. The truth is mixed with falsehoods and disinformation. It is difficult to explain to the population what is true and what is not true regarding the expected effects of the radiation. False pictures from the site are being spread showing a much larger explosion and greater damage than are actually the case.

Imposters and cheats

Imposters pretend to be someone they are not, i.e. they adopt the personal or professional identity of another person. Con artists claim to have expertise or credentials they lack, e.g. someone who falsely claims to be a medical doctor or a lawyer without having undergone the required training.

Potemkin villages

Malicious actors with sufficient resources can set up fake institutions and networks that serve to deceive and mislead. Potemkin villages are false companies, research institutions, or think tanks created to authenticate or 'legitimise' targeted disinformation.

Misappropriation

Misappropriation is the use of factually correct content presented on an unrelated matter to frame an issue, event, or person in a deceptive way. For example, a false news article might use pictures from an unrelated event as proof of something's existence.

Questions

- What functions and capability do you have to **anticipate** threats?
- What functions and capability do you have to **recognise** events?
- What functions and capability can you use to **adapt** to the situation?
- How do you **learn** from what has happened?

AI and deep fakes

A video of the prime minister of your country goes viral on social media platforms (mostly on TikTok and Instagram). The video shows the prime minister giving a press conference and pointing out that your organisation is part of a corruption racket. The government is quick to release information to mainstream media that the video is a sophisticated fake.

Nevertheless, hate comments follow and your organisation receives threats and your premises are damaged.

Narratives: Governmental agencies are corrupt and can't be trusted. This specific agency is swindling public tax funds.

Techniques: An advanced deep fake is circulating on social media and algorithms are affected by bots increasing views, likes, and shares.

Deep fakes

Advanced machine learning algorithms can now be used to manipulate audio and video very convincingly, for example showing a real politician delivering a fictitious speech. It is even possible to superimpose the face of another person onto pre-existing video footage and digitally reconstruct a person's voice.

Bots

Bots are computer programs that perform automated tasks, such as sharing certain types of information on social media or answering FAQs on customer service platforms. They can also be used to emphasise particular messages online, to spam discussion forums and comments, to like and share posts on social media, and to implement cyberattacks.

Questions:

- What functions and capability do you have to **anticipate** threats?
- What functions and capability do you have to **recognise** events?
- What functions and capability can you use to **adapt** to the situation?
- How do you **learn** from what has happened?

Annex 3: Suggested headings for the analysis

Note that this is just one example of how the analysis could be structured and that the specific details will vary depending on the workshop's objectives, participants, and challenges.

I. Introduction

- Brief description of the workshop and its objectives

II. Challenges and countermeasures

- Overview of the challenges presented in the workshop
- Identification of the countermeasures that the blue team proposed to address each challenge
- Analysis of the red team's response to each countermeasure, highlighting any obstacles or limitations

III. Existing capabilities

- Presentation of the existing capabilities that the actor can currently perform in the context of information influence activities, divided according to their functions (anticipating, recognising, adapting, and learning capabilities)
- Discussion of the capabilities that are marked with green stickers, indicating that they are sufficient for the actor's needs

IV. Development possibilities

- Presentation of the capabilities that are marked with yellow and red stickers, indicating that the actor wishes to develop them further or cannot perform them currently
- Discussion of the potential development possibilities for each capability, including any comments based on the prioritisation discussions conducted during the workshop
- Identification of the resources (e.g. staff, budget, tools) that are needed for the actor to be able to perform each capability

V. Conclusion

- Summary of the main findings and recommendations for capability development based on the workshop results

Endnotes

1 Daniel K. Jonsson, *Att använda scenarier i planering för civilt försvar* [Using scenarios in civil defence planning]. FOI-R-4434-SE. Totalförsvarets forskningsinstitut, 2017.

2 P. Becker, Sustainability Science—Managing Risk and Resilience for Sustainable Development. Amsterdam: Elsevier, 2014.

Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org