Capability assessment for StratCom - Using the new risk perspective to inform the development of effective response capability assessments for countering information influence operations

Lindbom, Hanna

2022

Document Version:
Publisher's PDF, also known as Version of record

978-9934-619-10-6

CAPABILITY ASSESSMENT FOR STRATCOM

USING THE NEW RISK PERSPECTIVE TO INFORM THE DEVELOPMENT OF EFFECTIVE RESPONSE CAPABILITY ASSESSMENTS FOR COUNTERING INFORMATION INFLUENCE OPERATIONS

Published by the
NATO Strategic Communications
Centre of Excellence

ISBN: 978-9934-619-10-6
Author: Hanna Lindbom
Project manager: Henrik Twetman
Design: Kārlis Ulmanis

Riga, March 2022
NATO STRATCOM COE
11b Kalnciema Iela
Riga LV1048, Latvia
www.stratcomcoe.org
Facebook/stratcomcoe
Twitter: @stratcomcoe

About the author:

Dr Hanna Lindbom is an Assistant Professor for the Division of Risk Management and Societal Safety at Lund University in Sweden. She is also Assistant Director for the master's programme in Risk Management and Safety Engineering and the bachelor's programme in Fire Protection Engineering. Her research focuses primarily on the proactive assessment of response capability and how such assessments support the reduction of negative consequences from potential future events. She works closely with public actors in Sweden on the local, regional, and national levels to study how various risk management activities are related and how they can be integrated to better contribute to the long-term reduction of losses. Hanna teaches several courses related to risk management and risk assessment and supervises graduate students working on various aspects of the field.

> When facing a potential threat, we don't want to just sit and wait for something bad to happen, experience the impact, and only then consider how best to respond.

Introduction

There are no established models for assessing an organisation's capability to respond to information influence operations (IIOs).[1] While great efforts have been made to improve our knowledge and understanding of IIOs and how to counter them,[2] and measures have been taken to strengthen democratic processes and to decrease societal vulnerabilities,[3] few efforts have been made to measure the impact of IIOs or to assess the efficacy of the countermeasures currently in place—the *response capability*—to mitigate those consequences.

When facing a potential threat, we don't want to just sit and wait for something bad to happen, experience the impact, and *only then* consider how best to respond. It is much better to be proactive and seek to develop a response capability that can prevent losses or effectively mitigate the negative impact of an adverse event when it occurs. To assess whether our response capability is sufficient we must be able to 1) clearly identify the critical assets we wish to protect and 2) accurately describe the response we have in place for when those assets are threatened.

Traditionally, 'risk' has been defined as 'a measure of the probability and severity of adverse effects',[4] but recent advancements in risk research have prompted a shift in thinking. The new perspective on risk management takes into account 'the effect of uncertainty on objectives'. [5] While these two orientations are largely compatible, incorporating what we know about uncertainties into estimates of response effectiveness rather than relying on probability calculations results in more robust and flexible capability assessments.

Capability assessments have been a key activity within crisis and emergency

management in the last decades. The purpose of these assessments is to support proactive decision-making concerning resource allocation for response preparedness. Traditional assessment models—the so-called indicator and index models—equate resources with capability; such assessments provide decision-makers with either a checklist of resources or a numerical representation that evaluates the resources available for a crisis response within a target range for acceptability.

While such models have proven utility in the business world, where production can be (more or less) planned, they are not well suited to crisis and emergency management where uncertainty plays a much larger role. The new risk perspective addresses this dilemma, suggesting a way forward for an assessment model that takes uncertainties into account, identifies the most effective response tasks and, in the absence of actual feedback and the wisdom of hindsight, provides the best possible information for making decisions regarding investments in capability.

The first part of this report describes response capability assessment—what it is for, what goes into preparing one, and why incorporating the new risk perspective leads to more useful information. The theoretical explanation will be illustrated with typical examples from the field of risk management concerning residential fires and the response capability of a local fire service. The second part of the report offers suggestions on how these concepts and ideas might be adapted for responding to IIOs. The report ends with concluding remarks and a glossary of terms.

Part I:
How to Describe and Assess Response Capability from the New Risk Perspective

Points of departure

We begin with four basic assumptions:

There are 'critical assets' we wish to protect from potential adverse events.

Most assets—the things we value—are relatively easy to identify and define. For example, we generally agree that human life and health, the environment, and the economy are important assets that should be safeguarded. However, the new risk perspective acknowledges that assigning value to tangible assets can at times be highly subjective; the definition and valuation of intangible assets, such as democracy, are even more complicated. Our understanding of what we wish to protect determines how we respond when these assets are threatened. We must clearly identify and define critical assets so that the premises underlying the response to protect them can be objectively assessed.

Example: A residential fire
A residential fire may result in serious consequences to human life and health, to the building itself, and to the surrounding environment—these are clearly critical assets we wish to protect. An effective response to a residential fire will mitigate the negative impact of the fire on these assets.

The future is uncertain.

We cannot say with certainty if and when an adverse event will happen and what consequences such an event would have. Although we take proactive measures to safeguard critical assets (for example, by investing in additional safety equipment or engaging in fire drills), we cannot fully guarantee protection. To improve our response capability, we must gather and analyse information to identify and understand the uncertainties involved.

Example: Uncertainties in the context of a residential fire
When considering the management of any potential risk, we must identify points of uncertainty. In the case of a residential fire, we might ask: When and where will the next fire occur? Will it be close to a fire station or far away in the rural countryside? Will the endangered building have ten floors or only one floor? Will there be people inside in need of rescue? Our response capability in the case of a residential fire, i.e., the extent to which we can mitigate the negative impact of the fire, will depend on all these factors.

It is crucial to differentiate between 'actual capability' and 'described capability'.

Actual response capability exists whether or not we have described it accurately; a fire service can influence the outcome of a fire even if its capability has never been assessed. This may seem obvious, but the distinction is crucial. Whenever we assess capability, we must strive to generate accurate information that is useful for the assessment. A poor capability description does not affect actual response capability, but an inaccurate description makes it impossible to assess capability effectively and may result in an unexpectedly insufficient response to a threat.

Example: Inaccuracies in the description of the response capability of a local fire service
Imagine that there are two fire engines at the local station, but one is in disrepair. Based on a capability description that includes two fire engines, the municipal government assesses the response capability of the fire station as sufficient. However, when called out to a large multi-dwelling residential fire, only one engine can actually respond. Conversely, imagine that several firefighters have been trained for smoke-diving, but have not registered their certification. The fire chief is unaware that this resource is available but, in the moment of need, one of the firefighters uses her new training to save a person who otherwise would have died.

There is an explicit link between response capability and the magnitude of the impact of an adverse event, but external factors and uncertainties also play a significant role.

Increased response capability will reduce potential consequences and diminished response capability will increase potential consequences. However, and this is a crucial point, the *actual consequences* of an adverse event may be worse than predicted even if response capability is increased. The reason for this is, again, uncertainty. Response capability is only one of many variables that can influence the outcome.

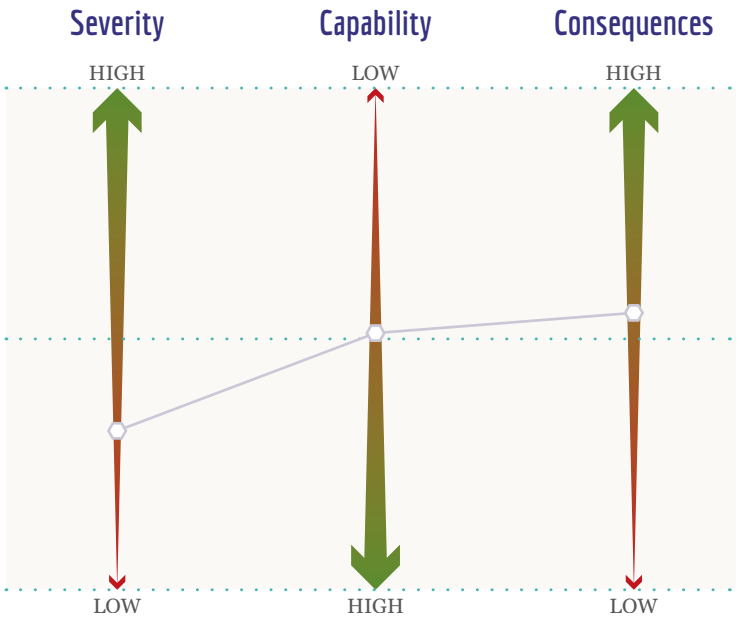

Figure 1. The relation between severity, capability, and consequences

The illustration shows that the severity of an adverse event can be measured on a scale from low to high. The same is true for response capability. These two factors together influence the magnitude of the consequences. High severity and low capability contribute to greater negative consequences, while low severity and high capability contribute to lesser negative consequences.

Example: Factors influencing the outcome of a residential fire

When the fire service responds to a fire, external factors can differ significantly. There is a substantial difference between the response needed to control a fire confined to a small space, such as a small storage building with a single point of access, and what is needed to control a fire that has spread into the attic of a multi-dwelling building. This example illustrates the relationship between the severity of an adverse event and response capability. Given identical resources and competences (knowable, internal factors), the capability of responders to mitigate negative outcomes will be completely different due to the difference in severity between the fires in the two examples.

These four assumptions—that there are assets we wish to protect, that the future is uncertain, that when we talk about responding to threats to critical assets it is important to be as accurate as possible, and that even when we invest in response the results remain unpredictable—are the cornerstones for the new perspective on response capability and response capability assessment.

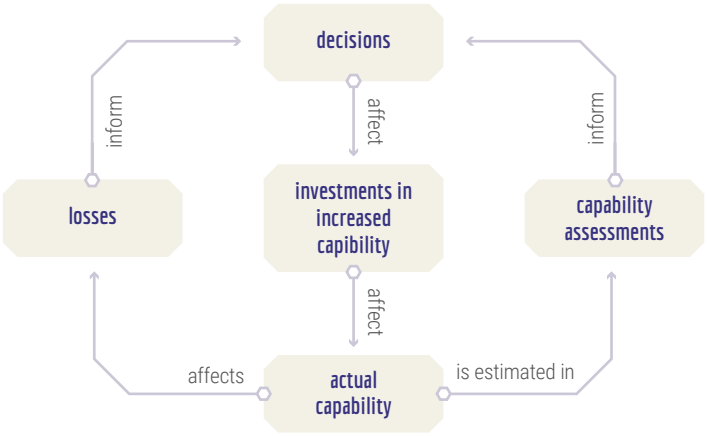

Figure 2. The role of assessments in informing decisions

This figure illustrates two sources decision-makers can use to inform their decisions regarding the need to invest in response capability: data concerning actual losses stemming from actual adverse events (as in the left-hand loop) and estimated outcomes from a response capability assessment (as in the right-hand loop).

Response capability and the purpose of assessment

'Response capability' can be defined as an organisation's *ability to mitigate the negative impact of an adverse event*. The purpose of a 'response capability assessment' is to support proactive decision-making concerning resource allocation for stated objectives, i.e., is our response capability sufficient to protect the defined critical assets or do we need to invest resources to increase capability?[6]

Actual response capability does not manifest outcomes until an adverse event actually takes place. An assessment provides a means of estimating capability in the absence of an adverse event. Of course, decision-makers can use information generated by actual events to assess if current capability is sufficient. However, the great advantage of the response capability assessment is that it creates the opportunity for proactive action—we do not have to wait for actual consequences to materialise but can base resource investment decisions on information provided by an assessment. When an assessment is well considered and its underlying assumptions are presented transparently, decision-makers have a solid foundation for justifying resource allocation.

Furthermore, inputs facilitating proactive action need not come only from direct experience or from assessments of one's own system. For example, the negative consequences of IIOs on the 2016 US presidential election rendered actual data that led decision-makers in other countries to proactively invest in response capability

Figure 3. Indicator and index models for capability assessment

The above list is a fictitious example showing how traditional indicators might be used to assess a fire service's capability for responding to a residential fire. The indicator model produces an assessment in which each indicator (a resource or procedure) is listed as either available (yes) or unavailable (no). The index model produces an assessment in the form of a numerical value that expresses capability—the greater the number, the greater the capability. In the index example we can see that if the fire service has *one* fire engine, the capability index is 5.657; with an additional fire engine the capability increases to 5.825.

based on indirect experience, i.e., what they had observed happening in the US.[7] However, carrying out an assessment of one's own capability will generate estimates grounded in data that is most relevant to one's own specific circumstances.

Traditional assessment models

Traditional assessment models—the so-called indicator and index models—equate resources and procedures with capability.[8] Both models describe the current state of the system using indicators, but index models assign a numerical value to each indicator, which is then multiplied by a predetermined weight expressing relative importance; the weighted indicators are then fed into a final calculation to arrive at a capability index—a numerical estimate of response capability.

Indicators and indices are suitable for stable systems with a low degree of complexity, where assessment designers have a good understanding of system behaviour and can validate that the selected indicators

demonstrate the successfulness of the system. One benefit of these models is that change in capability is relatively easy to measure—another boxed ticked or a higher number means an increase in estimated capability. Moreover, once they have been designed, such assessments are relatively quick and easy for decision-makers to use, as the terms are easy to present and explain and do not require detailed knowledge of the system.

However, as system complexity and rate of change increase, it becomes more difficult to design and validate indicators and indices. In complex systems the degree of uncertainty is significant, but indicator and index models measure only what can be known. For example, traditional assessment models will predict that the fire service has the same capability for mitigating negative outcomes in the case of a small, contained fire as in the case of a large, rapidly spreading fire, when of course it is reasonable to expect that, given the same response capability, the impact of a large fire would be much more severe. Moreover, what effect would an increase in capability from 5.657 to 5.825 have on critical assets (e.g., how many more lives can we save if we invest in a second fire engine as in the example above)?

In essence, indicator and index assessments are unable to reflect uncertainties and thus cannot inform decision-makers about how current response capability relates to the protection of a critical asset, nor do they provide guidance about what a specific investment could yield in terms of increasing capability. A response capability assessment grounded in the new risk perspective better supports decision-making, especially in complex environments. For this reason, the new risk perspective holds great promise for helping decision-makers address the complex challenges posed by information influence operations.

The new model for response capability assessment

At the outset we defined response capability as *the ability to mitigate the negative impact of an adverse event*. An assessment of such a capability grounded in the new risk perspective incorporates the four assumptions presented in Section 1.

Whereas indicator and index assessment models focus primarily on available resources, the new risk perspective stresses the importance of clearly identifying the critical assets to be protected (*Assumption 1*), including uncertainties in the assessment model (*Assumption 2*), describing as accurately as possible the effects of the tasks and sub-tasks that make up the response (*Assumption 3*), and making reasoned choices about which factors and what level of detail to include in the assessment model (*Assumption 4*).

First, the critical assets deemed worthy of protection must be identified and defined. This definition is a basic premise that must be explicitly understood as any protective

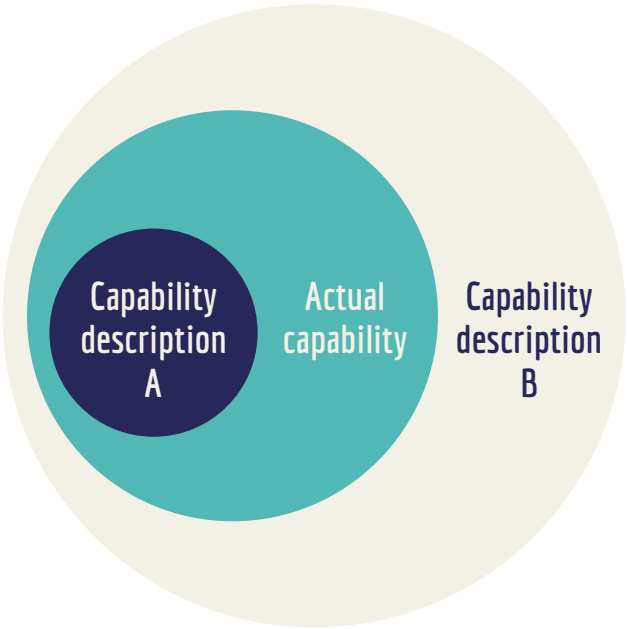

Figure 4. The difference between actual capability and possible descriptions of that capability

A capability assessment is only as good as the capability description it is based on. How well does the capability description represent actual capability?

response will be developed around this understanding.

Second, given that the future is uncertain, it makes sense to:

1. consider not only the potential impact of known and knowable factors on response capability but also consider and categorise the types of uncertainties—the unknown and unknowable factors—that might influence the effectiveness of our response in mitigating the impact of an adverse event on our critical assets.
2. to move from relying on an assessment of available resources to considering how those resources are used and what effect those actions have on mitigating the impact on the critical assets.

Research suggests that evaluating the effectiveness of *what responders do* yields better information about how an asset can be protected than simply listing the available resources for doing so. While indicator and index assessments generate descriptions using *nouns* (resources such as procedures, staff, equipment), the new model generates descriptions using *verbs*

(actions responders take) so that the *effect* of each action can be evaluated.

Third, to assess the suitability of our response capability, we must first formulate a 'description'. As mentioned above, *actual capability* exists whether we recognise it or not. To assess and operationalise capability, we must describe it as accurately as possible.

How does one go about formulating a useful capability description? Capability is not a monolithic entity. It is comprised of various tasks and sub-tasks of differing importance and efficiency, each of which can be described in terms of the *effect* it has on mitigating the impact of an adverse event. We can never be spot on but making our assumptions explicit allows others to understand what a description is based

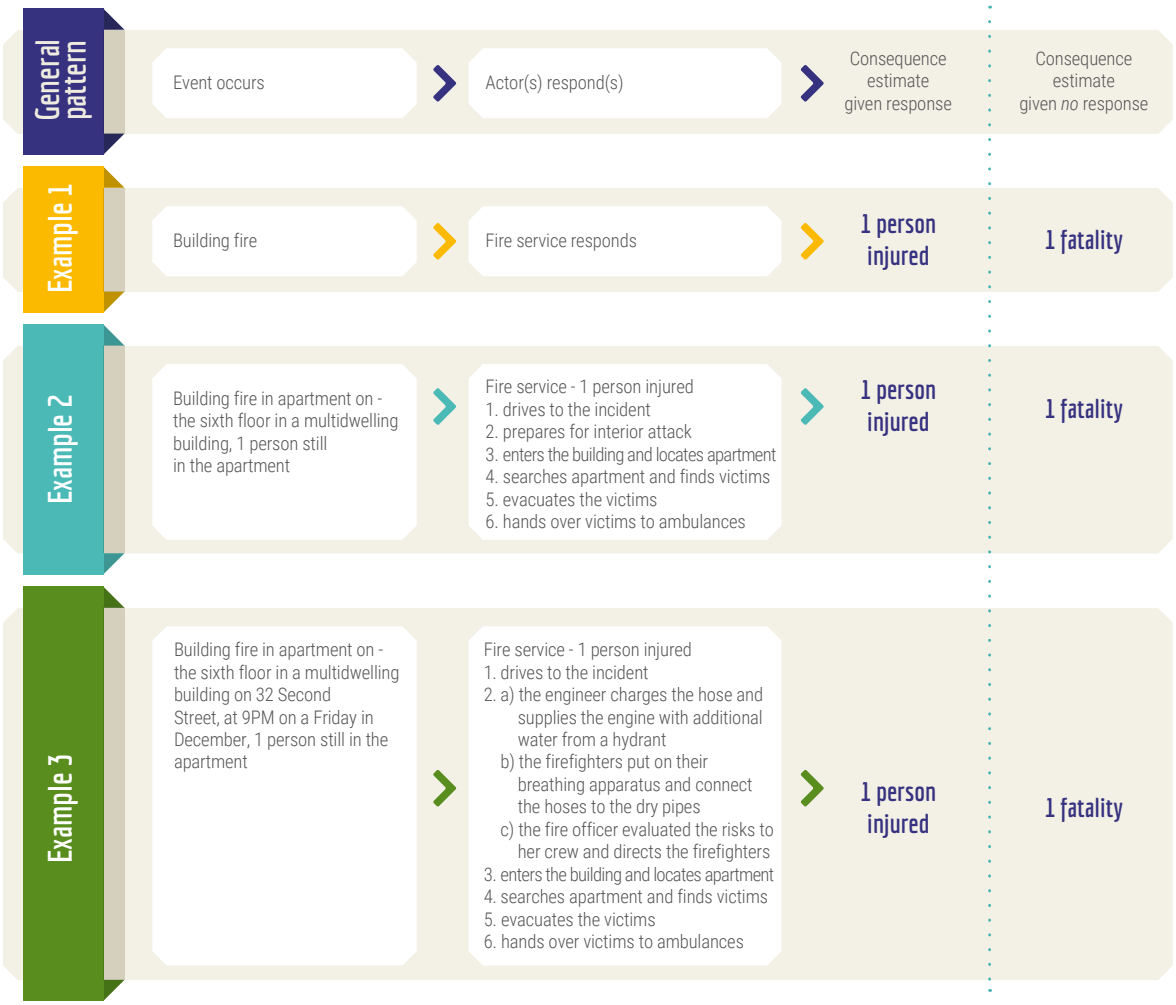

***Figure 5.* The *event–response–consequences* structure of a 'response scenario'**

This figure illustrates the underlying assumption that the impact of an adverse event is influenced by what responders do. Here, the same response scenario is described three times with increasing detail.

Figure 6. **General structure of a response scenario**

The first element of the scenario is the initiating adverse event, and the final element is the impact of this scenario on the defined critical assets. Between the two is a chain of potentially interrelated factors (input variables, or assumptions we make about each of the uncertainties when designing a potential response scenario) that influence the effectiveness of our planned response in mitigating negative outcomes.

on so they can judge its strengths and weaknesses.

Fourth, the new capability assessment model, which describes actions and their effects, can be informed by any number of 'response scenarios' that include varying levels of detail.

Example 1 provides only the most basic information. Example 2 includes more information about the event and lists the main actions performed by the fire service; this results in a better understanding of how we arrived at the estimated impact.

At first glance, the list of actions in Example 2 could be taken for a list of indicators as in *Figure 3* above; however, the key difference is that in *Figure 4* the response is comprised of tasks and not resources—verbs, not nouns. The new assessment, which frames response in terms of actions, makes explicit the connection between the actions taken and their effect on the outcome. This crucial connection cannot be elicited from the traditional models.

Example 3 provides even more detail. The analyst must determine what level is sufficient for a transparent and cogent depiction of the thought process behind the design but not so detailed that it becomes cumbersome and unnecessary.

Developing response scenarios using sensitivity analysis

To better understand the factors that influence what takes place between the onset of an adverse event and the outcome of that event in relation to protecting the defined critical assets, we can develop diagrams referred to as response scenarios. *Figure 5* illustrates the basic elements of a response scenario; the number of factors that can be included is flexible.

Every element of a response scenario represents an uncertainty. Some uncertainties we cannot control, for example where and when a fire will occur, what the weather conditions are like at the time, or how much fuel there is to feed the fire; some uncertainties

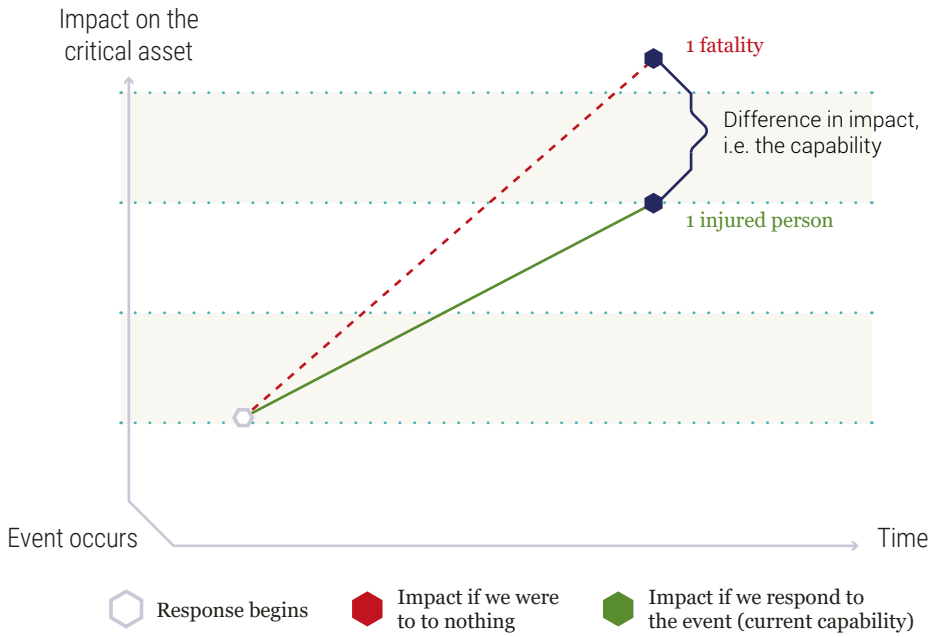

Figure 7. Capability description

This figure illustrates the difference in the impact of an adverse event if our planned response is carried out. It stresses the utility of the *effects* produced by response tasks in mitigating the negative impact of an adverse event. An organisation's *response capability* is the difference in impact between responding and doing nothing.

we can control, for example the actions we take when responding to the fire, how well trained the firefighters are, and what resources we choose to dedicate to this scenario. Each factor influences the next and response tasks are chosen depending on the factors included in the scenario.

Of course, including all potential influencing factors would make the scenario stretch towards infinity, so only those that have the greatest effect on the outcome should be included.

The most influential factors can be identified through 'sensitivity analysis', a tool commonly used in risk assessment. Sensitivity analysis identifies the most 'critical factors' to include in a response scenario by a systematic study of the magnitude of the effect a particular factor has on the outcome; by identifying the utility of each factor, sensitivity analysis can suggest how the number of factors can be reduced without losing crucial information.[9] Traditionally, sensitivity analysis is quantitative, but qualitative approaches also exist.[10] A well-executed sensitivity analysis can help analysts identify the most salient factors to include in a response scenario so that it contains sufficient detail to be useful, while not being so comprehensive that it becomes unworkable.

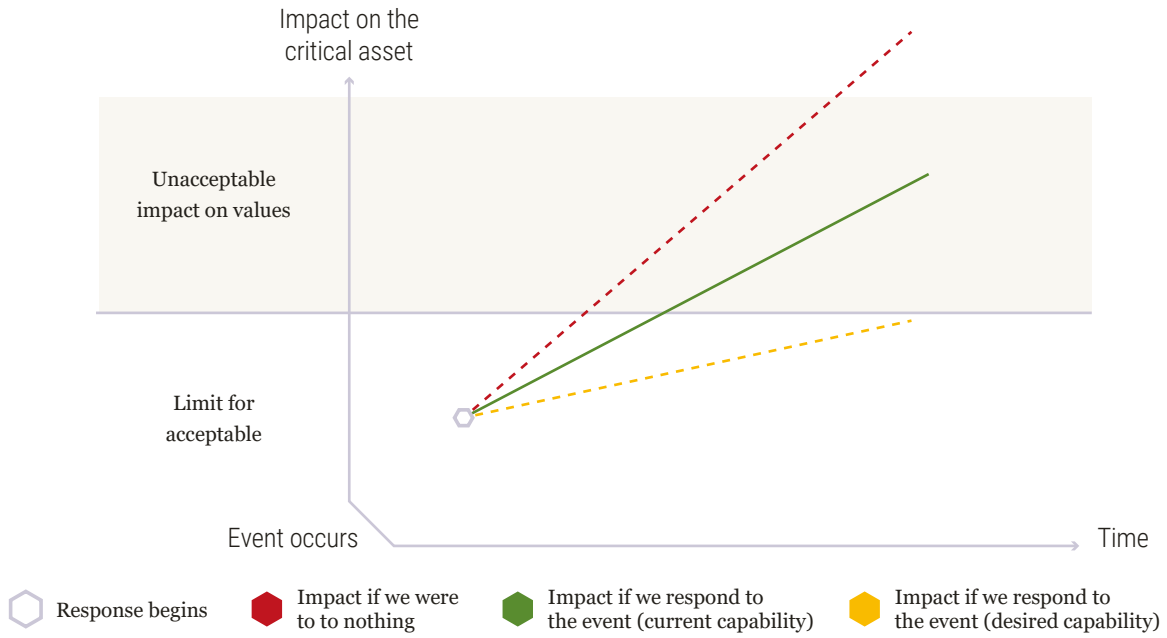

Figure 8. Diagram illustrating a response capability assessment

Comparing a capability description to assessment criteria results in a capability assessment decision-makers can use to justify their choices regarding investments.

Creating various response scenarios provides information about what effect we can expect to achieve with our planned response and demonstrates how we have arrived at this estimation. Transparency regarding these processes allows other stakeholders to evaluate and potentially improve the quality of the assumptions we rely on for the next steps.

There is much more to be said about response scenarios and sensitivity analysis but that is beyond the scope of the present article.

Capability description and what it tells us

Once we have addressed each of the basic assumptions inherent in the new risk perspective, we can combine the information gleaned into a simplified capability description. A useful description provides an estimate of the difference (compared to doing nothing) the planned response will make in protecting critical assets.

This might seem an unusual approach to conceptualising capability, but it is useful as an exercise in shifting the way we

think about assessments from a focus on indicators to a focus on effects. Perhaps it's easier to embrace this way of thinking if we acknowledge that we cannot escape uncertainties. There is no one correct answer here. The relevance of a capability description is situational and relies on which uncertainties are included in particular response scenarios.

Once a capability description has been formulated, it can be evaluated against selected criteria to come up with a capability assessment.

Capability assessment and how is it useful

A capability assessment compares the estimated effect of an organisation's response against specific criteria that allow decision-makers to determine whether it is sufficient.

Two common types of criteria used to determine the threshold for acceptable losses/negative impacts against which a response is measured are rights-based criteria and utility-based criteria.

Rights-based criteria establish the minimum acceptable state (whatever this might be) for critical assets. If the effect of a planned response results in an impact that exceeds this threshold, response capability must be increased.

Example: Deaths per year from residential fires

From the point of view of a regional fire service, an example of a rights-based criterion might be the number of fatalities per year caused by residential fires. If the fire service determines that 1 fatality/year is acceptable, then a description that predicts a higher number would indicate the need for investment to increase capability.

Utility-based criteria look at the cost of an investment in capability and compare it to the magnitude of reduction in impact on critical assets that investment would create; if the cost cannot be justified (the investment does not result in a big enough reduction in the impact), the investment should not be made. If a choice must be made among several investments, the one that provides the "most bang for the buck" will be the winner.

Example: Cost-benefit analysis

Utility-based criteria often go hand in hand with a cost-benefit analysis used to justify investment. For example, the cost of investing in increasing the life-saving capability of the fire service would be compared with the value of the lives saved. All investments in which the benefit is greater than the cost should be made.

Part II:

Adapting Capability Assessments for Countering Information Influence Operations

Now that we have described how to formulate a response capability assessment that includes uncertainties, we will explore how these ideas can be applied to countering IIOs by considering *critical assets*, *response scenarios*, and *capability assessment* in this context.

Critical assets in the context of countering IIOs

An important insight from the new risk perspective is that the starting point for understanding an organisation's capability to counter an information influence operation must be identifying the critical assets we wish to protect. Let us consider a case in which these assets have been identified as democracy, freedom of speech, and national sovereignty. In contrast to the example of the residential fire, the assets in this case are abstract, intangible, and likely to be defined differently by different groups. Even so, it is only possible to assess response capability as sufficient or insufficient if we have a good working definition of these assets.

Governments and other organisations have experienced IIOs and already have some idea of the negative impact such attacks can have. One idea for getting started is to work backwards: consider the experience of information influence operations we and others have had, identify the negative consequences they produced, and then frame those consequences in terms of the asset or value threatened.

Creating response scenarios to inform capability description

Research has shown that providing evidence to support the reasoning behind an estimation of response effects (i.e., capability) results in a more accurate estimation of those effects and therefore a better assessment of response capability.

The development of one or multiple response scenarios, as illustrated in

Figure 5, is a good mechanism for providing necessary evidence. This is a non-trivial task requiring substantial effort with reference to written materials (e.g., scientific articles, reports, countering IIO handbooks) and interviews with subject-matter experts. Key questions to ask would be: 'What countermeasures are currently being used or could potentially be used to mitigate the impact of IIOs?' and 'How can the mitigating effects be described?'

A sensitivity analysis can then be performed to identify the most critical factors influencing the consequences of an IIO and the most effective countermeasures for inclusion in a response scenario that can be used to support effective decision-making.

Developing different response scenarios is also helpful for identifying uncertainties and unknowns. For example, you may know that a certain disinformation narrative is being spread by malicious actors, but not how that narrative is being disseminated. Is the disinformation simply being reposted by gullible citizens who happen to believe it, or are proxy actors working in an organised manner on behalf of a foreign power? In this example, the unknown is 'the actor/s behind dissemination'. If sensitivity analysis demonstrates that this unknown is a critical factor for mitigating the impact of the IIO, it should be included in the response scenario. Subsequently, two scenarios would be generated for analysis: Scenario 1) Unaware citizens are unintentionally spreading misinformation. Scenario 2) Hostile proxy actors are intentionally spreading disinformation. If we define 'classifying the actor/s behind dissemination' as a critical factor, this informs decision-makers that allocating resources to tasks related to addressing this factor is effective for mitigating negative outcomes.

An estimation of the difference in the effect between a response given the current resources and a response after allocating additional resources to tasks identified as critical will provide information on how much bang for the buck this investment might have.

One way to address the many uncertainties inherent in a potential response is to use multiple scenarios to illustrate what might happen. Again, imagining all potentially relevant uncertainties would result in countless scenarios to analyse. Sensitivity analysis allows analysts to determine which uncertainties have the greatest impact on effects and should be included in the model. Risk and threat assessments are examples of tools already being used to manage uncertainties in the field of IIO.

Developing an effective response could begin with creating an extensive list of counter measures and then ranking them subjectively according to effectiveness for a given IIO. *Figure 8* below provides three examples of how a response scenario for countering an IIO could be structured with varying levels of detail.

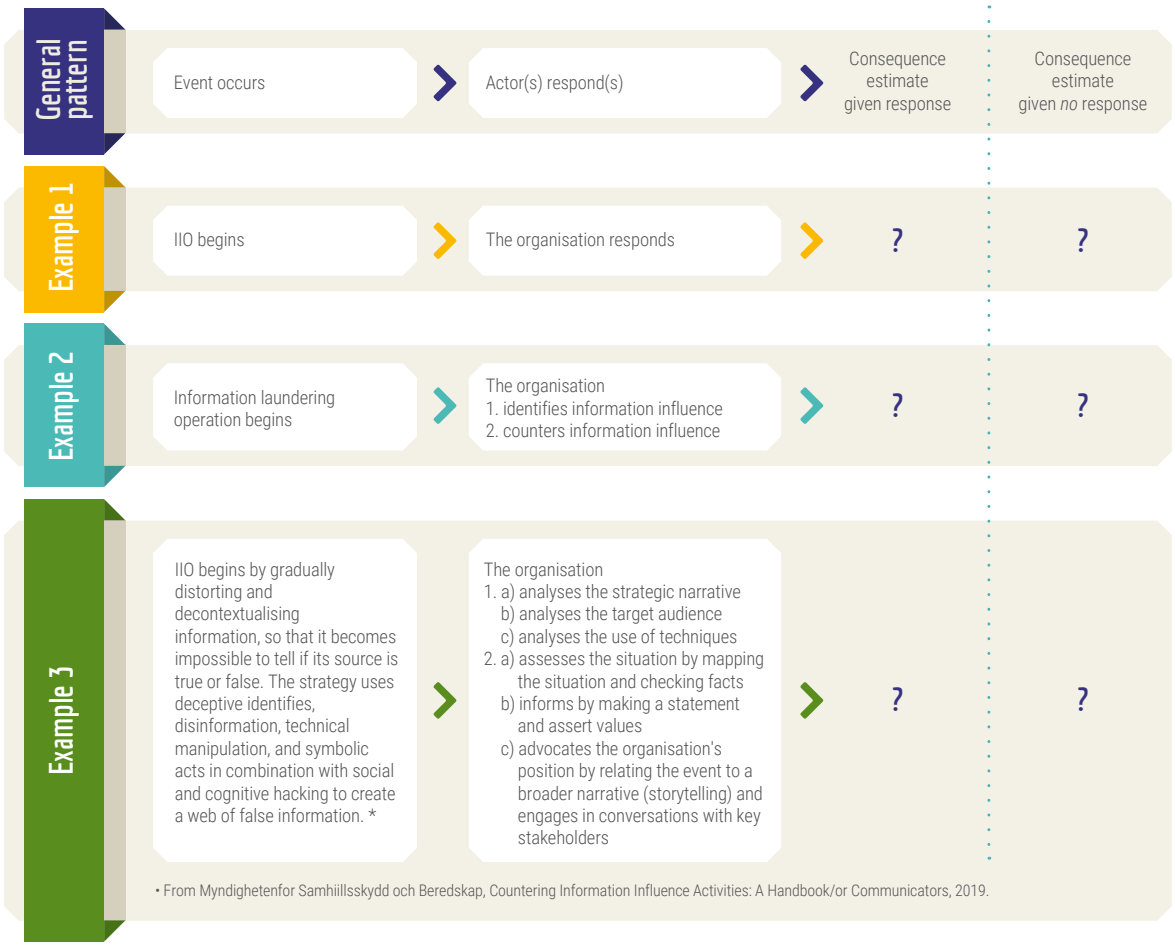

Figure 8. Examples of details that might be included in a response scenario for countering IIO

The examples given here are based on information drawn from *Countering Information Influence Activities: A Handbook for Communicators*.[11] The first response scenario includes only a few tasks, whereas the third is much more detailed. Just as in the residential fire example (see *Figure 4*), the level of detail necessary can be determined by applying sensitivity analysis to the available information.

Relevant questions for developing a response scenario might be: What markers can be used to identify an IIO? How quickly can we identify an IIO? When is speed of identification important? Can IIOs be categorised into types? Can target audiences be categorised into types? Which countermeasures are most appropriate for each type? What effect will countermeasure X have on the impact of the IIO?

The next step in refining a response scenario is describing the expected mitigating effect of the response. The development of response scenarios for countering IIOs would require substantial research, both to identify what is already known and to develop the new knowledge needed. This knowledge should likely be generated at a national or international level. Leading experts on countering IIOs could jointly

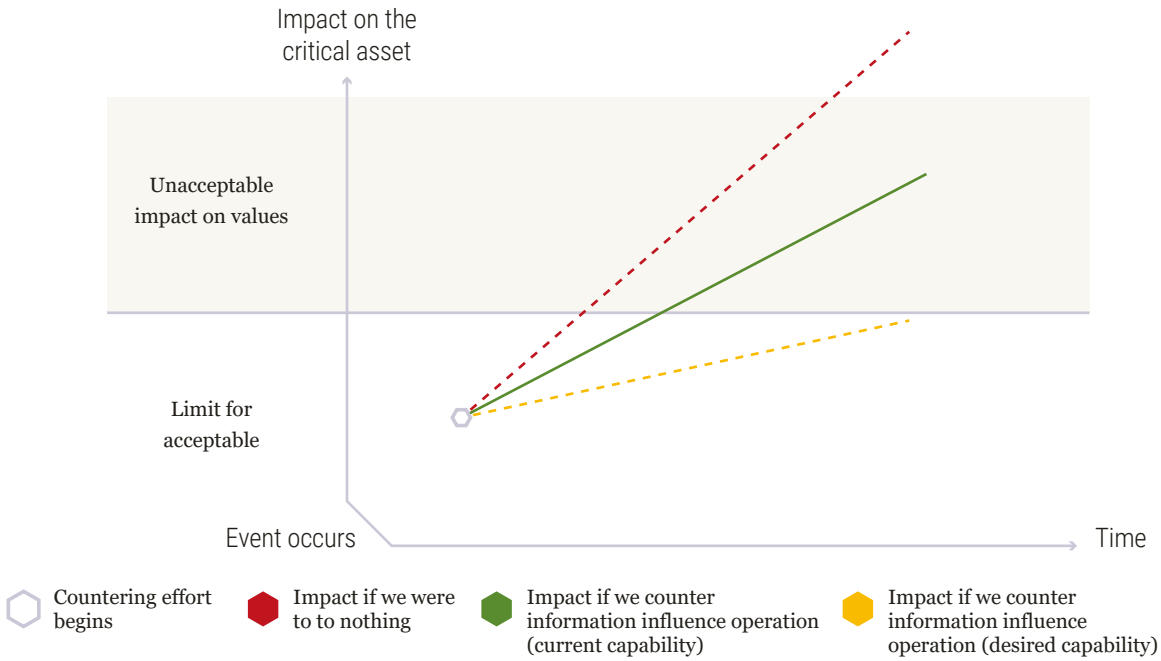

Figure 10. Evaluating an organisation's capability to counter an IIO

This diagram illustrates a threshold for an acceptable impact from an IIO attack on critical assets (blue line). Even if the current capability (black line) reduces the impact compared to doing nothing (grey line), the impact is still judged as unacceptable. In this scenario, response capability should be increased so the impact of an IIO does not exceed the limit of what is deemed acceptable (desired capability, brown line). This way of thinking about evaluation is in line with a rights-based perspective.

create a general response model (similar to Example 2 in *Figure 8*) and provide suggestions for what level of detail would be appropriate for case-specific response models (consider Example 3 in *Figure 8*). Guidance on what parameters to use to describe effects should also be developed.

The identification and definition of the critical assets to be protected from information influence operations, and the way in which we understand the impact of IIOs on those assets, can help us understand how best to assess response capability. If democracy is the critical asset we have determined to protect, at what level does it make sense to develop capability? Democracy is at work at local, regional, national, and international levels, and the impact of an IIO can be felt at any of these levels. This implies that it may become relevant for a local municipality to estimate the effects of their response efforts on the impact of an IIO in their jurisdiction. A response might also be a joint effort by multiple actors ranging from municipal-level communicators to national- and international-level decision-makers. For this we would need to develop multi-actor capability assessments: How can we estimate the individual efforts of

several responding actors and combine them into an aggregated estimate? The research on capability assessments from the new risk perspective is currently moving in this direction, but at present there are no guidelines for how to do this. However, the theoretical foundation of the new risk perspective holds promise for expanding research in this direction.

Assessing response capability for IIOs

Assessing response capability for IIOs means determining if current capability is sufficient as is, too high, or too low**,** as illustrated in *Figure 10*. Doing this in practice requires being able to say something about the magnitude of the difference between current capability and desired capability. Thus, before seeking to determine what is or is not acceptable in terms of IIO impact and response capability, there is a need to develop approaches to delineate purposeful descriptions of capability.

Using existing tools and guidelines for countering IIOs to guide the development of proactive *capability assessments*

Great efforts have been made to increase our knowledge and understanding of IIO and how to counter them. Guidelines and toolkits are available to support such activities, such as the "Resist 2: Counter-disinformation Toolkit"[12] and the "DIDI approach" to differentiate illegal IIOs from legitimate forms of influence.[13] While these tools focus primarily on what to do in response to an IIO, they can also support the development of proactive capability assessments helping answer key questions, such as: How good are we at recognising disinformation? How good are we at analysing the impact of IIO? How good are we at designing strategic communication responses?

The threat and risk assessments described in existing guidelines and toolkits can support the reduction of uncertainty regarding the impact of potential future IIOs and be used as a starting point for selecting which factors to include in a response scenario. An added benefit of detailed capability assessments is an explicit analysis of the effect of particular countermeasures on reducing the impact of an IIO.

Conclusion

This report introduces a model for creating response capability assessments for countering IIOs integrating the new risk perspective, in particular the research on capability and capability assessments. The starting point for this view is the strong focus on defining the critical assets that are threatened by IIOs. Instead of waiting to plan countermeasures for such operations by evaluating their final impact, response capability assessments enable practitioners to take a proactive approach to estimating their current response capability and assessing its mitigating effects. By implementing a system of estimation and assessment, measures can be taken proactively to increase response capability for IIOs, which in turn will decrease the impact of these events once they occur.

The research suggests that by developing response scenarios that estimate the difference in impact between doing nothing to counter an IIO, responding with current capability, and responding with increased capability, current response capability can be assessed as sufficient or insufficient, providing decision-makers with the information they need to justify allocating resources to increase (or decrease) capability.

Traditional indicators assess capability in terms of available resources. They are easy to explain but have limited usefulness for evaluating complex systems. They may contribute information useful for the initial planning stages by suggesting, for example, the need for response strategies and for education and training programs. However, traditional indicators are insufficient to inform the preparation of a dynamic, proactive response. The research on response capability assessment from the new risk perspective suggests that the way forward is to evaluate the effect of each response task in mitigating the negative outcome of adverse events on critical assets.

Glossary

Critical Assets [*skyddsvärde* in Swedish]: The tangible and intangible assets we wish to protect.

Adverse Event: An event is an incident that entails change in some condition or circumstance related to the critical assets. An *adverse event* is one that leads to negative consequences.

Risk: The uncertainty of adverse events occurring and uncertainty about the negative impact of such events.

Uncertainty: In the context of risk management, uncertainties are unknown, and sometimes unknowable, factors that influence adverse events, response capability, and the severity of the consequences. For example, we do not know if or when an adverse event will take place, or how severe the resulting damage might be. What we *can* do is to describe and analyse uncertainties to be able to act more purposefully despite what we don't know.

Consequences/Impact: The effect of an adverse event on critical assets. How an individual judges the severity of a particular set of consequences has both an objective and a subjective component.

Response Capability: The ability to mitigate the negative impact of an adverse event.

Effect: The result of the organisation's response on the consequences/impact.

Response Scenario: Certain events and circumstances that together describe a particular course of events. For the purposes of this article, a scenario begins with an "initiating event" and ends when it is possible to describe the "final outcome"—the consequences and their severity.

Critical Factor: A factor is a parameter whose associated value may be changed and influence the impact of an adverse event. A *critical factor* is one that has greater influence than other factors on the impact of an adverse event.

Sensitivity analysis: Sensitivity analysis identifies the most critical factors for inclusion in a response scenario by the systematic study of how much the variation and uncertainty surrounding a particular factor or assumption influences the final outcome of a scenario; in doing so, sensitivity analysis can suggest how the number of assumptions can be reduced without losing crucial information about possible variation in outcomes.

(Response) Capability Description: A qualitative and/or quantitative portrayal of capability, i.e., a structured capability description usually includes an explicit

statement describing the critical assets to be protected, a list of potential events/ scenarios that could have a negative impact on these assets, the potential response of one or several organisations to the event and its assumed effect on the impact, uncertainty and consequence representations, and the knowledge that the judgements are based on.

(Response) Capability Assessment: The process of comparing the potential effect of an organisation's response on the impact described in the capability description against specific criteria that allow decision-makers to determine whether it is fit for purpose (acceptable) and to prioritise its significance.

Rights-based criteria: To be able to assess capability, some type of basis for the assessment is needed, i.e., some kind of criterion for how to make comparisons. Rights-based criteria implies comparing the capability with some kind of limit of how low the capability may be. This means that boundaries have to be established and what applies if the boundaries are crossed.

Utility-based criteria: To be able to assess capability, some type of basis for the assessment is needed, i.e., some kind of criterion for how to make comparisons. Utility-based criteria depart from comparing alternative solutions and choosing the option that offers the greatest possible benefit. Utility is a concept used to weigh the pros and cons of a wide variety of aspects.

Endnotes

1 Information influence operations (IIOs) consist of a combination of various and multiple information influence activities. Such activities are "conducted by foreign powers to influence the perceptions, behaviour, and decisions of target groups to the benefit of foreign powers". Myndigheten för samhällsskydd och beredskap [The Swedish Civil Contingencies Agency] and Lund University, "Research Report: Countering Information Influence Activities: The State of the Art", 2018, p. 14.

2 Sean Aday, Māris Andžāns, Una Bērziņa-Čerenkova, Francesca Granelli, John-Paul Gravelines, Mils Hills, … Jonathan Terra, "Hybrid Threats: A Strategic Communications Perspective", 2019; Global Engagement Center (GEC), "GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem", 2020; Myndigheten för samhällsskydd och beredskap [The Swedish Civil Contingencies Agency], "Countering Information Influence Activities: A Handbook for Communicators", 2019; James Pamment, Howard Nothhaft, Henrik Twetman-Agardh and Alicia Fjällhed, "Research Report: Countering Information Influence Activities: The State of the Art (Version 1)" 2018; James Pamment, Henrik Twetman, Alicia Fjällhed, Howard Nothhaft, Helena Engelson and Emma Rönngren, "Resist: Counter-Disinformation Toolkit", 2019.

3 European Commission, "European Democracy Action Plan: Making EU Democracies Stronger", Press Release 3 December 2020; Christina Nemr and William Gangware, "Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age", 2019; Jen Weedon, William Nuland and Alex Stamos, "Information Operations and Facebook: Version 1.0", 2017.

4 Lowrance, W., 1976. Of Acceptable Risk – Science and the Determination of Safety. William Kaufmann Inc., Los Altos, CA.

5 Hanna Lindbom, "Improving Capability Assessments for Disaster Risk Management", (Doctoral thesis), Lund: Lund University, 2020.

6 Ibid.

7 Jean-Baptiste Jeangène Vilmer, "Effective State Practices Against Disinformation: Four Country Case Studies", 2021.

8 Hanna Lindbom, Henrik Tehler, Kerstin Eriksson and Terje Aven, "The Capability Concept - On How to Define and Describe Capability in Relation to Risk, Vulnerability and Resilience", Reliability Engineering and System Safety, 135 (2015): 45–54; Hanna Palmqvist, Henrik Tehler, and Waleed Shoaib, "How Is Capability Assessment Related to Risk Assessment? Evaluating Existing Research and Current Application from a Design Science Perspective", Proceedings of the Probabilistic Safety Assessment and Management (PSAM) 12 Conference (2014).

9 Marvin Rausand, "Risk Assessment: Theory, Methods, and Applications", Hoboken, N.J.: Wiley, 2011.

10 Roger Flage and Tore Askeland, "Assumptions in Quantitative Risk Assessments: When Explicit and When Tacit?", Reliability Engineering and System Safety, 197 (2020): 106799; Jahon Khorsandi and Terje Aven, "Incorporating Assumption Deviation Risk in Quantitative Risk Assessments: A Semi-quantitative Approach", Reliability Engineering and System Safety, 163 (2017): 22–32.

11 Myndigheten för samhällsskydd och beredskap [The Swedish Civil Contingencies Agency], Countering Information Influence Activities: A Handbook for Communicators, 2019.

12 James Pamment, "Resist 2: Counter-Disinformation Toolkit", 2021.

13 The DIDI approach analyses possible IIOs according to four factors—deception, intention, disruption, interference—to determine whether a coordinated attack is taking place and, if so, how best to counter it; for more information, see: Myndigheten för samhällsskydd och beredskap [The Swedish Civil Contingencies Agency] and Lund University, "Research Report: Countering Information Influence Activities: The State of the Art", 2018.

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.

Operating since 2014, we have carried out significant research enhancing NATO nations' situational awareness of the information environment and have contributed to exercises and trainings with subject matter expertise.

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