TOTAL WARNING

DOI: https://doi.org/ 10.37458/nstf.24.3.1

Giliam de Valk[*]

Abstract*:* It is explored[1] in what ways we can warn in order to protect our way of life and our critical infrastructures. From a methodological perspective, we could warn in four different ways. For to assess there is a threat, warning scenarios are composed for which critical indicators are developed. Subsequently, these critical indicators are monitored. It seems suited for a broad range of issues where access to information is limited. For to assess there is no threat, a barrier model can be constructed, focusing on critical chains of the process or production to be interrupted. It will lead to interventions for which politics must be willing to bear the costs. For to refute there is a threat, the adversaries modus operandi (AMO) are broken into visible activities during the preparation and execution of the hostile act. It is monitored though suspicious indicators, in which it is tried to refute that these indicators belong to a certain AMO. It seems suited to protect people and objects – like airports. For to refute there is no threat, the threat is broken down into its composing variables. For each variable, assumptions are formulated as if there is no threat. Subsequently, it is tried to falsify these assumptions. It seems suited for a wide range of issues, and can include both events and drivers in its analysis.

Keywords*:* critical infrastructure, early warning, threat, to assess a threat, to refute a threat, warning on events, warning on drivers

[*] In 2005, Giliam de Valk published his PhD on the quality intelligence analyses have to meet. He is specialized in the methodology of security and intelligence analysis. He has worked at the University of Amsterdam, the University of Utrecht, and the Netherlands Defense Academy where he coordinated and lectured a minor on intelligence studies. At the moment he is an assistant professor at the Institute for Security and Global Affairs, Leiden University. In 2021, he has won the Tudjman Scientific Excellence Award of the Zagreb Security Forum.

[1] The author thanks Ludo Block and Danny Pronk for their comments and suggestions.

Introduction

There are different types of early warning. There is, for example, the profiling on suspect behaviour at airports, or there is the monitoring of so-called warning scenarios. How can we warn, and how can we arrange these different types of warning?

In this article, it is explored in what ways we can warn in order to protect our way of life and our critical infrastructures. This is done from a methodological perspective. First, an arrangement is made by presenting four methodological approaches. Secondly, for each of these approaches it is explored what methods and techniques could be used. And finally, the applicability per type of warning is explored. This article is work in progress, therefore it is an explorative essay and not as the final answer.

Warning: four different methodological approaches

What is warning? Warning is a fundamental reason for intelligence activity. The aim is to prevent a threat from coming to fruition. We warn:

1. To provide early warning of potential threats of a developing situation.
2. To inform consumers (decision-makers) of future developments in time, in order to make decisions and to take actions.
3. To reduce the effects of adverse developments.
4. As put, first an arrangement is made from a methodological perspective. From a methodological point of view, we have different types of warning. Firstly, we can warn by to assess, or by to refute. Secondly, we may take the threat or the no-threat as the basic outcome. This way, we can compose a matrix with two axes, leading to four possible types of warning.
5. The first one is to assess there is a threat (top-left). The focus is on identifying indicators of that specific threat.

6. The second one is to assess there is no threat (top-right). The focus is on assessing that a crucial element of a threat to become to fruition is absent or neutralized.
7. The third one is to refute there is a threat (down-left). The focus is on to refute that identified indicators are related to that specific threat.
8. The fourth one is to refute there is no threat (down-right). The focus is on to refute 'no-threat' assumptions – based on the composing parts of a threat. If these assumptions cannot be refuted the threat is absent.

Table 1: Four types of warning: a methodological perspective

Concern Approach	**Threat**	**No Threat**
To Assess	*To assess there is a threat.* The focus is on identifying indicators of that specific threat	*To assess there is no threat.* The focus is on assessing that a crucial element of a threat to become to fruition is absent or has been neutralized.
To Refute	*To refute there is a threat.* The focus is on to refute that identified indicators are related to that specific threat	*To refute there is no threat.* The focus is on to refute 'no-threat' assumptions – based on the composing variables of a threat.

Other approaches may be possible, for example in the realm of quantitative methods and deep learning. In this article, we just explore these four qualitative approaches that are focused on causal relations – e.g. dealing with indicators, assumptions, and elements causing a threat.

The two top quadrants are aimed at assessing. If indicators are used, these are critical indicators. Critical indicators are meant to assess future events. If a critical indicator signals a threat, the steps to be taken are to warn and to act.

In the two quadrants down under, we refute. If indicators are used, these are suspicious indicators. Suspicious indicators are meant not to miss future events. Steps to be taken are:

1. To try to deny that the suspicious indicator is related to an adversaries modus operandi;
2. If denial is not possible, generally a technical investigation takes place;
3. If denial is still not possible: you warn or act.

The difference between a critical indicator and a suspicious indicator refers to a complete different methodological approach an outcome. In the case of a critical indicator, you try to reduce the value of the α – the chance that you incorrectly conclude that there is a significant relationship between phenomena. In short – you aim at assessing correctly that there is a threat.

In the case of a suspicious indicator, you try to reduce the β – the chance that you do not discover a relationship between phenomena. In short – you aim at not missing any potential threats.

These differences in approaches have effects on the type of outcomes each approach delivers, and by that the applicability and relevance of each approach. In the next session we will work out each quadrant with methods and techniques to make such a warning analysis.

Warning: methods and techniques per type of warning

The four methodological approaches will be worked out in research processes. Each research process will have its own emphasis and characteristics:

1. To assess there is a threat: the core emphasis is on developing critical indicators and to monitor their warning status.
2. To assess there is not a threat: the core emphasis is on the identification of the critical chain, and to assess if that critical chain – after our interventions – is now absent.

3. To refute there is a threat: for an external threat it is on predictive profiling and security question; for the internal threat is it on assessing and testing the vulnerabilities of an employee.
4. To refute there is not a threat: the threat is split up in its composing elements, and no-treat assumptions – to be refuted – are made for these composing elements.

Table 2: Four types of warning: methods and techniques per type of warning

Concern / Approach	**Threat**	**No Threat**
To Assess	Critical Indicators + Warning Status	Critical Chain Identification + To Assess Critical Chain is Absent
To Refute	*External*: Predictive Profiling + Security Questioning *Internal*: to refute the assessed vulnerabilities	To refute 'no-threat' assumptions that are based on composing elements of a threat

In this article, the purpose is not to make an inventory of all the different types of research processes that are possible. It is meant to give for each an example of a possible research process.

To Assess/Threat

In the approach of to assess a threat, the central items are warning scenarios, critical indicators and their warning status. First some *pro's* and *con's* are explained, then an overview is given of this research process.

Pro's and con's

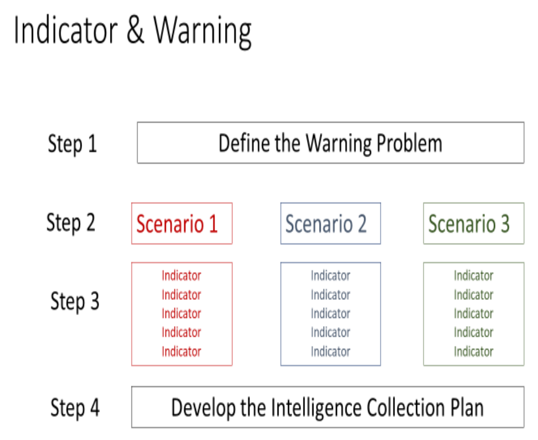
Pro's. It is a relatively easy method to learn at college level. The only challenging part from an intellectual perspective is the formulation of the right critical indicators – for which also thorough subject matter expertise is needed. If the critical indicators have been formulated, only on a limited number of items an intelligence collection plan has to be developed.

Con's. If the right warning scenarios – or the right critical indicators – have not been included, you may miss the threat. A compensation on this weakness can be the devil's advocacy role on the warning scenarios and critical indicators selected. Regularly the critical indicators need to be updated in order not to miss the threat.

An example of a method

A commonly used method to warn for a threat is the critical indicator approach (Grabo, 2004. Kriendler, 2006. NATO, 2001). Such methods are used by NATO, the UN, and corporate business. Here a general overview is presented, without choosing for a specific version. Often, it is represented as a four step – sometimes referred at as 'tiers' – system approach.

To assess a threat: a four-step system

Step 1. To establish the warning problem *Step 2*. To develop warning scenarios for that warning problem. *Step 3*. Per warning scenario: to determine the critical indicators; to put these critical indicators in a sequence of events; to assign an indicator status. *Step 4*. To develop an intelligence collection plan to monitor the status of the critical indicators.	 Indicator & Warning Step 1 Define the Warning Problem Step 2 Scenario 1 Scenario 2 Scenario 3 Step 3 Indicator Indicator Indicator Indicator Indicator / Indicator Indicator Indicator Indicator Indicator / Indicator Indicator Indicator Indicator Indicator Step 4 Develop the Intelligence Collection Plan

In the *Step 1,* the warning problem will be formulated. The next demands have to be met to define the warning problem rightly:

1. It must a clear, concise, statement focusing on single warning issue;
2. An interest must be formulated (choose the perspective of the threatened party);
3. An end state is presented that must be deterred.
4. The Warning Problem is composed of 5 W's, and nothing more than these five W's.
5. Who is the actor (state, non-state, regional, transnational);
6. What action is of concern for the intelligence consumer (war, humanitarian, instability, proliferation, terror, etc.);
7. When is this action to take place (near, mid, long term);
8. Where is this action likely to take place (internal, national, regional, transnational);
9. Why is this action taking place (… in order to [followed by threat]).

Example of a Warning Problem (fictional)

> "The Rockall Warning Problem is defined as the potential threat of regional instability caused by Dutch military activities in the mid-term to bring Rockall under *Dutch sovereignty* which could affect the interests of the United Kingdom"

In *Step 2,* the Warning Scenarios are developed. Practitioners often formulate three scenarios, including at least the most likely scenario and the most dangerous (worst case) one.[2] In all the approaches, the Warning Scenarios are composed of at least the next three elements:

1. Intentions: the actor's aims & objectives;
2. Capabilities: the actor's strengths & capabilities;
3. Activities: its practice & precedence.

The demands put to a warning scenario are:

1. Is it possible?

[2] If already a more broader scenario generation has been made, the selection can be made by carrying out an Analysis of Competing Hypotheses on these scenarios.

2. Does it represent a real end state?
3. Does it tie back to the warning problem?

Step 3 is the most critical step of the research process. It is the formulation of the critical indicators. Strict demands are put to the formulation of these indicators. The critical indicators are:

1. Collectable, early, distinctive, conditional, diagnostic, unambiguous, identifiable.
2. Limited in number (in most versions 6-10 critical indicators are advocated).
3. Truly critical turn points in the evolution of a situation.

Especially on the first aspect, different variations are circulating. If these are broken down into their composing parts, it leads to the next elements.

Composing elements of demands put to a Critical Indicator

Collectable: is your organization (country) actually capable of collecting this information through their sources?
Early: the predicted activity must be early to permit effective warning.
Distinctive: the indicator is only applicable to one scenario, not many scenarios.
Conditional: an indicator which is dependable – something that must occur or exist if the threat is to materialize.
Diagnostic: it leads the analyst to a certain scenario via a cause-and-effect reasoning – and thus the analyst should be able to make a decision on the indicator or come to a conclusion as to its meaning.
Unambiguous: the indicator points to one definite event only.
Identifiable: the indicator accurately identifies the activity which is taking place.

After the critical indicators have been formulated, some extra sub-steps are carried out:

1. Firstly, the analyst puts the critical indicators in a sequence of events – a timeline. It serves the insight in the

development of the threat. Sometimes, this timeline is split up in different phases.

2. Secondly, the analyst checks the critical indicators for their status. It is meant to assess how close we are to the end state of a specific scenario. It is presented by a color system, in which each color has its own symbol – in order to prevent confusion when a black-and-white copy is made.
3. Finally, a status is given to critical indicators. This can be presented in an assessment matrix, written text, or both.

In *Step 4* the intelligence collection plan is composed. Its purpose is to collect information to monitor the status of the critical indicators. It is analysed how the required intelligence can be obtained in an optimal way. To do so, the critical indicators are often broken down into requirements and priority requirements. The requirements are the composing parts of the indicator. The priority requirement is the element that is favourable to monitor as it meets the demands the best. Subsequently, the status of a critical indicator is then assessed through information collected on the priority requirement. Thus, with a minimum of collection effort, a maximum of assessing power is obtained.

Depending on both the warning problem and the organization involved, a report will be made for the consumer – either on a regular basis, or when the warning status has been changed drastically, or both.

To Assess/No Threat

In the approach of to assess there is not a threat, the central aspect is the so-called barrier-model. The idea is that a whole process can be neutralized by taking out a critical chain. The focus is on the identification of the critical chain, and to assess that this critical chain is absent. It results in the assessment that the threat has been neutralized. This is commonly referred to as a ‘negative’ warning. Often elaborate interventions are needed to reach such a result.

Pro’s and con’s

Pro’s. It is a relatively easy method to learn at college level. The method has a limited number of elements, and the analytical part can be carried out by a relatively small team with relatively a limited amount of data needed.

Con’s. Although the amount of data needed is limited, these data are often hard to collect, as in the case of secret nuclear sites. Also two models need to be mastered – both the barrier model (analysis) and the offensive counterintelligence model (operation). Furthermore, great costs and efforts can be involved in the executive part of the operation to reach the desired state – to take out the critical chain. Yet, the reward of a negative warning will be that the means can be used to deal with other threats. Finally, the method will only be successful if three conditions are met: a critical chain is present; the chain can be neutralized in actual practice; there is the political will to bear the costs of this approach – including its potential political fall-out.

An example of a method

In a process or a production line, a part of that process or production line may be so crucial, that – if it is taken out of it – the whole process comes to a halt. If this has been reached for an adversary’s process or production line, a negative warning can be given. In the Netherlands, within Dutch policing circles a method has been developed for this type of neutralization – the so-called it the barrier model. First, this barrier model will be explained, then a method is presented to give a negative warning – meaning: to assess there is no threat.

Barrier model

In 1993, the Dutch criminologist Cyrille Fijnaut tried to introduce a model of how to disrupt a (criminal) process or production. His aim was to erect barriers for organized crime (Lam, 2018). In the barrier model, the analyst assesses all the steps or phases that a process or a production line must go through. If one of these is taken out of it, the end result will not be reached. In this, there are some similarities with the Goal Tree.[3] An important difference with the Goal Tree is that in the barrier model every phase is sub-divided into four elements – the occasion, the signals, the facilitators, and the barriers. For every element, it is analysed of what it is composed of in that specific phase. With the sub-division of these four elements, a process or production line is represented in a form of a fixed business process. All the steps or phases that must be followed, are mapped this way. And also, at every step, an inventory will be made of overt or covert actors and activities (Gestel, 2014). This way, in the barrier model the processes and production are analysed, and are mapped together with the actors involved in these steps. The barrier model gives a detailed picture of the structure behind a certain process or production. It is richer and knows more finesses than the Goal Tree.

After the analytic part, there is the phase of the operation. The operation aims at neutralization of the adversary's end goal – what aspects need to be neutralized to prevent the adversary reaches the end goal – both as long as possible and as effective as possible. The operation is a three phased process, composed of identification, penetration, and neutralization[4] of the adversary's process or production line. The barrier model is a help to find targets or markets for the identification and penetration phase. It can be used to direct the creation of undercover agents. Furthermore, it identifies the most vulnerable parts of the process or production line.

If the neutralization is carried out successfully, a negative warning can be given. The most well-known example of a negative warning was given after the sabotage of the Norwegian Vemork heavy water installation in the Second World War. Nazi-Germany was working on a nuclear device. One of the crucial phases

[3] The Goal Tree is based on logic. It is an analysis of all the necessary conditions to reach a goal. This may refer to a (strategic) aim or the successful conclusion of a project (Hohmann, 2022).

[4] This main structure shows resemblance with offensive counterintelligence, but the factual input is provided by the information of the barrier model.

was the production of heavy water.[5] A negative warning could be given after the Norwegian heavy water production operation was knocked out, since this prevented the Nazi's from completing their vital experiments (Jones, 1962).

Method[6]

As put, this approach is based on the assumption that some chains in the process or production line are so critical that if they are taken out, the whole process will come to a hold. What is done is to analyze which steps – chains – are so critical for the process that neutralizing it will lead to a standstill of the whole process or production line. Generally, this will be a chain which is based on a] scarcity, and b] in which no alternative option for that chain is present. The more alternative options are possible, the bigger the effort will be to neutralize that chain, and the easier the adversary will find alternatives. In short, we look for scarcity and lack of alternatives of the opponent.

After interventions from our side, it needs to be assessed if that chain is indeed neutralized. If so, it also needs to be assessed 1] how long, and 2] under which circumstances, this neutralization will remain intact. Only then a negative warning can be given.

Steps of the method

1. Identification:

    a. Mapping process or production line for aspects as the occasions, the signals, the facilitators and, finally, the barriers (see next figure);

    b. Assessing the most vulnerable phases in that process or production line;

    c. For the selected elements of that phase: to map the actors involved (both overt and covert actors; legal and illegal facilitators), including their eventual specialism or unique skills, and to take out those that are not replaceable;

[5] Dideuteriumoxide (D2O or H2O).

[6] This text is largely inspired by CCV, 2022; Guijt, yr75; Kiemel, 2007; Sieber, 1993.

d. To identify object and actors to neutralize a phase in the model.

2. Infiltration:

a. General analysis to get access to the identified phase: three gates (digital, human, physical);

b. To select infiltration points (inventory of offensive counter-intelligence points). It can be that for this an additional social network analysis of the target needs to be made.

3. Neutralization, barrier neutralizes the adversary's end goal:

a. Object: objects are taken out of production line or production process;

b. Person: targets are neutralized.

4. Assessment:

a. To assess if that phase is indeed neutralized;

b. To assess for how long it will be neutralized;

c. To assess under which circumstances this neutralization will remain intact;

d. To present a negative warning – including the elements 4a, 4b, and 4c.

Detail step 1a: Each phase of the process or production line is sub-divided into four elements

Occasions	Elements that facilitates to carry out the process or production line, e.g.: • safehouses and anonymous sites, • access to countries/areas where the actors can move freely and anonymously.
Signals	Although it is carried out in a hidden way, aspects will always be visible, e.g.: • unaccountable absence/travelling, • a-typical informal networks (traffic analysis).

Facilitators	(Un-)conscious support by third parties with products or services to facilitate the process or production line, e.g.: • safehouses (conscious). • companies delivering dual use goods (unconscious).
Barriers	The toolkit of the parties involved to counter the adversary's activities, e.g.: • front stores, working under deep covers, etc. • all the Int's (as technint, finint, imint, geoint, sigint, socmint, humint), law enforcement and resilience enhancive measure (e.g.: awareness for companies producing dual purpose goods)

Often, for our consumer, this model is presented in a figure. Horizontally, all the different phases are listed that are needed by the adversary to reach the end goal. Vertically each phase is worked out for the following elements (top-down): phase of the process or production process; legal facilitators; identified barriers; illegal facilitators; aspects of their acting/role; our partners in stopping the adversary; aspects of our partners blocking potential of this specific phase.

To Refute/Threat

The approach of to refute a threat will be worked out for both the external and insider threat. In the approach of the external threat, the central items are identifying the adversary's method of operation, or adversaries modus operandi (AMO's), formulating suspicious indicators, to try to refute that the suspicious indicator is linked to the AMO, and red teaming to map possible new AMO's. In the approach of the insider threat, the central items are to assess vulnerabilities, and to test the employee on those identified vulnerabilities.

For the external threat, predictive profiling and security questioning will be explained. For the insider threat, during employment screening will be worked out.

External threat

To refute that there is an external threat, will, from a methodological approach, be carried out by a combination of techniques. Firstly, it can be done perpetrator related, in which the AMO's of the actor are broken down into its composing parts. These composing parts are then provided with suspicious indicators. When a security officer notices such a suspicious indicator, (s)he will try to refute that this indicator can be linked to the AMO. This approach is known as predictive profiling and security questioning. The unknown information has to be unveiled by the known method. Methodological, this is a known (method) – unknown (data) (Valk, 2020).

Secondly, the own vulnerabilities are tested. A Red Team will carry out an authorized attack on the own organization to see if new AMO's can be identified. In this approach the open experiment (= method) is crucial, and also the data (= new AMO's) that will be derived from that are still unknown. Methodological, this is an unknown (method = open experiment) – unknown (data).

Pro's and con's

Pro's. It is a relatively easy method to learn at junior college level. It makes the work of a security officer more challenging and therefore more interesting. You change from a reactive to a proactive approach, and try already to neutralize the threat in the preparatory phase. The marking is easy – there is a threat, or there is no threat. It is widely adaptable – for criminal, terrorist, and intelligence activities.

Con's. You need to update the inventory of your AMO's by Red Teaming. If Red Team experiments are limited to just test the security officers – or if these are limited in scope by the management – you will miss new AMO's.

Method for an outsider threat[7]

In predictive profiling a threat assessment is carried out for a person, object, or situation. It is done by assessing if suspicious indicators are related to an Adversaries Modus Operandi (AMO). Predictive profiling is composed of three elements:

1. The adversary and its possible AMO's are central in the process.
2. To prevent incidents before these take place.
3. A focus on the motivation and intentions of the adversary, instead of looking for the means (capabilities).

Often it is presented as a six phased cycle – starting and ending with red teaming. Red teaming is meant to identify the possible threats. The authorized attacks on the own organization are meant to assess if the identified AMO's are realistic and effective. It is not focused on the execution, but on the preparation. The idea is that the chance to be discovered is in the early stages of the preparation, because the adversary is then still in the dark of the norm that have to be met to operate under the radar. The whole method is based on the principle of monitoring deviations from the norm that may be linked to an AMO.

To identify signals of early preparation of an AMO, a model is made. This model is called the criminal, terrorist, or intelligence planning cycle – depending on its actual use. It is composed of eight phases:

1. Marking of the target

<u>2. Intelligence Gathering</u>

<u>3. Surveillance</u>

4. Planning

5. Tooling Up

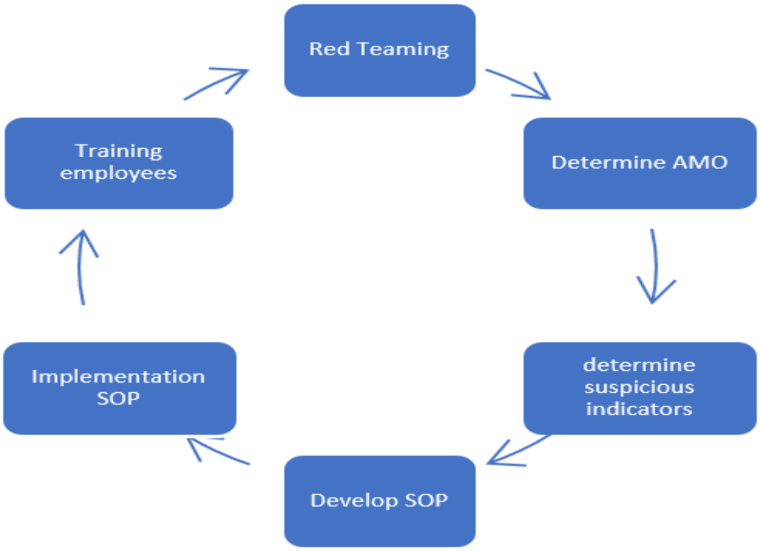
[7] Although nowadays a lot is written on predictive profiling, one of the first organization to lecture on this method was Chameleon Associates.

6. Rehearsing (including dry run) and Training

7. Execution

8. Getaway

Figure 1: Six steps to implement predictive profiling



Phase 2, 3, 6, 7 are the most difficult for an adversary, in the sense that (s)he can be monitored by the profiler most easily. Especially for these phases, suspicious indicators are developed – what is a deviation of the norm that possible can be linked to a certain AMO. For every AMO – and all its phases – this is worked out in a set of suspicious indicators to be observed on our side. Practical experience shows that if you prepare for terrorist AMO’s, most criminal AMO’s will also be covered.

The subsequent operational profiling process is as follows:

1. Detect suspicious indicators and/or deviation from the norm.
2. Link the suspicious indicator(s) and/or deviation of the norm to an AMO.
3. Try to refute the AMO (security questioning).
4. Give a classification.

5. Determine the level of control based upon the classification.

By trying to refute that the suspicious indicator can be linked to the AMO – step c of the operational profiling process – use is made of security questioning. The aim of security questioning is to try to refute the threat. If there is another explanation for the suspicious indicator, the threat is refuted.

Security questioning is an effective deterrence because it is the only time and place where the adversary is put on the defensive. Throughout the preparation the adversary is on the offensive, but when questioned the roles of defender and attacker switch.

If a suspicious indicator cannot be refuted, the employee reports this – including the AMO involved. This is the articulation of the threat. For a profiler a threat is continuous and immediate, and (s)he needs to act according to the established SOP.

As red teaming is meant to discover new AMO's. But it will also be used to assess if:

1. New or existing AMO's can be carried out successfully.
2. Employees are capable to identify suspicious indicators.
3. Employees are capable to link the suspicious indicators to an AMO.
4. Employees have a correct follow-up by security questioning and their SOP.

Insider threat

For the insider threat, the method for during-employment screening will be worked out. From research it is shown that cases of crossing to the dark side are unique, and the possible scenarios are too manifold. Also, an estimated 75% of the offenders have shown to have been actually bona fide at the original pre-employment screening (Valk, 2019). Just having pre-employment screening may therefore be too limited. Therefore, test will be carried out concerning the vulnerabilities of the insider – the employee.

Pro's and con's

Pro's. It is an effective method in the sense that an employee with bad intentions is on the defense. It is flexible, and therefore applicable for unique cases in a changing world. You will miss less than in the case of a pre-employment screening – as 75% was still bona fide during the pre-employment screening. You can diversify your organization more, including employees with a vulnerable background.

Con's. The skills of the interviewer are crucial. A lot of experience needed. It is demanding, especially if an interview takes 10 hours or more. Acceptance of this approach is not widespread in western countries (issue of legal incitement).

Method for an insider threat

During-employment screening is a three phased screening process. The first two phases are pre-employment, the third phase is during employment (Valk, 2019).

Three phases of during-employment screening:

Phase 1: A conversation between the candidate and the interviewer of at least 10 hours. The interview starts with how the candidate would describe him/herself. It includes going back in time in the life of the candidate, including the early 3-7 years. Going back so far in time gives an idea how the candidate's primary reactions are. At least 10 hours interview means also building rapport, which makes it easier for the interviewer to notice when the candidate deviates from its pattern.

Phase 2: The interviewer and the candidate – together – assess the vulnerabilities of the candidate. This may apply to the candidate itself (e.g. personality), or its surroundings (e.g. criminal family member). The interviewer and the candidate make a plan how to deal with these vulnerabilities.

Phase 3: This is the during-employment phase. Now the candidate can be tested – during its entire career at that organization –

on its vulnerabilities. The candidate – then employee – needs to report any incident that occurs in this field. By reporting, the employee refutes that his/her vulnerability is a threat. If the employee does not report such an incident, (s)he will be removed from the job.

To Refute/No Threat

In the approach of to refute a threat, the central items are to determine the variables of that threat, and to formulate assumptions in a way that there is no threat. You formulate the assumptions for each specific variable. Subsequently, you try to refute these assumptions.

Pro's and con's

Pro's. It can process a broad spectrum of warning issues – including warning on phenomena. The approach is primarily aimed at not missing variables of a threat, and thus likely to result in a very low beta.[8]

Con's. It is a more challenging approach in terms of to decide to include what variables. It can lead to a lot of variables compared to the limited number of critical indicators in the case of to assess a threat. A larger collection effort may therefore be needed.

An example of a method

In this approach, a warning issue can be varying from a person, a group, an object, a situation, up to a phenomenon. An approach if this type can be, for example,[9] based on the next steps.

1. Define the warning issue.
2. Formulate hypotheses.
3. Determine the variables of each hypothesis.
4. Formulate assumptions – for each of the variables – in a way that there is no threat.

[8] The β is the chance that you do not discover a weak, but actual existing, relationship between phenomena.

[9] A different arrangement of steps is possible. Also the following up after the fifth step is not presented. To illustrate the approach in its methodological purity, only the first five are presented.

5. Try to refute the assumptions (ICP).

Step 1. Define the warning issue

If you would take the earlier Warning Problem as a starting point, you may proceed as follows. Firstly, you may copy the original (and fictional) warning problem from there 'The Rockall Warning Problem is defined as the potential threat of regional instability caused by Dutch military activities in the mid-term to bring Rockall under Dutch sovereignty which could affect the interests of the United Kingdom.

Step 2. To formulate the hypotheses, as if there is no threat

For all the probable and possible options ('scenarios'), you formulate these as if there is no threat. In order to identify all the relevant options, the analyst can make use of hypothesis generating techniques as Starbursting, Quadrant Crunching, Analysis of Competing Hypotheses, and/or Red Teaming – depending on the nature of the warning issue (Heuer, 2011).

Assume that in the case of Rockall, the Netherlands could choose between three options: a naval blockade, a smaller specialized invasion, or a protracted guerrilla style approach. For all the probable and possible scenarios, you reformulate these as if there is no threat. In this example, you would formulate these as:

1. There will not be a naval blockade.
2. There will not be a smaller specialized invasion.
3. There will not be a protracted guerrilla style approach.

Step 3. To determine the variables of each hypothesis

Break down each hypothesis into variables for all of its applicable elements. This can be based on ICA/R, DIMEFIL/PMESII (Diplomatic, Information, Military, Economic, Financial, Intelligence, Law Enforcement/ Political, Military, Economic, Social, Information, Infrastructure) or a comparable applicable arrangement. For an ICA/R approach, that would be:

1. Intentions: the opponent's aims and objectives (I).
2. Capabilities: the opponent's strengths and capabilities (C).
3. Activities: the opponent's practice and precedence (A).
4. Resilience: our own composing elements of resilience (R).

The analyst may take into account specific variables within the ICA/R. The variables used may, for example, include:

- Actors involved; nature of the threat; location of possible targets; timeframe, assessment of potential impact; and assessment on the probability of occurrence.

- Depending on the issue at hand, you may consider also: past operational practices; means, opportunities & motive; doctrine & theory, legislative actions – including acquisitions; political climate – internal/external; civil stability factors; social/ethnic/religious/tribal factors.

Step 4. Formulate assumptions – for each of the variables – in a way that there is no threat

Formulate for each variable all relevant assumptions, and by that, covering the full scope of that specific variable. Formulate the assumptions in such a way that there is NOT a threat.

To break down a variable of step 3 in its composing elements, a system analysis can be a help – for example through a causal loop diagram. As horizon scans – with its system analysis – often precedes the warning problem in terms of sequence of analysis, such a causal loop may already be present. A causal loop diagram not only will give a more detailed insight in the composing elements, but also in potential cause-and-effect relationships – which will be of a help in formulating the assumptions.

If one of the drivers of the Dutch government could have been to create an external conflict to deflect the public attention from its domestic problems, then for this specific variable, the next assumptions could have been formulated:

Variable:	*Assumptions for this variable*:
The cabinet (doesn’t) want(s) to deflect internal problems	• There are no internal notes on creating external issues • There are no public claims/provocations in the media concerning Rockall • The cabinet is addressing home issues

For each variable, assumptions are formulated this way. It will result in a (relatively long) lists of assumptions. The assumptions are always formulated such that they deny there is a threat.

The assumptions are formulated in a SMART (specific, measurable, achievable, realistic, timely) way. The third assumption – ‘the cabinet is addressing home issues’ – is somewhat vague. What is enough to call it addressing home issues so there is no deflection of internal problems? It looks attractive to state that, as a way out, a SMART approach is needed – meaning to make the assumption specific, measurable, achievable (= here: collectable), realistic, timely. But to break down this assumption, it is most likely that also a system analysis is needed (causal loop diagram). A system analysis seems to be a promising tool for this fourth step in order to get an underpinned SMART formulation.

Step 5. Try to refute the assumptions (ICP)

An intelligence collection plan (ICP) is made to collect the data needed to try to refute each one of the assumptions. In the example of step 4, the first two assumptions are quite straightforward in terms of what to look for (e.g. internal notes, public statements, etc.). The third one has to be refined in order to make a collection effort more focused.

For a large part of the assumptions it is straightforward to assemble the elements for the ICP. As put, however, it is often needed to get a good picture of the underlying composing parts/drivers that have to be measured.

After the data is obtained from the ICP, it is assessed what this means for the threat level of that specific assumption. This part of the analysis – the assessing part – has not been worked out here. It also partly depends on the nature of the issue.

Summary of the four approaches

All the four approaches can be worked out in a method. All the approaches have a different chain of steps, with different composing elements and different emphasis along the process. In short: there is a wide diversity in its methodology. As this is an exploratory article, it must be stated that these methods are presented without having the pretention to cover all options, or that these are not open to improvement.

Having so much different chains of steps, two questions seems to be logic to reflect on. Firstly, which approach is the most relevant, or most relevant in certain circumstances? Secondly, what is the information input that you likely need for such an approach? These questions will be reflected on in the next session.

Warning: applicability per type of warning

In this paragraph, it is explored under what circumstances certain methods may work well. Firstly, this will be related to the information position. To illustrate the information position, different approaches can be used. Here it is chosen for the ICA-approach. A threat (T) can then be described as the combination of intentions (I), capabilities (C), and activities (A), reduced by the resilience (R) on our side:

$$\boxed{T = \frac{I \text{ x } C \text{ x } A}{R}}$$

Thus we have four composing elements of a threat: intentions, capabilities, activities, and our own resilience.[10] It will be explored what coverage is needed for a certain approach.

Secondly, the accessibility of information, there is also the type of issue that is likely to be dealt with by a certain approach – as a certain person, a production, a process, a case, or a phenomenon.

Thirdly, a warning analysis can be based on events or on drivers. If it is based on events, the actionable outcome will likely result in an intervention. If it is based on drivers, the actionable outcome will be used in policy making (compare Menkveld, 2021). It is assessed if a certain approach is events and/or driver based. In the following, we will explore these three aspects.

To Assess/Threat

Type of issue: case, phenomenon.

Information position:

- Main focus: ICA;
- Aspects: visible preparation, working up process;
- Condition: information collection is limited (e.g. limited access abroad).

This method works well for cases and big issues in which the information coverage is not optimal. Generally, this will be on foreign threats. Still, these threats can be serious with a high impact. It is looked for telling, early, and collectable data that assesses the threat. The analysis is based on events – critical indicators – and is aimed at to intervene.

To Assess/No Threat

Type of issue: production, process.

[10] It is not meant as a mathematical formula, but as a quick overview of the kind of relationship of the four composing elements.

Information position:

• Main focus: C(A);

• Aspects: identification of barriers;

• Condition: A critical chain is present (physical and/or human); the chain can be neutralized in actual practice; there is the political will to bear the costs of this approach.

This approach is likely to be relevant for cases that are a direct threat to the survival of a nation, or involve unreplaceable persons in society (like a king). In these cases, a lot of resources of the state will be put into neutralizing the threat. An example is to neutralize a critical chain in a WMD-programs of a hostile countries. Not only the facilities can be attacked, but also the persons involved.

This approach does not exclude other applications as well. Especially if there is a weak link in a very annoying production line/process, and the societal costs of breaking this link are not too high. An example of low societal costs is to neutralize the production of TATP, by controlling the distribution of peroxides.

The analysis will be based on events – critical chains– and is aimed at to intervene against objects and persons.

To Refute/Threat

Type of issue: people, individual.

Information position:

• Main focus: I(C)A. You monitor the activity, and then you try to refute the intention;

• Aspects: AMO’s to be broken down into visible activities of preparation and execution;

• Condition: It is possible to refute through human interaction (security questioning).

Outsider Threat

As the insider threat is just on screening a person, only the outsider threat will be dealt with. The outsider threat approach of predictive profiling is aimed at protecting humans and physical objects – including stand-alone computer systems.[11] It works well if through Red Teaming all the probable and possible AMO's are identified. The breaking down of these AMO's into observable suspicious indicators is mainly aimed at activities. The subsequent security questioning is aimed at to refute the intention. Often, if the biggest threat has been analysed, minor threats are also covered. By that, it provides a coverage for a large range of activities. It requires a relatively small collection in the protective rings around the persons/object to be protected.

The analysis is based on events – suspicious indicators – and is aimed at to intervene.

To Refute/No Threat

Type of issue: case, phenomenon.

Information position:

• Main focus: ICA/R + drivers;

• Aspects: generic; events and drivers

• Condition: information collection is near optimal on all composing parts of the threat. You must be able to monitor a broad variety of variables.

A good information position is needed resulting in a large collection effort. You must be able to monitor a broad variety of variables. It is likely to be adapted for domestic security – for the protection of the own society – because you are then in that more advantageous information position. Although it is not necessarily limited to the domestic domain if the stakes are high enough.

[11] For the logic gate, the kill chain can be used.

This fourth approach is the most encompassing option. It not only includes all the elements of a threat (IxCxA)/R, but you can also include drivers that are broken down into assumptions to be monitored. It is an approach in which you can steer developments both by interventions (event-based) and by policy making (driver-based). For a methodological perspective, this is a preferred approach. Successful intervention is easier to measure than driver-based policy making – although the latter one is better from the perception of prevention. It requires a certain mindset at a political level to appreciate this broader range of instruments.

Conclusion

The preliminary findings are that, for all approaches, methods can be constructed. These methods can be applied in a specific context for a certain information position. At least at an analytic level, they are realistic to execute. This way this exploratory research wanted to contribute to an arrangement and overview of different approaches of warning, without having the pretention to be complete in its methods possible.

For *to assess there is a threat*, warning scenarios are composed for which critical indicators are developed. Subsequently, these critical indicators are monitored. It seems suited for a broad range of issues where access to information can be limited and the collection effort must be focused.

For *to assess there is no threat*, a barrier model can be constructed, focusing on critical chains to interrupt the process or production. It seems suited for issues where the stakes are extremely high – as in the case of an opponent's WMD program – and politics is willing to bear the costs of any fall-out caused by the neutralizing measures.

For *to refute there is a threat*, the adversaries modus operandi (AMO) are broken into visible activities during the preparation and execution of the hostile act. It is monitored though suspicious indicators, in which it is tried to refute that these indicators belong to a certain AMO. It seems suited to protect people and objects – like airports.

For *to refute there is no threat*, the threat is broken down into its composing variables. For each variable, assumptions are formulated as if there is no threat. Subsequently, it is tried to falsify these assumptions. It seems suited for a wide range of issues, and can include both events and drivers in its analysis. Because of these drivers – and contrary to the other three approaches – not only interventions can be carried out, but also policy making can be implemented.

If we look at the four different types of warning, especially the fourth method – to refute there is no threat – has the capability to produce a warning based on both events and drivers. This is not only an analytical advantage, but in the case of a warning it allows options ranging from interventions to policy actions.

Secondly, it also implies that the events and drivers can be tested against each other. For example, by ACH – in which the events are filled out in the place of the evidence (vertically), and the drivers in the place of the hypotheses (horizontally). This way it can be used as a tool for deception detection by looking at incongruities. If there is an inconsistency found, a deception evaluation is made on that event and driver. As events are more prone to deception than drivers, the fourth approach will be more robust in this sense.

However, if this fourth approach of to refute there is no threat is carried out without any subsequent assessing elements, the false positive rates will be exceptionally high. Therefore, this approach is likely to be followed up by assessing elements.

If the elements on applicability are put in a matrix, we get the next summary.

Applicability per type of warning

Concern Approach	**Threat**	**No Threat**
To Assess	*Case, phenomenon* Main focus: ICA . Aspects: Visible preparation/ working up process. Condition: Information collection is limited.	*Production, process* Main focus: C(A). Aspects: identification of barriers. Condition: A critical chain is present. A broken critical chain leads to a de-warning
To Refute	*People, individual* Main focus: I(C)A. Aspects: MO's can be broken down into visible activities of preparation and execution. Condition: It is possible to refute through human interaction.	*Phenomenon/case* Main focus: ICA/R + drivers. Aspects: generic, events and drivers. Condition: Information collection is optimal on all composing parts of the threat.

Literature:

1. CCV, Project: mobiel banditisme. June 2022. https://hetccv.nl/themas/georganiseerde-criminaliteit-en-ondermijning/mobiele-bendes/ visited March 2022.

2. Gestel, B. van, Facilitering van mobiele bendes. Research Synthese. WODC, Cahier 2014-17.

3. Grabo, Cynthia, Anticipating Surprise: Analysis for Strategic Warning, Lanham, University Press of America, 2004.

4. Guijt, Linda & Sven van Schaik, De fenomeenmethode: een handvat voor probleem georiënteerd politiewerk. Het Tijdschrift voor de Politie, year75/nr.1/13, 25-29.

5. Heuer, Richards J. & Randolph H. Pherson, Structured Analytic Techniques for Intelligence Analysis. Washington, DC: CQ Press, 2011.

6. Hohmann, Christian, Goal Tree: http://christian.hohmann.free.fr/index.php/thinking-processes/249-goal-tree , visited March 2022.

7. Jones, Reginald Victor, “Scientific Intelligence,” CIA, Studies in Intelligence. National Archives (Washington D.C.): Records of the CIA : RG 263; declassified NND 947003, Summer 1962, 76.

8. Kiemel, J., & ten Kate, W., De programmatische aanpak van mensenhandel en mensensmokkel: Een verkenning aan de hand van Sneep. Justitiële verkenningen, 2007, 5(7), 8.

9. Kriendler, John, NATO intelligence and Early Warning, Conflict Studies Research Centre, Special Series 06/13, March 2006.

10. Lam, Jerôme, Ronald van der Wal, Nicolien Kop, Sluipend gif. Een onderzoek naar ondermijnende criminaliteit. Boom Criminologie, 2018.

11. Menkveld, Christiaan, Understanding the complexity of intelligence problems. Intelligence and National Security, 2021, DOI: 10.1080/02684527.2021.1881865.

12. NATO, Generic Early Warning Handbook, EAPC(COEC)D(2001)2, 30 October 2001.

13. Sieber, Irich & Marion Bögel, Der Logistik der Organisierten Kriminalität, 1993. Logistik der organisierten Kriminalität: wirtschaftswissenschaftlicher Forschungsansatz und Pilotstudie zur internationalen Kfz-Verschiebung, zur Ausbeutung von Prostitution, zum Menschenhandel und zum illegalen Glücksspiel. Bundeskriminalamt, 1993.

14. Valk, Giliam de, ‘On Screening and the Insider Threat – A Methodological Exploration’, National Security and the Future, Volume 20, 1-2, 2019.

15. Valk, Giliam de & Onno Goldbach, Towards a robust β research design: on reasoning and different classes of unknowns, Journal of Intelligence History, 2020.