CASE STUDIES INTO THE UNKNOWN – LOGIC & TOOLING

Giliam DE VALK*

Abstract

Case study is the most common method in intelligence research. Intelligence analysis takes place in a context of denial and deception by opponents that also constantly innovate themselves. In that context, the analyst does not want to miss threats.

Can a research design on threats be structured such that less relevant relationships are missed? In methodological terms: to reduce the value of the β. A tool is presented in which different types of unknowns are distinguished, in which either the data or the technique to retrieve those data are unknown. In this tool – the Rumsfeld Matrix – both the quantitative and qualitative approach is integrated. Also, all three types of logic – abduction, deduction, and induction – can be applied. Thus, the change of missing relevant relationships on threats is reduced.

Next, a model is presented to assess what is covered in a case study in terms of logic. It is tool to organize and evaluate your case research. Through this Standard Logic Model it can be visualized what the current coverage of a case is, and what the desired state would look like. It is also assessed what techniques will cover what part of a case. It integrates three aspects. Firstly, all three forms of logic are included. Secondly, it combines both the qualitative and quantitative approach. Thirdly, analysis by humans and analysis by machines is combined. It will lead to an enhanced way of working – that of augmented analysis in which humans and machines are paired in their analytic effort.

Keywords: *β, unknown, tooling, Rumsfeld Matrix, logic.*

Introduction

In this article, it is dealt with case studies into the unknown. In the context of intelligence, dealing with the unknown tends to be more complex than in other disciplines as denial and deception are endemic.

* Assistant Professor Phd at the Institute for Security and Global Affairs, University of Leiden, email: g.g.de.valk@fgga.leidenuniv.nl

Also the nature of the threat will evolve as opponents are constantly innovating themselves.

How do you draft a case study in such a context? Firstly, a tool is presented that deals with different types of unknowns that have to be investigated. Secondly, another tool is presented to assess to what extent the complete picture of the case at hand – a so-called C-theory – has been covered, and to what extent it deals with possible future innovations by an opponent. Both aspects will be visualized in one scheme in which an ordinal – not absolute – impression is given of what has been covered.

The two tools are aimed to be of practical use for the intelligence practitioner. The practitioner can make assessments and design policies to cope with future developments. At an academic level, it points at methodological issues to be addressed. It can help to organize academic teaching and research around methodological issues and practices.

The focus is on threat related intelligence case research into the unknown. The tools will be illustrated with examples of preparing a Peace keeping Operation (PKO). But first, it will be dealt with some basic methodological insights.

Case-theory, α and β

Academics usually understand theory as a general or nomothetic theory. A phenomenon is explained in a general sense. This type of theory is referred to as a level-A theory (De Groot, 1981). Practitioners also develop a theory, but in the form of a level-B and level-C theory. The level-B theory is a problem oriented special theory, and limited to a certain category of cases. The level-C theory is developed for an individual case. This is also referred to as an idiom theory (Van Strien, 1986).

The level-C theory – or Casus-Theory – is used by intelligence practitioners to analyze a concrete case. It is aimed at actions concerning future situations, and not at scientific theory. It is primarily aimed at interventions – to achieve a situation that is believed to be the desired one. This is contrary to scientific research that is primarily aimed at truth finding. By that the object of intelligence research is more *mutandum* than *explanandum* (Van Strien, 1986).

But how do we use a C-theory in intelligence analysis? There are high quality publications on case-study research, as by Robert Yin (Yin, 1994), but they are not calibrated to the specific methodological needs of applied intelligence research. His publication is written for scientific purposes in order to explain. Intelligence is, however, in the first place aimed at not to miss threats. This is complex as denial and deception, and future innovations by an opponent are characteristic for this type of research. The aim of intelligence is to give warnings to avert a threat. This difference in setting and orientation leads to a different methodological approach of intelligence case research, compared to other methods.

To explain versus not miss are central in some basic methodological terminology. To explain is related to the α (and Type I error). Not to miss is related to the β (and Type II error). The α is the chance that you *incorrectly* conclude that there is a significant relationship between phenomena (a Type I error means accepting a hypothesis when in reality this hypothesis is false). The β is the chance that you *do not discover* a weak, but actual existing, relationship between phenomena (a Type II error consists of rejecting a 'true' hypothesis).

In academic research, the emphasis is on to reduce the α – the chance that you incorrectly conclude that there is a significant relationship between phenomena. In intelligence research, however, the emphasis is primarily on not to miss a threat – the β – the chance that you do not discover a weak, but actual existing, relationship between phenomena. To put it in plain language: in intelligence it is often more critical that you do not miss a threat (β orientated research), than that you scientifically prove or explain that a threat will occur (α orientated research). This calls for a research design, and the application of logic, methods and techniques, with respect to their β capabilities (De Valk, 2011).

Although the emphasis is on the β, the issue of the Type I error is not to be excluded from intelligence research. The intelligence equivalence of the Type I error is to err on the side of caution. For example, this implies overestimating the enemy's capabilities. Concerning the Type II error, scientists may ignore or discount the

significance of these errors in their studies. However, intelligence analysts do not have this luxury. Thus they are confronted by these two simultaneous pressures that require them to minimize both types of error simultaneously. Therefore, the calibration process of intelligence assessments is far more demanding than scientific calibration, and the likelihood of mistakes is higher (Goldbach, 2012). It calls for research design tools that are related to both errors – the α and the β.

Secrets, puzzles, and mysteries, and Structured Analytic Techniques

In intelligence, case studies will differ in complexity. The tools that will be presented in this article are meant for the more complex ones, that Treverton called puzzles and mysteries (Treverton, 2009). A problem with data in those complex case studies is that the noise can obscure the signal – including the issue of overfitting (Silver, 2012). The more complex a problem is, the less favorable will be the relationship between the data in terms of noise and signal (Menkveld, 2018). To reduce the change of biases in such situations – as for puzzles and mysteries – the analyst has to rely on tooling and multiple Structured Analytic Techniques, or SAT's (Moore, 2011. Menkveld, 2018). But how do you arrange your SAT's to assess as accurate as possible (to reduce the value of the α), and at the same time not to miss a threat (to reduce the value of the β)? First, it is dealt with the tooling to reduce the value of the β (Rumsfeld Matrix), and then the focus is on the overall research design in terms of logic (Standard Logic Schedule).

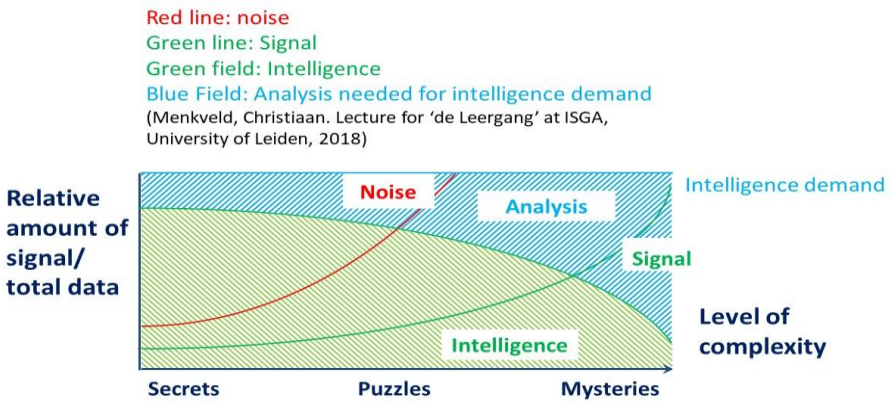

Figure 1: The relationship between the data in terms of noise and signal (Source: Menkveld, 2018)

Rumsfeld Matrix: How not to miss a threat?

There are no manuals on a β research design. Some publications concern β-aspects, for example when they deal with techniques as Quadrant Crunching, Red Team, Red Cell or Alternative Analysis (as in Heuer/Pherson, 2011; *Red Team Handbook*, 2012). However, the β research design itself remained a blind spot. In the Netherlands, some initiatives were taken by Onno Goldbach and Giliam de Valk to explore the possibilities of such a β research design. As a starting point a statement by Donald Rumsfeld was taken. In 2002, the then United States Secretary of Defense, Rumsfeld stated:

> [T]here are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – there are things we do not know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones (U.S. DoD, 2002).

A Rumsfeld Matrix derived from what he said that day, has been used more often. However, the Rumsfeld Matrix had never been used for a methodological arrangement of the β capabilities until 2013. The composition of such a β research design is since 2013 part of the Minor Intelligence Studies, first at the University of Amsterdam (Ad de Jonge Centre) and, since 2017, at the University of Leiden (ISGA). This subsection on the Rumsfeld Matrix is a reworked version of De Valk, 2018. Starting point was to distinguish between different types of unknowns – whether the way to *retrieve* data is known or not, and whether these *data* themselves are known or not. It leads to four combinations of *retrieval* and *data*. Each of those combinations is a quadrant of the matrix, and refers to a certain combination of elements that you may miss. Each quadrant covers a part of the puzzle of the [un-]known-[un-]known, and is part of the research design to reduce the value of the β as much as possible. If his statement is thus rearranged in a matrix, it results in the following composing elements of, for example, a Peace keeping Operation (PKO) mission (the mentioned techniques will be explained later in this article):

PKO	KNOWN	UNKNOWN
KNOWN	Critical Thinking	Early Warning & Critical Indicator Driver Based Scenario Building
UNKNOWN	Data Science Cell	Red Cell & Red Reaming

Figure 2: The Rumsfeld Matrix: data and retrieval
PKO arrangement for near term early warning and mid-term policy planning
(Source: The Rumsfeld Matrix is a reworked version of De Valk, 2018)

Known-Known

In the *Known-Known* quadrant, both the technique to obtain the data [*retrieval*] and the *data* are known. The known-known quadrant refers to the contents of assumptions, information, and knowledge of which we know that we know them. In general, this quadrant is about

challenging: are you really sure about what you think that you know, that you know?

For a PKO, for example, an *Early Warning and Critical Indicator (EWCI)* system is vital to warn on the near term. Within such an *Early Warning and Critical Indicator* system you need to check if the so-called Critical Indicators of a Warning Scenario are still accurate (*Known-Known*). The accuracy of a Critical Indicator is vital because it then will provide an accurate warning in case of threats (EAPC, 2001).

Known-Unknown

In the *Known-Unknown* quadrant, the technique of *retrieval* is known, but the *data* themselves are unknown. In a PKO, for example, you are aware that a threat is present, but the exact possible courses of action are unknown. In order not to miss threats, methods and techniques are used. In the context of a PKO, for example, *Driver Based Scenario Building (DBSB)* can be used for mid and long term policy planning. The likelihood of the different scenarios is monitored by collecting data for the indicators that are formulated for each scenario. The *data* are not available yet, but the technique of *retrieval* is known (scenario building, including the formulation of indicators).

Unknown-Known

In the *Unknown-Known* quadrant, the technique or algorithm to obtain data [*retrieval*] is unknown, but the *data* as such are present. It is about, for example, finding relevant correlations by big data-analyses. In intelligence, tooling is developed for, among others, data mining, criminal profiling, geographic profiling, spatial analysis, social network analysis, SOCMINT and GEOINT. The quantitative part can be automated in so-called Data Science Cells, who will play a major role in a PKO to get a grip on the developments.

Unknown-Unknown

In the *Unknown-Unknown* quadrant, both the technique to obtain data [*retrieval*] and the *data* are unknown. This is a difficult quadrant to deal with. Not only because it is hard to reflect on things you do not know of, but also because there are just a few techniques developed to

detect unknown-unknowns. These techniques mainly take the form of an experiment. In such an experiment a group of persons is asked to carry out an authorized attack on their own organization, to see if something is overlooked. Such an experiment is often referred to as Red Team or Red Cell. Red Teaming is not limited to the opponents' perspective, but can also include the broader scope of society itself, including secondary and tertiary effects (*Red Team Handbook*, 2012). Based on the results of Red Team and Red Cell experiments, security measures are taken. The outcome of a PKO Red Cell experiment can be that insurgents may, for example, adapt *satellite patrol* – in which this patrol intentionally separates itself visually and physically from the base unit of the patrol, outside the visual contact (*Urban Operations III*, 2016). It is effective to neutralize traditional road blocks and ambushes. Subsequently, these road blocks are to be organized in a different way, to cope with this new modus operandi.

Some last remarks on the Rumsfeld Matrix. Firstly, it is to be approached as a matrix, and not as a cycle, in the sense that techniques are not applied in a sequential, but in a parallel way. Only the inductive experiments of the unknown-unknown quadrant (Red Team/Red Cell), are to be executed *after* you have carried out your analysis for the other three quadrants. If not, you will infinitely carry out inductive experiments.

Secondly, if you start a new case, e.g. a new PKO, it is likely that your databases are not filled yet. The β gap will now be felt mostly. This may hamper the application of some of the tooling within the unknown-known quadrant, especially the ones that are based on quantitative (abductive) correlations (De Valk, 2018), as in Data Science Cells. As a result, the known-known quadrant then needs an extra emphasis to challenge causal connections made over data. This is needed, among others, because of the persistence of impressions based on already discredited evidence in the causal connection (Heuer, 1981).

Thirdly, for an optimal coverage, it is advised that in the overall matrix techniques are used from all three classes of reasoning – deduction, induction, and abduction (for an explanation, see the next heading). As every class of reasoning has biases and limitations, these are likely minimized by combining them. Only a combination of them

will reduce the number of relationships that otherwise would have been overlooked. Also, to compose the matrix, you do not need to limit yourself to one technique per quadrant.

To summarize, the Rumsfeld Matrix does not only deal with the four different types of unknowns, it also combines both qualitative (EWCI, DBSB) and quantitative aspects (Data Science Cells), and all three classes of reasoning. By this robust methodological approach, it is aimed at not to miss any relevant threat – to reduce the value of the β.

Standard Logic Model: Case-theory and future innovations

After presenting a tool on different combinations of unknowns, we now turn to a tool to assess what part of your case is covered, and to what extent you are prepared for future innovations by other parties in play. It refers to reducing both the α and β. In the tool, the different classes of reasoning – inductive, deductive and abductive – are arranged. This is done in an ordinal way, not an absolute one. However, before we can present the scheme, we first will have to discuss the three classes of reasoning, as they are defined for their effect on reducing the α, but hardly for their effect on reducing the β.

Different classes of reasoning

In the methodological literature, reasoning is defined for their effect on the α. Firstly, in deductive reasoning you argue from the general to the specific – a top-down approach. In a logic way, the conclusions are deductive of the premises presented. An argumentation is deductive, meaning that if the premises are correct, the conclusion therefore will inevitably also be correct. Secondly, there is inductive reasoning – the ex-consequentia reasoning. Here, a general rule – generalization – is made based upon a number of specific observations, experiments etc. These observations and experiments indicate that the premises of an inductive logical argument have some degree of support. It is a bottom-up approach. The conclusions that result from inductive reasoning – and in which the premises are true – *are likely* to be true, but also can be false. Thirdly, there is the inference to the best explanation (IBE), or abductive reasoning, in which an explanation is selected based upon likeliness. In abductive reasoning, it is assumed

that the most likely conclusion is the correct one. It is reasoning through successive approximation (Voulon, 2010).

As formulated above, the reasoning is on how to reach your conclusions and on the absoluteness of your claim (α). However, it is *not* on not to miss relationships (β). To be relevant to the β orientated intelligence research, reasoning needs to be reformulated, and calibrated from an α approach to a β approach. Yet, not only in general literature on methodology, even in intelligence handbooks reasoning is only presented and explained in the context of reducing the α, and not the β (De Groot, 1981; Grabo, 2002; Voulon, 2010). At the Ad de Jonge Centre, University of Amsterdam (UvA), *Red Team* and *Red Cell* experiments were carried out. In such experiments, the unknown-unknown is addressed, to reduce the residual threats. It deviates from the regular scientific experiments in which a hypothesis is tested – and, by that, is related to the α. During these β-related *Red Team* experiments, some insights were obtained on how reasoning may contribute to reduce the chance we miss a threat – i.e. to reduce the value of the β. Without claiming definitive conclusions, the UvA-experiments indicate some strong and weak points for their potential to reduce the value of the β. In a scheme, this can be summarized as follows (De Valk, 2018).

Logic and β?

Hardly developed: some Red Cell experiences

Logic	Strength	Weakness
Deduction	Fast, general inventory + directs research at residual threats.	Weak in making an inventory of a *deviation* from the general pattern. Hardly covers real innovations.
Induction	Maps innovations (new modus operandi). Aims at the unique + Verstehen.	Slow in making an inventory. Maps only a small part of the case (= C-theory).
Abduction	Big data (quantitative): generates many correlations, otherwise overlooked (additional hypotheses) + trends	Often lacks causality (limited relevance of many correlations). Limitations concerning the future (significant amount of data from past & present is needed).

Figure 3: Logic and β? (Source: De Valk, 2018)

Standard Logic Model

As every class of reasoning has biases and limitations, these are likely to be minimized by combining different classes of reasoning in a research. For an optimal reduction of the value of the α, it is therefore assumed that all different classes of reasoning have to be used. Concerning the reduction of the value of the β, the preliminary findings at the Ad de Jonge Centre points the unique weak and strong points for each type of reasoning. It also supports the assumption that it is advisable always to use all classes of reasoning in a threat related case study.

The next scheme is an ordinal presentation and not an absolute one. The reason is that it is work in progress, and not a fully developed model. It has been composed after testing and reflection of intelligence analysts on how logic contributes to a case-study. This is done for two aspects: firstly, to compose a C-theory (x-axis); and, secondly, to be prepared for future innovations by the parties involved (y-axis).

The three forms of logic are represented by a color: abductive (yellow), inductive (red), deductive (blue). Abductive reasoning (yellow) will be for a large part composed of finding quantitative correlations, as, for example, by Data Science Cells. To find a correlation, things must already have happened to some extent in the past. So, future innovations can be assessed, but only limited. That is why they are positioned at the bottom half. On the other hand, these big data will result in a large number of correlations, and therefore it covers a large area of the case.

In inductive reasoning (red) – by 'Verstehen' (Weber) as in, for example, Red Team – elements are less connected to the overall picture – the C-theory. That is why they are put on the left side. But they can prepare you for future innovations, even an opponent had not thought of yet. That is why they are listed at the top of the y-axis.

Finally, in deductive reasoning, inventories are made, for example, on possible futures. Afterwards, scenarios and indicators are composed to monitor what scenario eventually will be the most likely one. It covers all main likely futures and makes an inventory of the elements in play. It both contributes to the C-theory building and assessing future developments. Therefore, it is positioned right-top. It results in the next ordinal – not absolute – areas in the following scheme.

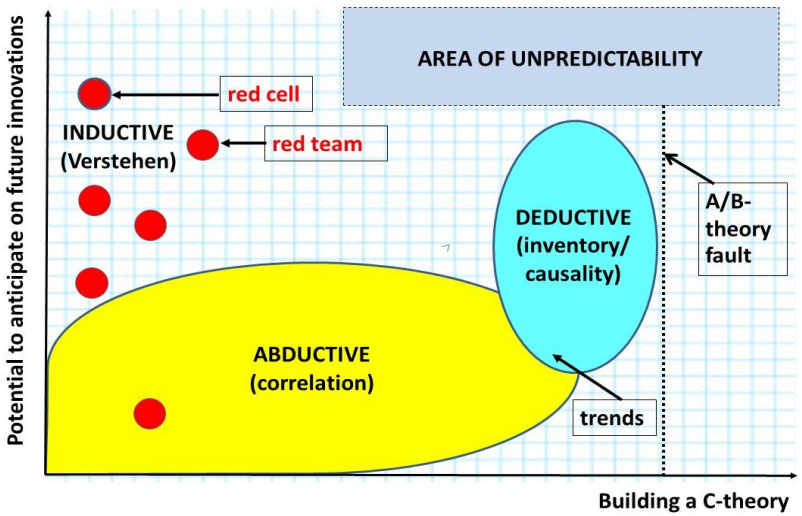

Figure 4: C-theory building (author's approach)

A methodological disclaimer needs to be made. In methodology, logic is mainly developed to apply A/B- theory to a case, less for logic *within* a C-theory, and not at all for the β. Right of the A/B-theory fault, the traditional α oriented insight of reasoning and logic is in place. The whole field left of this fault is nothing more than an ordinal representation. Yet, the relevance of the scheme is that we now can assess what we have covered of our case already, and where most likely our white spots are. Still, there will always remain an area of unpredictability (top-right).

The Standard Logic Model encompasses three elements. Firstly, it includes both the α and β aspects concerning the way correlations and causalities found (α), and of what you may have missed in the overall picture (β). Secondly, all three logic forms of logic are included. And finally, it encompasses both the qualitative and quantitative aspects of a research. All are represented in one overall scheme. In the next section, we will deal with a sub-optimal approach, and how you can develop it into a more optimal one. As put, this illustration will be on a PKO mission.

Standard Logic Model: SAT's and tooling

This section will start with a sub-optimal situation of an analysis. It will be illustrated how a more optimal situation can be reached. Actual methods will be presented.

A sub-optimal way of using logic in a case.

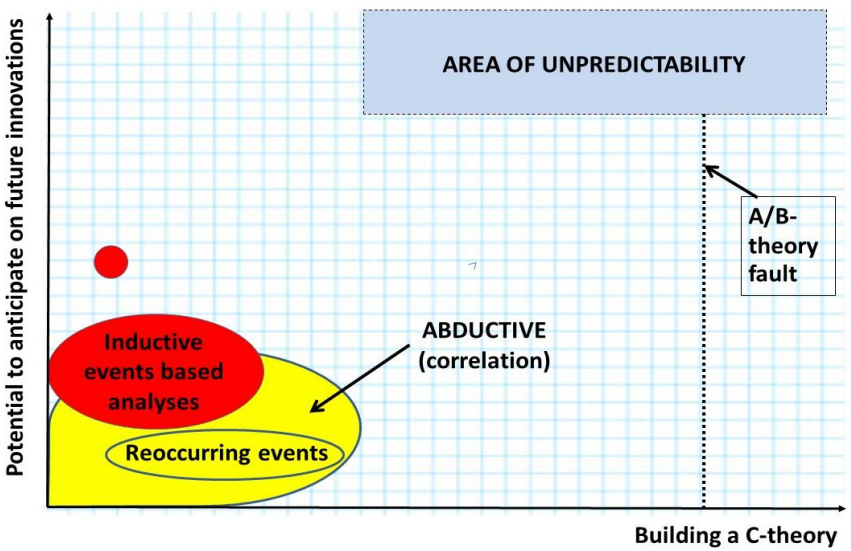

Figure 5: *A sub-optimal way of using logic in a case* (author's approach)

To what failures could this lead to? A simple illustration. Say, there is a new type of youth gang. After a certain time, the street violence diminishes, and the police make an inductive event based analysis only (scheme above). It concludes that there is less violence, so society has a lesser problem now. If a Driver Based Scenario Building had been carried out, it may have resulted in an opposite outcome. What were the drivers behind this 'appeasement', because not only the chapter in the capital, but *all* the chapters of this gang, including in the border area and the small harbors, suddenly committed no street

violence anymore? The main driver was that the gang became big in the international drug trade and did not want any unnecessary attention. The gang changed from petty crime to undermining or disruptive crime. As such, this calls for more police investigation instead of less, but it remains unveiled if you limit yourself to an event based analysis instead of a driver based one.

If you make, in a PKO, an inductive event based analysis, you will miss the deeper drivers of developments. It is exactly these drivers that yield the mid- and long-term insights. So, the policy planning will be hampered and the PKO will be less prepared on the mid- and long-term. But also, the potential of near term warning will be limited. Grabo's ground breaking research on failures of sub-optimal analysis led to the development of an elaborate early warning and critical indicator approach (EAPC, 2001). Furthermore, computer systems need to be filled with data to provide automated alerting on those critical indicators. Finally, as Red Team/Red Cell is absent, the analytical unit will be unable to reflect accurately on possible new modus operandi by the other parties. Thus, it cannot be anticipated on them. In the next sub-section, it will be – step by step – explained how this gap can be filled by SAT's and tooling, so that a case-theory can be build that includes future developments also.

(Sets of) techniques and Structured Analytic Techniques (SAT's)

How can you transform the presented suboptimal situation, into a more optimal one? The presented approach is based on inductive events analysis. Furthermore, this PKO makes scenarios for reoccurring events, as, for example, annual clashes between farmers and cattle keepers (scheme above). Yet, no elaborate scenarios should be building, but these events should be mitigated for their impact only. Scenario building in case of reoccurring events is a waste of energy and resources of the analyzing unit. How could you improve the presented situation? The following suggestions are meant as an illustration only, to show how the Standard Logic Model can be a steering instrument for, for example, the planning of your training and education. For an elaborate explanation of most of the following techniques, see Heuer/Pherson, 2011.

A first set of techniques is needed for your policy planning on the mid- and long-term. You want to know in what different ways the situation may develop, and then formulate for each of those options a policy to cope with it, so you are prepared to act if it occurs. A set of techniques could be a Driver Based Scenario Building approach. It is composed of two columns. The left column is to generate hypotheses and to test them for the data (events) available. The right column is to analyze on a deeper level the drivers that drive the events and pattern of events. This can be done, for example, by assessing the drivers on actors through a Strength Weakness Opportunity and Threat (SWOT) analysis, and assessing the drivers on factors through a Causal Loop Diagram. Subsequently, the drivers with the highest impact and highest uncertainty are selected as the axes that are the basis to build the scenarios on – together with wild cards and trends. Finally, all these scenarios will be the input for the hypotheses (x-axis) of Analysis of Competing Hypotheses (ACH), and the data of the event column will be the input of the evidence (y-axis) of ACH. Thus, the factual observed events are tested against the deeper level of analysis (drivers), and vice versa. It has the potential to reveal yet undisclosed deception within the realm of the events (the 'evidence' of ACH), and vice versa. This way of scenario building was experimented with in 2018 in the Minor Intelligence Studies at ISGA, University of Leiden.

This approach results in an inventory of all main courses of action possible (β), but also assesses what the most likely ones are, including by assessing the speed and direction in which drivers will develop (α). In the techniques, all classes of logic are used at some point of the process. As you cover all the main options, you are working on your C-theory. As it is on the mid- and long-term, it will be somewhere middle/top. Therefore, this set of techniques will be situated somewhere at the right-middle/top of the Standard Logic Model.

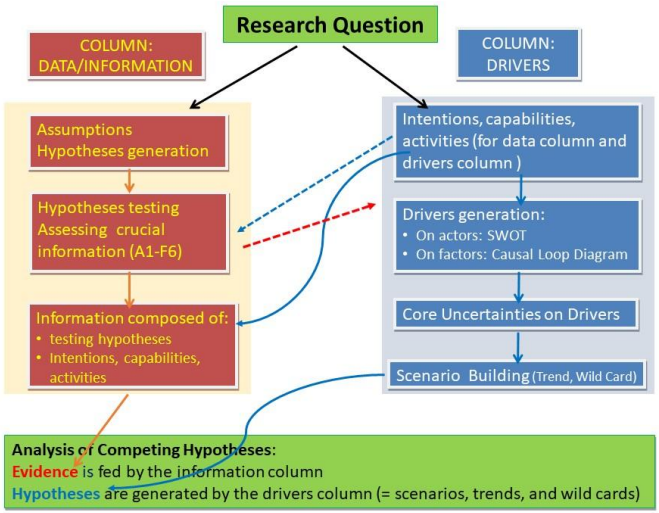

Figure 6: Standard Logic Model (author's approach)

Secondly, besides a policy planning on the mid- and long-term, you also want to act on the near term when a threat actually occurs. If possible as early as possible. Based on the work of Grabo (Grabo, 2004), a set of techniques has been developed to warn as early as possible by monitoring so-called critical indicators (EAPC, 2001). Such a research starts with formulation of a *Warning Problem*. Then *Warning Scenarios* are developed for the possible outcomes of this specific *Warning Problem*. For each scenario, a set of *Critical Indicators* is developed that is unique for that specific scenario only. Finally, an *Intelligence Collection Plan* is made to monitor the development of these indicators. When an indicator changes from normal (green) to, for example, an extreme state (red), the analyst decides if a warning is needed. The warning process needs to be supported by good data management and preferably by an automated alerting on the *Critical Indicators* if the status of an indicator changes.

It results in an inventory of the scenarios to warn for on the near term. All main scenarios to warn for are covered (β), and the Critical Indicators tell if a specific scenario actually will occur (α). As it is on the more specific warning issue, it will contribute less to the C-theory than

Driver Based Scenario Building (middle-right). It is also on the near term, instead of on the mid- and long-term, therefore it is situated around the middle of the y-axis. So, this set of techniques will be situated somewhere at the middle-right of the Standard Logic Model.

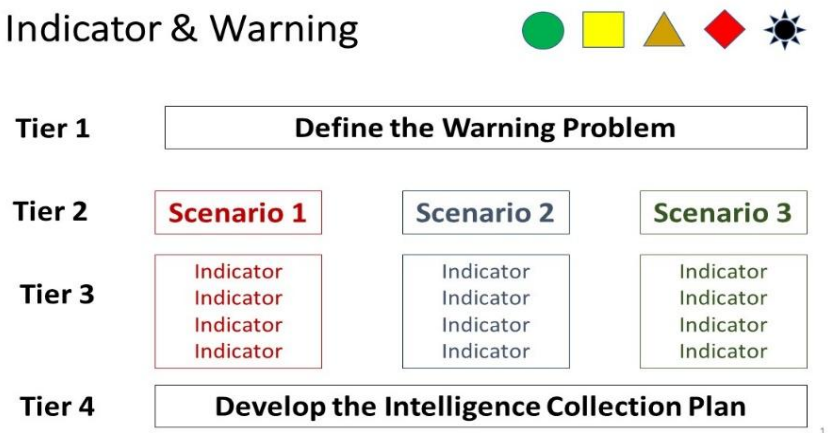

Figure 7: Driver Based Scenario Building (author's approach)

A third set of techniques is Red Team/Red Cell. It is an experiment in which – through inductive reasoning ('Verstehen') – it is assessed, for example, what new modus operandi may be developed by another party that has not been used yet. It deals with the unknown-unknown (β). These experiments are hardly connected to the overall picture – the C-theory. Therefore they are situated at the left. But they can prepare you for future innovations, even this other party itself has not thought of them yet. That is why they are listed at the top of the y-axis. As they are relatively isolated experiments, they will only cover a small part of the total picture (red dots).

A fourth group deals with the quantitative approach. We live in a time of information overflow and need to process enormous amount of data that can never be processed in that quantity by humans. Furthermore, often real time intelligence is needed (by machines), instead of close to real time (by analysts). Machine Analysis plays a

central role here. It can be organized in a so-called Data Science Cell. Different aspects of Machine Analysis can take place, as shown in the scheme below. In the scheme RGAP stands for Research Guided Action Planning. The way machines reason, learn, and analyze, is presented in the next scheme (De Valk, 2019a).

Machine learning will be often based on a more abductive way of reasoning. It will yield enormous amount of correlation (large area of coverage, α). Correlations that would not have been included if only humans were looking for them (β). The results are not always connected to the C-theory (from left to right). As the data must be in the system – have taken place in a significant manner – the future orientation will be limited (bottom-to middle), although it will, for example, generate a lot of trends. That is why it is situated as the big yellow area at the lower half of the model.

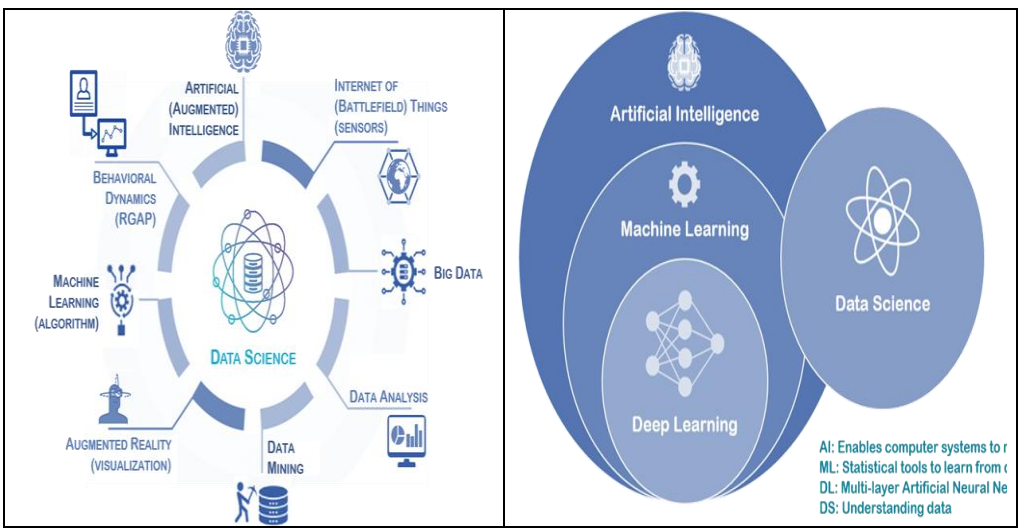

Figure 8: The way machines reason, learn, and analyze
(Source: De Valk, 2019a)

If we put all the techniques and tooling in place, it will result in the next scheme. The different element will support each other. A Data Science Cell, including the input from criminal profiling, geographic

profiling, spatial analysis, social network analysis, SOCMINT and GEOINT, will be used, for example, to compose, to refine, and to assess the scenarios. It will also lead to a better source management by a more optimal assessment of the reliability of the source (A-F), and the credibility of the information (1-6) (*AJP 2.0*, 2002).

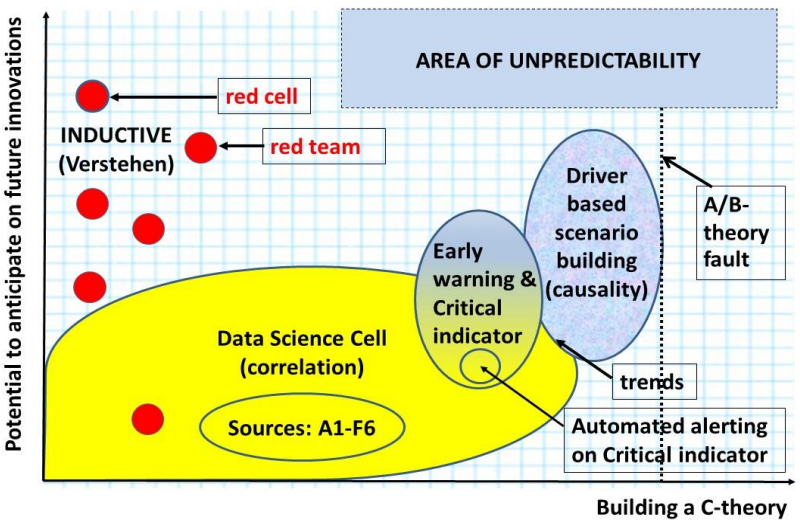

Figure 9: C-theory building (author's approach)

The aim was to illustrate, how the Standard Logic Model can help both to plan (what you need) and to evaluate (what you may have missed) your intelligence process. It can be used as a planning instrument for your training and education program. It also indicates that the combination of human and machine analysis will result in a more genuine threat intelligence (Pace, 2018). This way, it can contribute to the so-called Augmented Intelligence in which humans and machines are paired in their analytic effort (Sabhikhi, 2017).

The incomplete practice – the case of positive vetting

Another illustration would be if we are confronted with a situation in which you never will reach an optimal combination of

techniques – as in the PKO example – because the files are not kept, the options are too divers, and the incidents too unique to formulate scenarios for. Can the Standard Logic Model still provide insight to evolve to a more optimal situation? An illustration is presented for positive vetting. HRM officials do not like disclosure on this sensitive issue, so data are presented in an anonymous and abstract way.

Let's assume, we have the next system of positive vetting in place. Firstly, it is assessed if the candidate does not pose a risk by its personality or by being potentially subject of black mail. Secondly, it is assessed if the candidate is not part of a vulnerable environment. Apart from extensive file checks, it is also composed of an extended interview of several hours by two persons – one to interview, and one to observe. In the whole vetting process it is tried to assess that the candidate cannot be black mailed (alcohol, drugs, sex, money, past, etc.), and hasn't had an extremist or violent history. The emphasis is on information of 16+ years of the candidate. Also, it is tried to assess that there are no vulnerabilities in the environment of the candidate, as extremists, criminals, or visits of and influencing by suspect countries. The approach is to assess. To asses implies it is mainly an α oriented approach.

What is the problem in this setting? HRM officials do not like disclosure, so colleagues cannot learn from incidents. Furthermore, a different culture is needed, especially at the HRM office. Often, HRM steers on mistakes, and is not a safety net for people that have (personal) problems. The effect is that the person in question, in case he/she is vulnerable (e.g. a life changing event), will not contact HRM for help. Colleagues will hardly have incentives to report on suspect indicators. And superiors hardly will keep files. This applies to many Dutch organizations. It results in a too little & too late situation (Houtzager, 2018).

A complicating factor is that there is no typical profile of someone taking the wrong turn. Actually, in reconstructions, about 75% had no problems when he/she accepted the job. There are some weak correlations – having an open ended contract, working more than 10 years at the same organization, experiencing a life changing event, and having a Narcissistic personality are overrepresented. But the

correlations are far too weak to compose scenarios for in which indicators are developed that will be monitored. The picture of offenders is too divers (De Valk, 2019b).

As data are simply absent, it is hard to rely on big data correlations. So the yellow field of quantitative abductive correlations will be limited, even close to absent (yellow: bottom half). Offenders and incidents being too unique will make it hard to compose scenarios for (blue-red: middle-top, right). As a result, it is hard to develop a system of critical indicators, even more so as colleagues hardly have incentives to report, and superiors hardly will keep files (blue-yellow: middle, right). It ends up as the following situation for the Standard Logic Model:

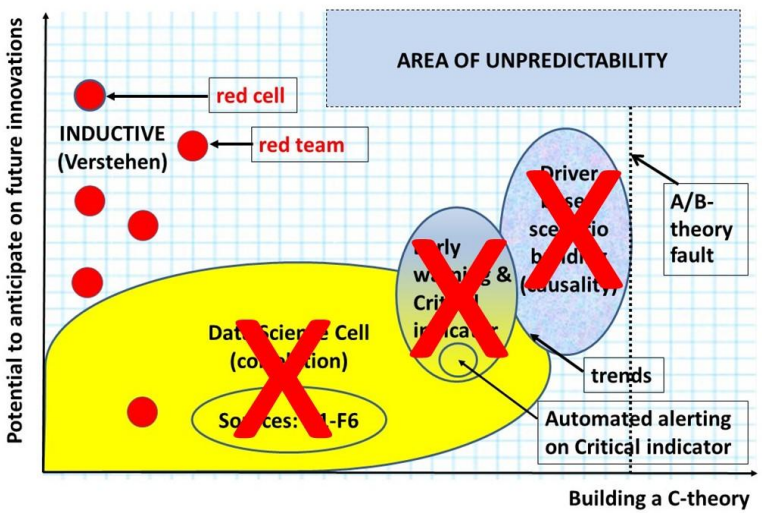

Figure 10: C-theory building (author's approach)

What is left in the original scheme are the red dots at the left. It is on experiments on eventual undisclosed weaknesses. If that was to be included into the vetting process, it would result in an on-the-job testing of the integrity of an employee. The vetting system would then shift from a pre-employment into an in-employment or during-

employment approach. It would lead to some adaptions compared to the original approach. The employee can now be tested on its vulnerabilities. It could be represented as three phased strategy to *deny* that the candidate is a *threat*. It starts with a long interview, preferably by one person to build up report. The interviewer will ask the candidate to describe him/herself nowadays, and then go back in time, finally with also a focus on 3-7 years old – to assess more primal reaction patterns of the candidate. Then they, together, assess the candidate's vulnerabilities, and develop a plan to cope with these vulnerabilities. Finally, the candidate will be tested – Red Teamed – during his/her entire career on these vulnerabilities. The approach will shift from an α (to assess) into a β (to test in order to deny that there is a threat) approach.

The second illustration indicates that the Standard Logic Model can provide a methodological underpinned improvement for an imperfect situation as well. Knowing this, the Standard Logic Model could also be used the other way round. For example, in a state on state situation, an opponent does not employ elaborate 'Verstehen' experiments (Red Teams, wolf packs with a free role to monitor the movements of an opponent etc.) for its defensive counterintelligence. You then only have to analyze its counterintelligence SOP's to create your red carpet into that country. The Standard Logic Model can serve different functions – how to design your analysis in an optimal situation (PKO), how to improve it in an imperfect situation (positive vetting), and how to analyze weaknesses to attack the opponent (counterintelligence).

Reasoning and the Rumsfeld Matrix

After the illustrations of the Standard Logic Model, we now return to the Rumsfeld Matrix. Some quadrants of the Rumsfeld Matrix seems to prefer certain classes of reasoning, although other classes of reasoning are not excluded completely. The unknown-unknown quadrant will almost exclusively rely on inductive reasoning, since Red Team/Red Cell has a 'Verstehen' approach, and takes place in the setting of a β *experiment* (De Valk, 2012). The unknown-known quadrant will be dominated by abductive reasoning (big data), but

inductive reasoning will be present, as in statistical syllogism (a syllogism – Greek for conclusion or inference – is a logical argument in which a conclusion is based on two or more propositions that are asserted or assumed to be true; unlike many other forms of syllogism, a statistical syllogism is inductive). In the known-known quadrant, abductive reasoning will play a main role in belief revision – to take into account a new piece of information. In the known-unknown quadrant, all three types may be present. The type of logic largely depends on the technique chosen. Deductive techniques of this quadrant will be of help to get fast, general, inventory, in order to look for the residual threats to be addressed.

The difference between the Rumsfeld Matrix and the Standard Logic Model is that in the Rumsfeld Matrix the different types of *unknown* are addressed by selecting analytical *techniques*. In the Standard Logic Model, it is shown how the different *classes of logic* interact, and how they, together, *compose* the future oriented *C-theory*. The two tools – the Rumsfeld Matrix and the Standard Logic Model – are complementary in designing a threat related, future oriented, C-theory.

Conclusion

Intelligence analysis takes place in a context of deception and denial, in which opponents constantly innovate themselves. In that context, you don't want to miss threats. A research design tool is needed to cope with the unknown, or, in methodological terms, to reduce the value of the β. The presented tool, the Rumsfeld Matrix, can help to identify different types of unknowns in which data or technique/tooling is missing. In this Rumsfeld Matrix, both the quantitative and qualitative approach is integrated. Also, all three types of logic can be applied. Thus, the change of missing relevant relationships on threats is reduced.

Next, the Standard Logic Model assesses to what extent a case study has been covered in terms of logic. Abduction, as it is implemented now in quantitative analysis, is good at producing large quantities of correlations. Deduction is strong at making inventories, and induction is good at anticipating on new innovations by an opponent.

With the help of the Standard Logic Model it can be visualized what the current overage of a case is, and what the desired state would be. It assesses what sets of techniques will cover what aspects. For the long term, Driver Based Scenario Building deals with both case-theory building and future developments, and is suited for policy planning. Early Warning & Critical Indicator does the same on the near term, and is oriented at acting on threats. Red Team and Red Cell experiments are good to anticipate on possible innovations by an opponent, as new modus operandi. Finally, the establishment of Data Cells will result in quantitative and automated calculation and processing of data, and even in analysis. The model assesses where additional training and education is needed, or additional Data Cells need to be implemented. If an optimal situation cannot be reached – it can be assessed what alternative solutions are possible, as was the case in the illustration on positive vetting.

The Standard Logic Model integrates three aspects. Firstly, all three forms of logic, abduction, deduction, and induction, are included. Secondly, it combines both the qualitative and quantitative approach. Thirdly, analysis by humans and analysis by machines can be combined. It will lead to an enhanced way of working – that of augmented analysis in which machines and humans are paired in their analytic effort.

Where the Rumsfeld Matrix is a tool specialized to design a β oriented research, the more general Standard Logic Model is both suited for an overall planning of the analytic needs, as well as an instrument to evaluate. The combination of the Rumsfeld Matrix and the Standard Logic Model can be used to refine the process of preparation, composition, and evaluation of threat related intelligence case research. The Rumsfeld Matrix can, per quadrant, fine-tune what specific techniques and/or data are needed not to miss a threat. In combination with the Standard Logic Model, it is – in an ordinal way – visualized what part of the case-theory has been covered, and to what extent it has been anticipated on future developments and future innovations.

References:

1. *AJP 2.0. Allied Joint Doctrine for Intelligence, Counterintelligence and Security.* NATO, 2002.

2. De Groot, A.D., (1994), *Methodologie: Grondslagen Van Onderzoek En Denken in De Gedragswetenschappen*. Assen: Van Gorcum.

3. De Valk, Giliam, (2011), "Effectiviteit vanuit methodologisch perspectief: welke gevolgen heeft de introductie van nieuwe methoden en technieken?" In *Contraterrorisme en ethiek*, edited by Michael Kowalski and Martijn Meeder, 69-82. Amsterdam: Boom.

4. De Valk, Giliam, (2012), "Red Team and Science." Presentation at De Nederlandsche Bank (DNB), Den Haag, June 8.

5. De Valk, Giliam, and Willemijn Aerdts, (2018), "Inlichtingenwerk Vanuit Een Methodologisch Perspectief." *Justitiële Verkenningen* 44, no. 1, pp. 114-32.

6. De Valk, Giliam, (2019), *Analytic Blackholes*. Unpublished Paper. Dutch Ministry of Defense.

7. De Valk, Giliam, (2019), "Critical Infrastructure and the Insider Threat." Presentation at The Zagreb Security Forum, Zagreb, March 15.

8. *DoD News Briefing - Secretary Rumsfeld and Gen. Myers*, (2002), United States Department of Defence. February 12, retrieved from https://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636.

9. *Generic Early Warning Handbook*, (2001), Report. EAPC/Council Operations and Exercise Committee. NATO.

10. Goldbach, Onno. Letter to the author, 2012.

11. Grabo, Cynthia, (2004), *Anticipating Surprise: Analysis for Strategic Warning*. Lanham: University Press of America.

12. Heuer, Richard, (1981), "Biases in Evaluation of Evidence." *Studies in Intelligence*, winter, pp. 31-46.

13. Heuer, Richard J., (1999), *Psychology of Intelligence Analysis*. Langley: Centre for the Study of Intelligence, CIA.

14. Heuer, Richard and Randolph Pherson, (2011), *Structured Analytic Techniques for Intelligence Analysis*. Washington, DC: CQ Press.

15. Houtzager, Wil. Lecture at University of Leiden, 11 October 2018.

16. Menkveld, Christiaan. Lecture for '*de Leergang*' at ISGA, University of Leiden, 2018.

17. Moore, David T., (2011), *Sensemaking: A Structure for an Intelligence Revolution*. Clift Series on the Intelligence Profession. Washington, DC: National Defense Intelligence College Press, retrieved from http://ni-u.edu/ni_press/pdf/Sensemaking.pdf.

18. Pace, Chris, ed. (2018), *The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence*. Annapolis: CyberEdge.

19. Sabhikhi, Akshay, (2017), *Augmented Intelligence. Executive Guide to AI.* Austin, Texas: Cognitive Scale, retrieved fromhttps://www.cognitivescale.com/wp-content/uploads/2017/05/Augmented_Intelligence_eBook.pdf.

20. Silver, Nate, (2012), *The Signal and the Noise: The Art and Science of Prediction*. London: Allen Lane.

21. Treverton, Gregory F., (2009), *Intelligence for an Age of Terror*. Cambridge: Cambridge University Press.

22. *The Red Team Handbook.* (April 2012), Report. University of Foreign Military and Cultural Studies, retrieved from https://usacac.army.mil/sites/default/files/documents/ufmcs/The_Red_Team_Handbook.pdf.

23. United States. Department of the Army. FM 34-2 Collection Management and Synchronization Planning. March 1994, retrieved from https://www.globalsecurity.org/intell/library/policy/army/fm/34-2/index.html.

24. *Urban Operations III: Patrolling.* Student Handout. Marine Corps Training Command, retrieved from https://www.trngcmd.marines.mil/Portals/207/Docs/TBS/B4R5579XQ-DM Urban Operations III – Patrolling.pdf?ver=2016-02-10-114414-840.

25. Van Strien, P. J., (1986), *Praktijk Als Wetenschap: Methodologie Van Het Sociaal-wetenschappelijk Handelen*. Assen: Van Gorcum.

26. Voulon, Rosa, (2009), *Handboek Analyse. Theorievorming En Methodologie in Inlichtingenanalyse*. 't Harde: Defensie Inlichtingen En Veiligheids Instituut.

27. Yin, Robert K., (2014), *Case Study Research: Design and Methods*. Los Angeles: Sage.