CRITICAL INFRASTRUCTURE AND THE UNKNOWN: A METHODOLOGICAL QUEST

Giliam de Valk[1]

ABSTRACT: At the the Ad de Jonge Centre, University of Amsterdam, over a period of almost ten years there was experience in Red Team experiments of, among others, the Dutch critical infrastructure. The tests regularly started with the outcomes of the National Advisory Centre Vital Infrastructure (NAVI), to see if any residual threat had been overlooked. The project also encompassed a more methodological approach of how to deal with the unknown.

This article starts with a tool of how to deal with the unknown. The tool is a specific Rumsfeld matrix that was developed in cooperation with the Dutch Intelligence and Security Institute of the Dutch

[1] 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.

defense forces (DISI). The Ad de Jonge Centre used this tool to cope with the different types of unknowns. A focus will be on the so-called unknown-unknown – in which it is both unknown of how to retrieve data, as well as the data themselves.

By using this framework, it will be evaluated of how the Centre came to a more methodological approach in dealing with residual threat. First, the Ad de Jonge Centre took over the already more established technique of Red Team experiments. Secondly, it enriched these experiments, by looking at the β aspects – in order not to miss a threat – of so-called Structured Analytic Techniques. Thirdly, it dealt with the issue of logic – reasoning – in the context of not missing threats. And finally – in an intelligence setting that is dominated by positivistic Empiricism – it turned to continental philosophy, to assess if this would lead to new insights in the dealing with the unknown.

Eventually, the Ad de Jonge Centre developed its own approach in dealing with the unknown and residual threat. This article is meant to share this approach, and to inspire those working in the field of securing the critical infrastructure and working with the unknown.

KEYWORDS: critical infrastructure, methodology, β, residual threat, Rumsfeld matrix, Blind Spot

1. Introduction

When the Ad de Jonge Centre of University of Amsterdam was asked to see if anything was overlooked in protecting of some of the critical infrastructure, it started with a twofold question[2]. First, it looked at the outcomes of and assessments by the National Advisory Centre Vital Infrastructure (NAVI).[3]

The Ad de Jonge Centre inquired if these assessments could be challenged, especially concerning the assessed level of security. This was, as such, a straightforward process. Secondly, it looked at the methodology of such a tasking. This last issue, on methodology, turned out to be more complicated one.

This article will give an overview of the quest at the Ad de Jonge Centre to try to formulate a more methodological approach to test the security of the critical infrastructure. For a large part the focus is on the issue of residual threat. It turned out that some techniques were available, as the Red Team experiment, but a more methodological approach of the issue was almost completely absent. Over the years, it was tried at the Ad de Jonge Centre to get a better insight concerning a possible methodological underpinning of dealing with the unknown and the residual threat.

[2] In 2017, the Ad de Jonge Centre moved to Leiden University and integrated in the Institute for Security and Global Affairs. It transformed into the intelligence working group of the ISGA that, together with other institutions in Europe, wanted to aim at founding an own Continental School for Intelligence (CSI) in Europe.

[3] The NAVI - Nationaal Adviescentrum Vitale Infrastructuur - ceased to function in 2010, after it has made its assessments on the different critical infrastructures in the Netherlands. Advisors of the NAVI continued its activities in the Adviescentrum Bescherming Vitale Infrastructuur. http://www.adviescentrumbvi.nl/search_stats_over_ons.htm, consulted May 2018.

2. The unknown-unknown – positioning, tooling, and methodology

Before focusing on the residual threat, it is first tried to place the residual threat in a bigger picture of unknowns. This section will result in the conclusion that residual threat can be formulated as an unknown-unknown, in which both the way to retrieve the information, and the data itself is unknown. To explain this in more in-depth, it is first turned to a statement from 2002, of the former United States Secretary of State, Donald Rumsfeld.

> [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. Department of Defense, 2002).

2.1 Rumsfeld matrix

Rumsfeld made his remarks in the context of the Iraq war and the absence of evidence of weapons of mass destruction. The emphasis on problems caused by unknowns were a starting point to arrange methods and data. Goldbach & De Valk transformed the quote of Rumsfeld into two axes of unknowns. On the x-axis, it is put whether the way of how to retrieve data is known or not [retrieval]. On the y-axis, it is put whether the data themselves are known or not

[data].[4] This leads to four combinations of retrieval [known/unknown] and data [known/unknown]. Each of those combination is a quadrant of the matrix. Rumsfeld did not refer to the unknown-known. From the perspective of logic, however, there is no reason to exclude this option If his statement is thus rearranged in a matrix, it results in the next composing elements:

Table 1: The Rumsfeld matrix: to retrieve and data

Retrieval **Data**	*Known*	*Unknown*
Known	Known-Known	Known-Unknown
Unknown	Unknown-Known	Unknown-Unknown

The main focus of the Ad de Jonge Centre was on the unknown-unknown – in which both the way to retrieve the information, and the data itself is unknown. Yet, testing the other quadrants also could result in leads of security aspects that were overlooked. As it was assumed that the NAVI had carried out its work well and processed many data with established techniques, the repetition of its work was not the primary focus. As the Ad de Jonge Centre focused on the unknown-unknown, it tried to

[4] A research design with the Rumsfeld matrix 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).

further define – at a methodological level – the type of activity it had to carry out.

2.2 Threat, β and Adversaries Modus Operandi

A question the Ad de Jonge put itself was, if it had to focus on risks or on threats. A risk is here shortly defined as the change an incident might take place multiplied by the impact. Or more formally: risk is the quantitative multiplication of the probability of the occurrence of an event by its estimated impact. In this discipline, the probability is often estimated on a subjective basis – referred at as uncertainty (see Glendon, 2016). This approach implies that, for the risk mitigation, you try to reduce the number of incidents and the impact itself. To assess the risk, it is calculated on data available in the past and present. At the Ad de Jonge Centre this risk approach was assessed as inappropriate for its assignment for two reasons:

(1) it would – to a large part – duplicate the work of the NAVI.

(2) real innovations by humans cannot be assessed by a risk calculation.

Especially for this second reason, the Centre decided to focus on threats only. A threat is here shortly defined as an undesirable event by an opponent that you do not want to take place. Or more formally: a threat is a too hard to handle causes of events that may result in harm. A threat is generally associated with malicious actors (National Institute of Standards and Technology, 2006, 9). A threat does not necessarily cause actual harm. It is on the nature of occurrence (National Information

Assurance Training and Education Center, consulted in 2013). Contrary to the risk approach, it could include to warn for new Adversaries Modus Operandi [AMO] that were never used by this opponent. If it was likely that an opponent could apply this AMO – although it had never used it before – the change it could happen was assessed as 1 [possible]. If not so, it was assessed as 0 [not possible]. A large part of the assignment at the Ad de Jonge Centre was dedicated to identify such new AMO's. Such exercises were already carried out by many groups and were known under various names as Red Team/Red Cell exercises. In this article, Red Team will be used as an overarching term that both includes Strategic Red Teaming – including its assault scenarios, as applied by the military – and Red Cell exercises. Although such exercises can serve different purposes, such as creating awareness, or to develop Standard Operating Procedures (SOP's), the prime focus at the Ad de Jonge Centre was on a third – AMO's and options that apparently were not identified by the NAVI (De Valk, 2012). Then, it was tried to define – from a methodological perspective – more precisely what these exercises exactly encompassed.

Intelligence analysis aims at reducing the uncertainty regarding the courses of action of an opponent. The aim is to give timely warnings for these threats, so actions can be taken to avert a threat. Characteristic for opponents is that they will try to confuse and to mislead to deny information regarding their courses of action.

The orientation on this type of threat has consequences for the so-called α and β, compared to traditional scientific research in which the primary focus is on to explain, to proof something. The α is the chance that you incorrectly conclude that there is a significant relationship between phenomena. The β is the chance that you do not discover a weak, but actual existing, relationship between phenomena. In traditional academic research, the emphasis is to reduce the value of the α – the chance that you incorrectly conclude that there is a significant relationship between phenomena. In intelligence research, however, the main emphasis is on not to miss a threat – the β – the chance that you do not discover a weak, but actual existing, relationship between phenomena (De Valk, 2005, 66-67).

In short: in intelligence research it is more critical to identify the threats and not to miss these (β orientated research), than that you in-depth prove or explain that a threat will occur (α orientated research). This calls for a research design, the application of logic, methods and techniques, with respect to their β capabilities. As we defined risk as the change an incident might take place multiplied by the impact, a risk assessment is thus associated with reducing the α. The threat – an undesirable event by an opponent that you do not want to take place – is about not to miss, and therefore associated with the β. Furthermore, the Centre already decided it was only interested in the threat and the whether or not an opponent could carry out an attack with a certain AMO. As a result, the Ad de Jonge Centre defined the Red Teaming exercises it carried out for the critical infrastructure as follows:

Red Teaming is an experiment to reduce the value of the β by identifying threats that belong to the category of the unknown-unknown to assess if that threat is possible or not (1 or 0). (De Valk, 2012).

Especially in the first phase of dealing with residual threat of the critical infrastructure, this was the prime focus – together with trying to falsify the assumptions the NAVI made concerning the level of security and safety. Now, it is established how the Ad de Jonge carried out its assignments, it is turned to its prime focus – the unknown-unknown quadrant of the Rumsfeld matrix.

3. The unknown-unknown quadrant

In the unknown-unknown quadrant, both the technique to obtain information [retrieval] and the data are unknown. For the unknown-unknown quadrant, the Ad de Jonge Centre could use Red Teaming. At the Centre, only one time a full elaborate Strategic Red Teaming was carried out. In all other cases it was a mix of challenging the assumptions of the current level of security (see, section on known-known quadrant), and looking for unidentified options and AMO's by an opponent. In most cases, it had the resemblance of an upgraded Red Cell exercise.

From the beginning on, the Centre tried to innovate the more classic Red Team and Red Cell approach. First, it was looked at the β aspect of so-called Structured Analytical Techniques (SAT's). For this, it was assessed what aspect of a certain technique could contribute to unveil unidentified aspects concerning threats. In the section on the known-known, an example is given concerning Quadrant Crunching. Second, some of the SAT's were put in a sequence in order to give the upgraded Red Cell experiment more structure. For a series of experiments, different steps were worked through, to see if there were any anomalies discovered that could be a lead for further research. These steps included techniques as Quadrant Crunching, SWOT-inventory, Ease x Impact matrix, CARVER + Shock (for an explanation of some of these techniques, see the heading 'known-unknown quadrant').

What is important to note here, is that these techniques were not used to make an analysis of the case at hand. The techniques were only used to give structure to the experiment. They had shown to be productive in triggering elements and anomalies concerning the established level of security. These identified anomalies would then be the input for the actual Red Team exercise. Furthermore, the Red Team was explicitly instructed not to limit itself to these techniques, and it was encouraged to use whatever the team thought to be useful. In the second phase, the experiment could move into every direction, based upon anomalies found. In this phase, the real experiment into the unknown-unknown started. The approached showed to generate vital new unknowns in nearly all the experiments. Only one critical infrastructure showed to be extremely resilient – and this infrastructure had a very fragmented, network-like and multilayered structure.

4. The known-known quadrant

In the known-known quadrant, both the technique to retrieve the data and the data themselves are known. Besides the Red Team experiments of the unknown-unknown quadrant, the Ad de Jonge Centre also tried to falsify the assumptions the NAVI made concerning the level of security and safety of the infrastructure. Concerning the Rumsfeld matrix, we now deal with the known-known quadrant, as the NAVI based its assumptions on the level of security after elaborate research. In its research both established methods were used and data processed, or – in the system of the Rumsfeld matrix, both the method of retrieval was known, as the data itself.

To challenge the assumptions of the NAVI, the Centre applied Structured Analytic Techniques (SAT's) with a high β potential (see, previous section on the unknown-unknown quadrant). One of those techniques was Quadrant Crunching. To use the technique this way, it had to be simplified a bit – as originally it was used if only a few data are known, to obtain a wide array of hypotheses (Heuer, 2014). For one of the infrastructures, the NAVI had established that it was resilient against attacks, and all the AA-locations were protected at a reasonable level. After Quadrant Crunching, it turned out that this infrastructure was only protected as an object of attack. It was not tested as a means to attack other infrastructures. Furthermore, the implicitly assumed AMO by the NAVI, to blow this structure up, turned out not to be the most effective one, if it was used as a means. The Red Team experiment resulted in an AMO that was easy to carry out. Now, a new inventory was made of these additional AA-locations to be protected. And in practice, additional measures were implemented (for reasons of security, no details can be disclosed).

A second example concerned an object that thought it was save, as it was within the perimeter of another object that had – as a part of its security – a professional counter observation team. Any hostile activities – so the original assumption was – would be noticed by the professional counter observation team. To test this, the Ad de Jonge Centre composed a counter counter observation (CCO) team of a few students, supplemented by one football hooligan. The hooligan was added to the team to include street-wise instinct – and this required some deconfliction with the authorities. This CCO team was only given three very simple directions: 1] work from the outside inwards; 2] make a line of sight map; and, 3] reflect on you timing. With these simple directions the CCO team managed not only to identify the different rings of the counter observation, but it could also identify all the members of the counter observation team – including making close range pictures for identification. None of the members of the CCO team was at any time noticed by the professional counter observation team. The object – that initially thought to be save as it was within the perimeter of the counter observation team – from then on started to rely on its own (new) measures.

5. The known-unknown quadrant

In the known-unknown quadrant, the technique of retrieval is known, but the data itself is still unknown. The known-unknown quadrant was only used in later years of the Red Team exercises, and then mainly for new leads. In those instances, the Centre made an inventory of the techniques that were likely to be used in this quadrant. The Centre used this quadrant also when it was asked to Red Team the security of major events. It could result in threats and scenario's that were overlooked in the original plans.

An example is given of how the protection of a critical infrastructure can be split up in sub-issues. For reasons of anonymity and security, it will be explained for a critical infrastructure that was never investigated by the Ad de Jonge Centre – the electricity network, or national power grid. The protection of the electricity network can easily be split up in three sub-issues.

First, there is the issue of possible perpetrators. In the case of the electricity network, a wide variety of groupings can pose threats. For many years, in the Netherlands, to exercise and to shoot with airguns at the spacers that keep the power lines – in the sections between the power pylons – apart from each other, was a kind of national sport that bothered electricity companies a lot. Furthermore, some decades ago, protestors – under the name of Front of Resistance Gyro Gearloose and the Little Helpers – sabotaged power lines that were connected to Dutch nuclear energy power plants (BVD, 1981, 33). And, it can be a target of terroristic activities. There are many possible perpetrators. How do you then select the most dangerous ones from the different categories mentioned? A method could be, for example, SLEIPNIR,[5] to rank the groups in terms of their

[5] SLEIPNIR is "an analytical technique developed to rank order organized groups of criminals in terms of their relative capabilities, limitations and vulnerabilities. The rank ordered lists of groups are components of strategic intelligence assessments used to recommend intelligence and enforcement priorities". To cope with organized crime, for example, attributes are selected as (in rank): 1 corruption; 2 violence; 3 infiltration; 4 expertise; 5 sophistication; 6 subversion; 7 strategy; 8 discipline; 9 insulation; 10 intelligence use; 11 multiple enterprises; 12 mobility; 13 stability; 14 scope; 15 monopoly; 16 group cohesiveness; 17 continuity; 18 links to

relative capabilities, limitations and vulnerabilities. Furthermore, one could assess for each group the weak and strong points, and the opportunities and weaknesses, with a SWOT-inventory. Finally, as the perpetrators can choose between multiple targets, a CARVER + Shock analysis[6] could be carried out.

Secondly, in order to protect the AA-locations that are most crucial and critical for the infrastructure, one will compose rings of barriers – physically and through security personnel – around these locations. Perpetrators can use different AMO's to enter. Then, a technique will be selected to calculate the time needed to take the barriers for the different AMO's. A Quantitative Intrusion Path Analysis[7] could be used to calculate the delay

other organized crime groups; 19 links to criminal extremist groups. For terrorism, a different attribute set is made (Strang, S.J., 1-5).

[6] CARVER + Shock is an acronym for criticality (measure of impact of an attack), accessibility (ability to physically access and egress from target), recuperability (ability of system to recover from an attack), vulnerability (ease of accomplishing attack), effect (amount of direct loss from an attack as measured by loss of production) and recognizability (ease of identifying target) + shock (the combined health, economic, and psychological impacts of an attack). It is a prioritization tool, a system of target acquisition, to rank potential targets according to a scale. By identifying and ranking the potential targets, attack resources can be efficiently used. It assesses the vulnerabilities within a system, industry, or infrastructure. Originally developed for US special forces, it is now also applied by, among others, the US Food and Drug Administration to enhance 'food defense.' (<http://www.fda.gov/ForConsumers/ConsumerUpdates/ucm094560.htm>; <http://www.fda.gov/Food/NewsEvents/ConstituentUpdates/ucm180608.htm>) (last visited 2012)

[7] The Quantitative Intrusion Path Analysis is a method that is known under different synonyms – with many different variants – often referring to the name of the specific software that is used to carry it out. It is designed not only to weigh physical security measures, but also the human factor. Thus, it could be measured if an opponent could enter – and at what speed, by what AMO – secured critical

at the security rings opponents have to pass. Finally – as it is likely that additional measures are needed – INFOSEC and OPSEC analyses can be carried out based upon the previous findings. In the Red Team exercises, INFOSEC and OPSEC was a returning point of attention. Sometimes, technical personnel – crucial for the maintenance of the infrastructure – complained on social media about their managers. In other cases, the target organization had their INFOSEC intact, but others, like local municipalities and provinces, published sensitive material on their sites that could be used to plan a terrorist attack.

Thirdly, to keep the external communication intact – vital in cases of, for example, a terrorist attack – a Fault Tree Analysis[8] is a logic option. It means that for the second question – to protect the AA-locations – a different techniques is used than for the third question – to keep its external communication intact. The three sub-issues and the techniques that are likely to be used are presented in the next table.

infrastructure. It measures the delay by physical barriers, and calculates issues as recognition, warning and reaction time (for a full system case study, see, for example: Proliferation Resistance and Physical Protection Evaluation Methodology Working Group (2009), Section D). It is also worked out in several variations for cyber.

[8] In 1962, H.A. Watson of Bell Telephone Laboratories developed the Fault Tree Analysis – also referred at as Event Tree Analysis – for the US Air Force (Minutemean). It is a logic diagram to relate conditions that precede faults and undesired events. At the top of the schedule, the undesired event – end state – is placed. It can be applied in both a qualitative and quantitative way (Martensen, et al. (1987), 1-3, 6-9).

Table 2: The known-unknown quadrant & a quick scan of techniques: three sub-issues in the protection of the national power grid

Sub-issue	*Technique*
Perpetrator analysis	SLEIPNIR SWOT- analysis CARVER & Shock
To keep the perpetrator out of the AA-locations	Quantitative Intrusion Path Analysis INFOSEC analysis OPSEC analysis
To keep the communication intact in case of an emergency	Fault Tree Analysis

Such a quick scan by the Centre could lead to outcomes that were not identified in the original plans. This was especially the case if the plans were based on experiences in the past, and not on a thorough analysis.

6. The unknown-known quadrant

In the unknown-known quadrant, the technique or algorithm to obtain information [retrieval] is unknown, but the data as such are present. This quadrant was never used in any of the Red Team exercises by the Ad de Jonge Centre. The simple reason was a lack of resources. However, it could be fruitful to uncover correlations that otherwise would remain unidentified. Working this way with AMO's can lead to new insights. In the Netherlands, for example, large numbers of copper cables were stolen from the railway company. After additional measures, the theft of copper moved to the public space (art). After additional measures here, a waterbed mechanism developed. This mechanism was discovered by the Dutch Sosecure company that had initiated a data base for AMO's (Plas, 2018). The unknown-known quadrant can eventually lead to a new sub-branch of Red Team exercises that is hardly made use of yet. It eventually could result in elaborate scenarios of how to counter these identified threats. This scenario building does not need to be carried out by the Red Team itself, but it could also be produced by the organization itself.

7. Reflecting on the assignments

When in 2017 the Ad de Jonge Centre moved from the University of Amsterdam, to Leiden University – where it integrated in the Institute for Security and Global Affairs – it reflected on the past decade of dealing with the unknown. For its Red Team experiments, the Centre applied known Red Team approaches, had made use of its Rumsfeld matrix, enriched it with the β aspects of SAT's, and had challenged the assumptions of the assessed security level.

It felt the need to evaluate its past on an even more abstract methodological level. First, it looked at how the different quadrants of the Rumsfeld matrix could contribute to test an already developed security plan. Secondly, it tried to assess how logic – reasoning – could contribute to reduce the β. Thirdly, it looked at the philosophical traditions in which security and intelligence had developed.

7.1 Residual threat and the quadrants of the Rumsfeld matrix

In the beginning, the Ad de Jonge Centre focused on the unknown-unknown quadrant – in which both the way of retrieval, and the data themselves are unknown. It turned to more established Red Team approaches, and finally developed an own – upgraded – Red Cell experiment that fitted the need of testing the assessments by the NAVI. But to what extent could the incorporation of the other quadrants of the Rumsfeld matrix also contribute to reduce the value of the β – the reduce the threat level as assessed by the NAVI? Now, a reflection is presented, focusing on the potential of a certain quadrant to minimize the value of the β – in order not to overlook a threat.

First, there is the known-known quadrant – in which both the method of retrieval and the data themselves are known. This quadrant showed to be fruitful in challenging assumptions concerning the level of security, as assessed by the NAVI. Especially a simplified version of Quadrant Crunching showed to be simple, fast and very effective in challenging assumptions. After additional research, it led to convincing results and practical measures were taken by the responsible authorities.

Secondly, there is the known-unknown quadrant – in which the method of retrieval is known, but the data themselves are unknown. This quadrant showed to have a potential to check if in the original security plan the most effective methods of analysis were used. Especially if the main issue was split up in sub-questions, the known-unknown quadrant resulted in SAT's likely to be used to make an analysis of the problem. This quadrant also showed to have potential for securing major events. Often, the security of such events is protected based on scenarios of the past. The methodic approach of the known-unknown quadrant had then a large potential of yielding additional insights.

Thirdly, there is the unknown-known quadrant – in which the method of retrieval is unknown, but the data themselves are known. The Ad de Jonge Centre itself had no experience with this quadrant. However, the private Sosecure/Kenniscentrum made and inventory of AMO's and discovered cross-sectorial crime. The preliminary findings here tend to indicate that it will uncover AMO's and trends that otherwise will stay unnoticed in the more traditional way of minimizing residual threat.

To summarize: in the case of future Red Team experiments, elements could be included of the other three quadrants, besides the unknown-unknown. Quick checks could produce anomalies for further experimenting. But for testing the unknown-known quadrant, it would require databanks as developed by Sosecure/Kenniscentrum.

7.2 Logic: three types of reasoning

In evaluating the Red Team experiments of the Ad de Jonge Centre, it was also assessed how logic had contributed to reduce the value of the β – to reduce the threat. This was done for the logic applied in all quadrants of the Rumsfeld matrix. It turned out to be a challenging evaluation, as the theory for reasoning was only developed in the context of reducing the value of the α – but not of the β. The findings presented here are therefore still preliminary and partly unmatured.

It is assumed for reasons of robustness that all different classes of reasoning have to be used to minimize the value of the β as much as possible. In research, robustness refers to applying several methods and techniques in an analysis. The more such independent tests are survived, the more plausible the conclusion will be. Consequently, the finding does not depend on the analytical method used. To apply many methods to the same set of data, the margin of error is reduced (De Valk, 2005, 67-68). And it is assumed here that it is not only reduced by applying more methods, but also by applying different classes of reasoning. These classes of reasoning are deduction, induction, and the inference to the best explanation (IBE or abduction).

A short description is presented on the classes of reasoning. First, there is deductive reasoning in which you argue from the general to the specific. An argumentation is deductive, meaning that if the premises are correct, the conclusion therefore will also be correct. Secondly, there is inductive reasoning in which a general rule is made based upon a number of specific observations or experiments. If the premises are true, the conclusion is likely to be true. Inductive reasoning is probabilistic, the premises do not make the conclusion absolute. Thirdly, there is the inference to the best explanation (IBE), or abductive reasoning, in which an explanation is selected based upon likeliness. It is assumed that the most likely conclusion is the correct one (Martensen, 1987, 24-27. Grabo, 2002, 42-43). It is reasoning through successive approximation.

As formulated in the above, the reasoning is developed in the context of reducing the value of the Such a quick scan by the Centre could lead to outcomes that were not identified in the original plans. This was especially the case if the plans were based on experiences in the past, and not on a thorough analysis.

6. The unknown-known quadrant

In the unknown-known quadrant, the technique or algorithm to obtain information [retrieval] is unknown, but the data as such are present. This quadrant was never used in any of the Red Team exercises by the Ad de Jonge Centre. The simple reason was a lack of resources. However, it could be fruitful to uncover correlations that otherwise would remain unidentified. Working this way with AMO’s can lead to new insights. In the Netherlands, for example, large numbers of copper cables were stolen from the railway company. After additional measures, the theft of copper moved to the public space (art). After additional measures here, a waterbed mechanism developed. This mechanism was discovered by the Dutch Sosecure company that had initiated a data base for AMO’s (Plas, 2018). The unknown-known quadrant can eventually lead to a new sub-branch of Red Team exercises that is hardly made use of yet. It eventually could result in elaborate scenarios of how to counter these identified threats. This scenario building does not need to be carried out by the Red Team itself, but it could also be produced by the organization itself. α: on how to reach your conclusions and on the absoluteness of your claim. β research, however, is about to avoid missing relationships. In such a context, reasoning – deductive, inductive, or via inference to the best explanation (IBE) – need to be reformulated, and to be calibrated from an α approach to a β approach. Then it is not about to proof or to explain, but about to avoid to miss a relationship. Not only in general publications on methodology, but also in intelligence handbooks, reasoning is presented and explained in the context of reducing the α, and not of the β (De Groot, 1981, 38, 76-82, 38. Grabo, 2002, 42-44; Voulon, 2010, 24-27).

To what extent can reasoning - deduction, induction, and IBE – contribute to avoid to miss relevant relationships – threats? During the Red Team experiments, some insights were obtained. Without claiming definitive conclusions, the experiments at the Centre indicated some strong and weak points of these three ways of reasoning (De Valk, 2018, 120-122).

Table 3: Reasoning and to reduce the value of the β

Reasoning	***Strength***	***Weakness***
Deduction	Fast, first, general inventory on already identified threats. It directs the research at	Weak in making an inventory of a deviation of the general pattern. Hardly covers real innovations.

Reasoning	***Strength***	***Weakness***
	possible residual threats. Good at calculating the resilience.	
Induction	Maps innovations, as new AMO’s. Aims at the unique [e.g. by Verstehen].	Slow for making an inventory of possible threats. Maps only a small part of the case at hand.
IBE [abduction]	To challenge assumptions. Big data [quantitative]: generates many correlations, otherwise overlooked. These correlations may lead to additional hypotheses and maps patterns with a prognostic value [trends].	Often no causality. A minority of the correlations found will be of relevance for the threat issue. Often, additional qualitative checks are needed. Limited mapping of innovations [only for trends], because the data needs to be present in a significant number.

As a result of these preliminary findings, it is recommended to include all types of reasoning in the Rumsfeld matrix when developing an overall security plan. Although not actively tested during the assignments, it looks also promising to make use of all three types of reasoning in Red Team experiments. This would imply also quick checks for the other quadrants – as described in the previous paragraph – as the unknown-unknown quadrant is by its nature inductive.

7.3 Residual threat: Empiricism and The Idea

In what tradition has the thinking on security and intelligence evolved? If we look at the literature, it is dominated by Anglo Saxion publications. In turn, reflecting on security and intelligence is highly influenced by Empiricism. In this tradition, there is a focus on the object and on to measure the object. How could this object be best measured and what are the pitfalls in the measurement? In our field, an important emphasis is put on the concepts of denial and deception – the opponent who tries to deceive us in making an assessment. To cope with denial and deception, security services have developed dogma's as to mobilize extra sources and other means of investigation (De Valk, 2005, 351). Attention is also paid to biases by ourselves. In Heuer's Psychology of Intelligence Analysis, for example, it is put that the analytic traps caught the intelligence expert as much as anybody. The 'pitfalls the human mental process sets for analysts cannot be eliminated; they are part of us. What can be done is to train people how to look for and recognize these mental obstacles, and how to develop procedures designed to offset them' (Heuer, 1999, x & xi). Solutions are found in options as working with SAT’s, as for example formulated by Heuer and Pherson (Heuer, 2014).

Could we miss something as a result of this dominance of Empiricism? Another tradition is the continental philosophy or The Idea. Concepts that have been developed here, could contribute to additional insights to reduce the value of the β. One of these concepts is The Blind Spot. When we view reality, our mind – ourselves – is always included in our viewing of it. Since we are part of the universe, whatever we view will always include us as a distortion. This is a blind spot we cannot account for.

> [t]he observed difference is not simply "subjective," due to the fact that the same object which exists "out there" is seen from two different stations, or points of view. It is rather that, as Hegel would have put it, subject and object are inherently "mediated," so that an "epistemological" shift in the subject's point of view always reflects an "ontological" shift in the object itself. Or, to put it in Lacanese, the subject's gaze is always-already inscribed into the perceived object itself, in the guise of its "blind spot," that which is "in the object more than object itself," the point from which the object itself returns the gaze (Zizek, consulted in 2018).

The potential of this approach is that the focus is not on the object of research – including in relation to pitfalls in the analyst’s mental process – but on the distortion of what we view as we are part of the world we are researching. Eliminating residual threat would – according to the concept of the Blind Spot – an unsolvable issue. Also, it points at the need of different perspectives – to cope with at least a part of our own Blind Spot – in order to reduce the value of the β.

The concept of the Blind Spot points at the importance of team composition and the guidance of people of different backgrounds that use different ways of working. It is needed to show how each could contribute to the total by its own specific quality. Concerning the concept of the Blind Spot, there is a difference in emphasis compared to Red Team handbooks in the way it calls attention for the group composition and mental pitfalls (Command Red Team, 2016). During the most successful Red Team exercises at the Centre, the teams were composed of different backgrounds and personalities. This also called for some extra guidance to keep the team together. Also to include more street wise people into the team had showed to be of great value – as, for example, concerning the earlier mentioned football hooligan.

Maybe, this diversity also applies to security and intelligence agencies. The issue of the Blind Spot may point at problems when the selection is biased by the recruitment of employees with an academic level, from a middle class and autochthonous background. It will lead to limitations in perspectives. To recruit from minority groups – or sailors who have seen the darker side of the harbors around the world – could be of an added value for the services. Concerning the Dutch General Intelligence and Security Service, a bias was noticed in the recruitment of new personnel: ‘well-educated, ambitious, liberal ladies in their thirties enter the service, who first want to put their off-spring to school with their box bikes' (NRC, 2018). It may lead to adjustments in both the assessments during the recruitment and the methods of screening by services.

8. Final observations: A Game of Perspectives

When the Ad de Jonge Centre tried to assess its position to test the assessment of the NAVI, it started with a methodological definition concerning its Red Team activities. It defined Red Teaming as an experiment to reduce the value of the β by identifying threats that belong to the category of the unknown-unknown to assess if that threat is possible or not (1 or 0). In the following years, it developed its own approach to cope with the residual threat, that eventually evolved into A Game of Perspectives.

A Game of Perspectives is composed of different elements. First, it explores all the four quadrants of the Rumsfeld matrix. There is a main emphasis on the unknown-unknown quadrant. But also the assumptions concerning the level of security are challenged – the known-known quadrant. For this, it is looked at the β aspects of the SAT's. A quick stress test will be carried out on the methods used in the known-unknown quadrant. There is the possibility to include the unknown-known quadrant as well, if relevant databanks are available. Secondly, all three types of reasoning are included in the exercise. Finally, the concept of the Blind Spot indicates to focus on different perspectives, not only in assessing the opponent, but also within our own community in order to minimize our own blind spot as least a little bit more.

However, this evaluation and rethinking on its activities is a snapshot in time of work in progress.This also applies to A Game of Perspectives. It is the conviction of the author, however, that to develop tools like the Rumsfeld matrix, and to obtain a better methodological understanding, will serve our activities of minimizing the value of the β. The ultimate goal is to keep the value of the β as low as possible. We hope this evaluation will lead to inspiration and a more methodological oriented reflection on the unknown and residual threat.

References

1. *Binnenlandse Veiligheidsdienst (1981), quarterly survey 4 of 1981 (unreleased).*
2. *Command Red Team (2016), Joint Doctrine Note 1-16.*
3. *Glendon A.I., Clarke, S. McKenna, E. (2016), Human Safety and Risk Management, CRC Press, second edition.*
4. *Groot, de (1981), Methodologie. Grondslagen van onderzoek en denken in de gedragswetenschappen. Den Haag: Mouton, 1981 (11th print).*
5. *Grabo, C.M. (2002), Anticipating Surprise: Analysis for Strategic Warning. Washington: DIA.*
6. *Heuer, R. (1999), Psychology of intelligence analysis, CIA, Center for the Study of Intelligence, History Staff.*
7. *Heuer, R., Pherson, R.H. (2014), Structured Analytic Techniques for Intelligence Analysis, CQ Press, 2014*
8. *Martensen, A.L., Butler, R (1987), The Fault-Tree Compiler. NASA, Langley Research Center.*

9. *National Information Assurance Training and Education Center (consulted in 2013), Glossary of Terms. URL: http://niatec.info/Glossary.aspx?/term=5652 &&alpha=T*
10. *National Institute of Standards and Technology (2006), Minimum Security Requirements for Federal Information and Information Systems, Federal Information Processing Standards, FIPS PUB 200, March 2006, 9.*
11. *NRC Handelsblad (2018), 'De politiek krijgt te veel invloed op de AIVD' (by Kees Versteegh), 15 February 2018.*
12. *Plas, L. van der, interviewed by De Valk, April 10, 2018.*
13. *Proliferation Resistance and Physical Protection Evaluation Methodology Working Group (2009), PR&PP Evaluation: ESFR Full System Case Study. Final Report. October 2009.*
14. *Strang, S.J. (-). Project SLEIPNIR: An Analytical Technique for Operational Priority Setting. RCMP.*
15. *U.S. Department of Defense, Office of the Assistant Secretary of Defense, Public Affairs (2002), News Transcript DoD News Briefing - Secretary Rumsfeld and Gen. Myers, February 12, 2002 11:30 AM EST.*
16. *Valk, G.G. de (2005), Dutch intelligence - towards a qualitative framework for analysis: with case studies on the Shipping Research Bureau and the National Security Service (BVD), Boom Juridisch.*
17. *Valk, G.G. de (2012), "Red Team and Science", Presentation for De Nederlandsche Bank (DNB), June 8th, 2012.*
18. *Valk, G.G. de, Aerdts, W.J.M. (2018), 'Inlichtingenwerk vanuit een*

methodologisch perspectief', Justitiële verkenningen, year 44, no. 1, 2018.

19. *Voulon, R (2010), R. Voulon, Handboek analyse. Theorievorming en methodologie in inlichtingenanalyse. DIVI/DISI.*
20. *Zizek, S. (consulted in 2018), 'The Parallax View. The Stellar Parallax: The Traps of Ontological Difference'. URL: http://www.lacan.com/zizparallax.htm*