Achieving Cyber Situation Awareness Through a Multi-Aspect 3D Operational Picture

Mees, Wim
Royal Military Academy, Brussels, Belgium

Llopis, Salvador
European Defence Agency, Brussels, Belgium

Debatty, Thibault
Royal Military Academy, Brussels, Belgium

Abstract

A military commander in an operational environment needs to underpin his decision-making and evaluate situations based on the information available to him. To that end, a 3D operational picture, specific to the cyber-domain, is described in this research paper that helps the decision maker to comprehensively assess the criticality of different mission elements in a given scenario.

The paper provides a practical analysis of how different types of information can be combined into a single multi-aspect 3D visualization, further completed by a number of specific sub-views. An intuitive display of the essential information is built, and this at different levels of abstraction, each time proposing appropriate ways for encoding the principal information components. The 3D overview is built around a conceptual "spring-model", called "Mission - Attacker – Controls" (MAC) triangle per asset, which considers various planning factors that the commander and his staff should take into account.

The components of the forces that are represented in the MAC triangle are derived from low-level security metrics that are in turn based on low-level data and measurements. The low-level information is evaluated using fuzzy domain knowledge and approximate reasoning and finally aggregated into a single value that quantifies the strength of each force component.

Keywords: 3D operational picture, multi-aspect 3D visualization, security controls, security metrics, cyber-defense situation awareness.

1 Introduction

A military commander, or for that matter any decision maker, is mainly interested in the "cyber-situation" of his organization for as far as this has an impact on the mission [MD15]. The decision maker is not interested in a set of specific, quantifiable metrics representing partial aspects of information security. A high-level operational

picture (OP) must be a useful tool that the commander can immediately interpret to assess the situation and make decisions with respect to the mission, such as resource allocation, tasking, etc.

Authors have explored how novel man-machine interfaces might help the decision maker achieve situation awareness, and as a result produce better decision making. In this paper we introduce an approach that combines different types of information into a single multi-aspect 3D visualization, using representations that are familiar to the decision maker. This allows for a rapid, intuitive access to the information in the operational picture and in this way contributes to producing a timely and accurate situation awareness.

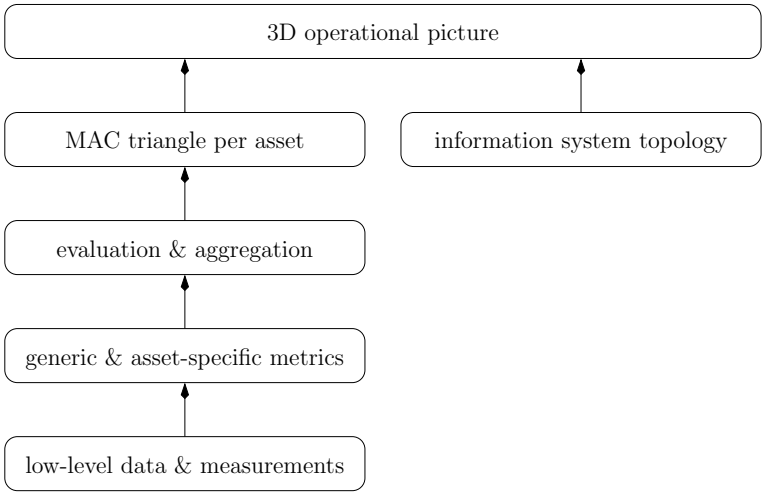


Figure 1: concept

Figure 1 shows the global approach. A 3D operational picture, explained in section 2, is the first view that is shown to the operator. It is primarily based on the logical information system topology, yet also incorporates a global security level for every asset that is determined by the corresponding "Mission - Attacker - Controls" (MAC) triangle.

This triangle is explained in more detail in section 3. It combines three mission relevant security characteristics in a single view, that makes it possible - for instance during "Course of Action" (CoA) development, to easily compare different assets with respect to their current security posture for a given mission.

The components represented in the MAC triangle are derived from lower level, specific metrics that are in turn based on low-level data and measurements, as is explained in section 4.

Finally, in section 5, the way in which domain knowledge, expressed using fuzzy logic, is used to evaluate the metrics and to aggregate the partial results is presented.

2 3D operational picture

The decision maker is not interested in a dashboard full of gauges and meters, displaying a large number of quantified metrics. The interpretation hereof requires too much effort, is prone to errors, and slows down the decision making process. The decision maker simply needs answers to the following types of questions:

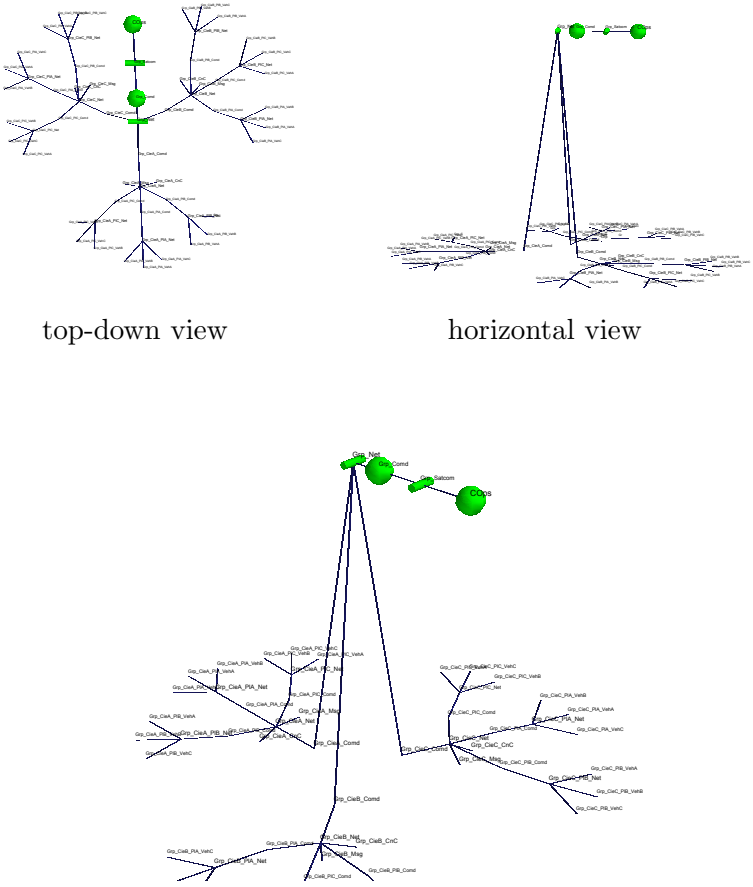
- Does the cyber-situation jeopardize the ongoing mission?
- Do I need to change the allocation of resources in response to the evolving cyber-situation?
- When comparing different possible courses of action, what are the threats and opportunities produced by the cyber-situation?
- ...

What is needed therefore is an intuitive display of the essential information, elevated to the level of abstraction that is of interest to the decision maker, applying encoding mechanisms for this information that allow the decision maker to assess the situation in a glance. We therefore propose the following ways of encoding the principal information components in an intuitive way:

- *shape:* different classes of assets are represented by different shapes that are easily distinguishable and recognizable,
- *size:* when the size of a symbol is bigger, this means that the represented asset is more important to the mission,
- *color:* when the color of a symbol is closer to red a lot of interest in this asset is observed on behalf of the opponent, whereas when the color is closer to green, there is less or no hostile activity observed against the asset,
- *height:* when symbols are "tied down" close to the ground this means their security is considered to be well controlled, whereas when they are floating up high in the air they are more at risk of "breaking off and flying away in a storm",
- *motion:* motion represents change, therefore when one or more characteristics of an asset are changing, the symbol representing the asset will be shaking, with an amplitude that reflects the intensity of the change.

All these characteristics, that are easily understandable by any human being, are used to build an intuitive 3D visualization for the decision maker, as is shown in figure 2. In this simple example horizontal "tubes" represent multi-access networks, boxes represent servers or services, and spheres represent end-user equipment.

The horizontal plane is used for laying out the topology of the distributed information system. The height at which assets are represented, reflects the extent to which their



top-down view horizontal view

perspective view

Figure 2: visualization

security is considered to be well controlled at this time, with greater heights meaning less well controlled.

Figure 2 shows an example scenario of a coalition task group in a peace enforcement operation, that consists of three company level entities (Cie A, Cie B, Cie C) from different nations, with a task group commander (Grp Comd) that has a link to the battle group's operations centre (COps). At the start of the operation the companies are in a staging area and only Grp Comd and the COps are important to the mission at that time, and therefore large in size, as well as the link between them and the network that allows the Comd to reach out to this companies.

The first mission requires an intervention to restore order in a town where riots have broken out, instigated by a local warlord, who is known to dispose of powerful VHF jamming equipment that he uses to disrupt the C2 of an intervening force and in this way isolate individual vehicles or dismounted patrols before attacking them. At the decision brief, following the CoA development by his staff, the commander decides that

a company-sized unit should be sent out in order to intervene in the riot area of town.

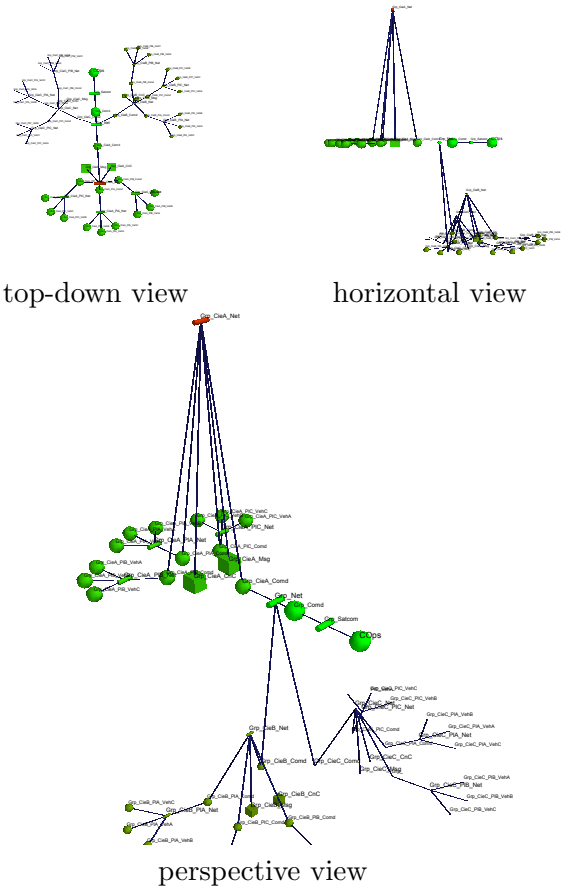
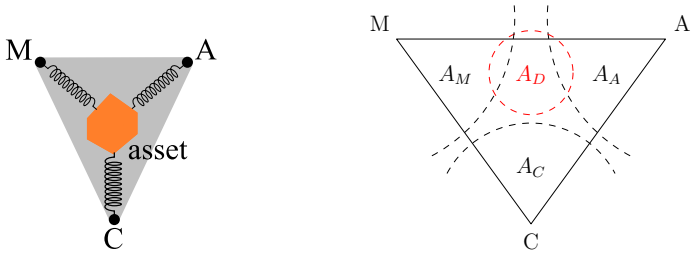


Figure 3: visualization

Based on a number of criteria they identify Cie A as the most suitable choice, with Cie B appointed to stand by in order to provide support to Cie A when needed. This leads to the operational picture shown in figure 3, where the mission importance of Cie A leads to large symbols, and the stand-by role of Cie B to medium-sized symbols. When the Comd and his staff look at the cyber operational picture corresponding to this CoA, they see however that the Cie A network is high up in the visualization and dark red, and therefore represents a risk to the mission.

3 The MAC triangle

The height of an asset in the 3D operational picture serves as an indicator that shows whether the asset is sufficiently well protected by security controls ("C") or not, given the attacker's ("A") interest in the asset and the asset's importance to the mission ("M"). These three characteristics are represented in the MAC triangle.



(a) spring model (b) typical zones

Figure 4: MAC triangle

The position of an asset within the triangle is determined by a spring-model, as is shown in figure 4(a). Two forces pull the asset upwards:

- F_M: the importance of the asset to the mission,
- F_A: the attacker's interest in the asset,

and one force pulls the asset downward:

- F_C: the security controls in place to protect the asset.

The magnitude of these generic forces results from the aggregation of a number of more specific metrics, as will be discussed in more detail in section 5.

Four characteristic areas can be identified in the MAC triangle, as depicted in figure 4(b):

- A_D: assets in this area are important to the mission and receive a lot of attention from attackers, yet have insufficient controls in place to properly protect them. Assets in this area are in a very dangerous situation and require immediate attention.
- A_M: assets in this area are important to the mission, not very well protected, but have not yet drawn a lot of attention from the enemy. This may however change at any time, therefore this situation should be addressed during future CoA development and decision cycles.
- A_A: assets in this area are being targeted by the attacker, yet are not important to the mission. If they will not become important to the mission in the near future, and cannot be used to launch attacks against other assets, it may be a deliberate choice to use these assets as a honey-pot to discover the adversary's capabilities and intentions.
- A_C: this is the target situation for all assets that are, or will be at some point in time, important to the mission. The security of these assets is well controlled. Based on the shape and the color of the symbol we can distinguish assets that

are important to the mission (big), or that are targeted by the enemy (red), but it does not matter since the installed strong security controls keep the assets' representations close to the bottom of the triangle.

The 3D overview only shows the vertical position of the assets, that results from the vertical component of the composition of the three forces. In order to analyse in more detail the situation, and identify possible options for modifying the CoA that would reduce the cyber-risk, the commander and his staff need to examine the causes for the high position of the Cie A "network" asset in figure 3 in more detail.

They furthermore want to compare the Cie A network situation with that of the two other Cie networks, and therefore select all three objects in the 3D view and call up a representation of these three assets in the MAC triangle, as is shown in figure 5 (since CieC has no mission assigned, its F_M force is zero, hence no blue arrow).

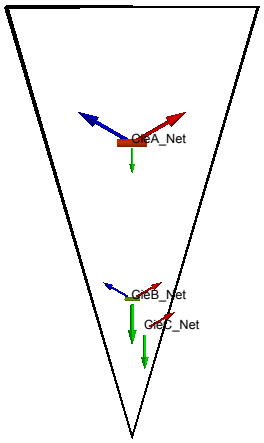


Figure 5: detailed view

It is clear from this view that the upward forces are stronger for the CieA_Net asset, since being the primary intervention entity, Cie A is more important to the mission, and will also be targeted more intensely. However the MAC triangle also shows that the protective controls for the other units' networks are stronger.

The commander and his staff might for this reason consider switching to Cie B or Cie C as primary intervention force. However, other reasons outside of the cyber realm, for instance political, cultural, religious, ..., dictate that the other companies are less well suited for intervening in that specific area of town where the riots have started, and therefore a solution is sought for improving the F_C force for the CieA_Net asset.

The forces that are shown in the MAC triangle, represent the high-level result of an aggregation of lower-level more specific metrics. Therefore the Comd and his staff select the "C" corner of the triangle and then the option to develop in further detail the F_C force of the represented assets, resulting in the visualization shown in figure 6.

As an example, the "controls" force F_C is decomposed into the following five components, depicted from right to left:

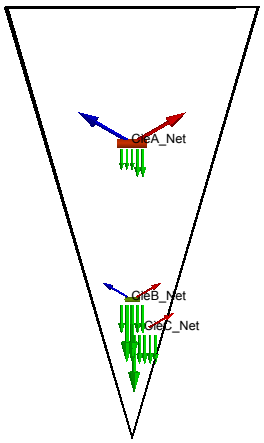


Figure 6: detailed view

- pro-active human controls: user training & awareness programs, controls management, ...
- pro-active technical controls: asset management, configuration & change management, vulnerability and patch management, ...
- re-active human controls: trained incident handling staff, forensic experts, ...
- re-active technical controls: system monitoring, attack detection, ...
- continuity controls: service continuity management, disaster recovery capability, alternate circuits, ...

An illustrative use case would be to consider that Cie C has "Satcom on the Move" (SotM) available as an alternative to the VHF radio network, explaining the high "continuity" score. This solution can however for technical reasons not be transferred to Cie A. However, Cie B shows a strong re-active capability in the MAC triangle, which is due to the fact that they have the necessary equipment to perform a rapid localization of jamming sources, so they can engage them to render them ineffective. This capability can be provided in support of Cie A if needed.

In this example we have shown how a Comd and his staff were able to understand the cyber risks associated with a CoA during the planning phase, and look for alternatives to reduce the risk, going from a generic to a more specific level of understanding of the situation using an intuitive 3D visualization and subsequently the MAC triangle representation. Figure 7 shows the impact on the 3D OP resulting from the CoA design change of adding the jammer detection capability of Cie B to Cie A.

It would be possible to have the staff officers develop a number of CoA alternatives and present the possible new positions of the involved assets in the same 3D view, with an arrow from the old to the new position that has a thickness that is for instance

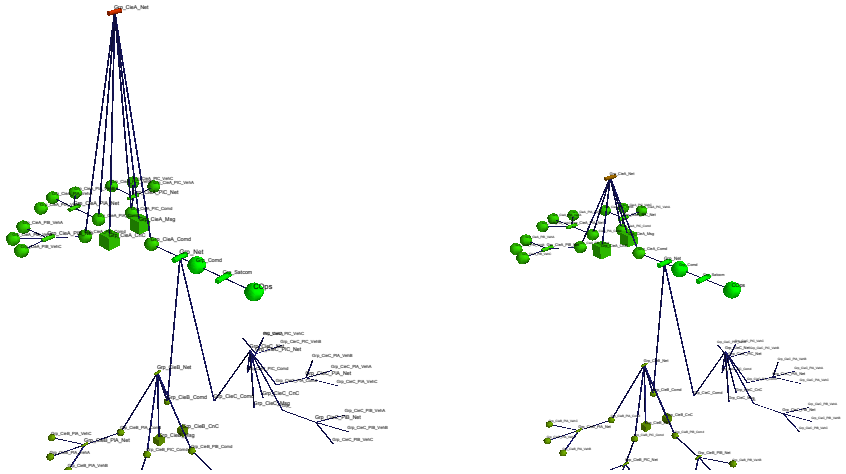


Figure 7: perspective 3D view before & after modifying the CoA

proportional to the "cost" of the change. Currently this process is triggered manually for the different operational phases to produce new assessments as the situation evolves from the given initial setting. The dynamic updating of the 3D view is planned as a future development.

4 Low-level security metrics

The MAC triangle per asset as the basis for the 3D operational visualization requires the choice of a number of security metrics for quantifying the strength of the components of the force F_C. The components used in the context of the scenario introduced above are classified as pro-active, re-active and continuity controls. They need to be calculated by using appropriate metrics and the corresponding evaluation methodologies.

Once the mathematical elements are selected, a technical staff can conduct an analysis of which mitigation actions or countermeasures produce better results to reduce the cyber-risk to the mission when needed. By applying this reasoning, the components of F_C shall grow in magnitude and pull down to counter the forces F_M and F_A. The use of the security metrics defined in this context enables the controls' measurement and contributes more objectively to a 3D representation of the cyber-situation. Besides, security metrics achieve a maturity level when they are put into practice repeatedly to test that the obtained results are meaningful and commonly accepted as mission relevant by staff planners. An interesting testbed for this are "wargaming" exercises where red teams and blue teams oppose actions and reactions following a scheduled order as part of the operational planning process to agree informed conclusions before the commander's decision brief.

According to NIST 800-55 [NIS03b], information security metrics are used to facilitate decision-making and improve performance and accountability through the collection,

analysis, and reporting of relevant performance-related data. Hence, security metrics are functions on a set of parameters aiming to describe characteristics not only in the area of information security, but also in telecommunications or procedures with certain restrictions in their applicability. Hecker [Hec08] distinguished the low level metrics as those that are direct results of measurements on subsystems and isolated system elements and are different from the high level metrics.

Given the complexity of capturing significant parameters for the evaluated scenario from section 2, an exercise has been performed to consider different variables per control area. Subsequently, the group of variables is submitted to a selection process to choose the ones deemed most suitable for the metric design. Arguably, very instance-dependent and not commonly generalized without a proper adaptation. What is essential is that a wrong selection will dramatically influence the results becoming a worthless effort for the analysts. Indeed, all the process reinforces the value of the so-called "operational art".

Cyber staff with the participation of Communication and Information Systems (CIS) personnel analyses what resources are available to accomplish the mission and ultimately manage the Cyber Situation Awareness as part of the overall operation domain. The security controls must be checked with regards to the mission goals and objectives. In this case, security metrics are fit for purpose, mission-specific and adjusted to the situation. Ideally, a modeled and simulated environment able to run the security situation over time would come up with valuable results to confirm or discard mission assumptions.

Some questions may arise to the technical staff when analysing the joint operational environment:

- Are the controls established enough to satisfy the minimum mission-specific requirements?
- How can the mission success rate be improved?
- Is there any mission-critical aspect that leads to a "no-go" operation or calls for a re-evaluation of the situation?

It is expected to approach answers to these questions with the development, test, refinement and experimentation of the security metrics applicable to the situation. To find meaningful security metrics, a deep analysis of what should be measured and why is to take place. Every output must be carefully treated to verify reality with the best knowledge available and to demonstrate some tangible results useful for mission planners. Continuing with the introduced example of the CieA_network asset and returning to the planned mission to restore order in a town, the exercise would consists of determine associated specific variables per control area.

components of F_C	control areas	associated specific variables per control area (meant to be more or less significant to one or several controls in an identification process)
pro-active human controls	• user training & awareness programs, • controls management	• people trained on cyber defence, • reporting and control echelons, • subordinate/ supporting units, • human factors, • asset usability
re-active human controls	• trained incident handling staff, • forensics experts	• people trained on incident handling or forensics, • incident handling or forensics mechanisms, • human factors, • asset usability, • response time to a security event
pro-active technical controls	• asset management, • configuration & change management, • vulnerability and patch management, • rapid localization of jamming sources	• network vulnerabilities, • vulnerability severity, • impact, • cyber hygiene mechanisms, • asset availability, • asset survivability, • protection level, • compromised devices, • time to operate, • network failures or malfunctions, • communication losses
re-active technical controls	• system monitoring, • attack detection	• network critical points, • network strengths, • cyber incidents detected

continuity / resilience	• service continuity management, • disaster recovery capability, • alternate circuits	• service availability, • operational capacity, • network readiness, • network resilience, • redundancy, • contingency links, • communications diversity

Table 1: force components / associated specific variables per control area

The list of controls presented in table 1 is not exhaustive and others may be more appropriate depending on the situation. The controls' correspondence with the associated variables has been made with enough flexibility to address one or several controls in the same area. Others administrative aspects such as procedures or organisational structures are not evaluated although they are a crucial part and should be considered by the planners including other security principles like confidentiality and integrity.

Yi Cheng et al. [CDL+14] proposed a set of security and performance metrics, mainly focusing on network vulnerability assessment, attack risk evaluation and mission impact analysis, that are adequate for this exercise. The example in section 2 uses the CieA_network as the primary asset and some appropriate metrics for this asset have been identified in table 2 by analysing information from the required mission. It is not always possible to easily identify a metric that covers a desired feature despite the fact that existing observable variables may be available.

The process of constructing the associated metrics generated the following list:

metric & type	description	score/value
cyber training of staff *(soft)*	expert assessment of the cyber readiness level of the staff as a result of training	set of terms (e.g. "sub-standard", "average", "good", "expert")
average response time *(hard)*	average time needed to handle a security event or incident	measured average response time (in hours)
average time to operate (cyber deployable assets) *(hard)*	average time needed to operate cyber deployable assets under the planned conditions (e.g. individual vehicles or dismounted patrols)	measured average time to operate deployable assets (in minutes)
network readiness *(soft)*	is CieA_network ready to accomplish the mission? e.g. all required services are supported by available servers	set of terms (e.g. "not ready", "some critical services down", "critical services available", "all services available")

asset survivability *(soft)*	survivability aspect of the CieA_network after being degraded, attacked or compromised	set of terms (e.g. from "no survivability" to "fully survivable")
communications diversity *(hard)*	number of direct communication links able to establish by different means simultaneously	number of direct communication links by different means simultaneously
network critical points *(hard)*	a revision of the network architecture can identify critical points subject to be exploited by an attacker	number of system critical points
resource redundancy *(soft)*	is there any redundant (backup) resources assigned or allocated for a critical task/mission?	set of terms (e.g. "no backup solutions", "some services have backup solutions", "critical services have backup solutions", "all services have backup solutions")

Table 2: low-level security metrics

Similar work shall be possible in the continuation of activities to define the components of F_A and F_M based on controls and metrics.

Multiple metrics applied together to a scenario by statistician researchers can provide an accurate assessment to the military commander for mission assurance. From a commander's point of view, the challenge is the deployability of the network not the static operation itself and for this reason the information security variables (e.g. vulnerabilities, compromised devices) are not transferred into security metrics in this particular case. What is becoming a possible further avenue of research activity is how these security metrics can be mixed with the indicators defined for the overall military operation. Similarities with this reasoning are implied in the study of the Operation Assessment concept defined by US JDN 1-15 [Div15] as "a continuous process that supports decision making by measuring the progress toward accomplishing a task, creating a condition, or achieving an objective" where two types of indicators are explained: Measures of Effectiveness (MoEs) and Measures of Performance (MoPs).

5 Aggregating the metrics

In section 4 it is shown how the forces in the MAC triangle can be decomposed into a number of components, that are made observable through a number of metrics. Some of these metrics produce a hard quantitative output, whereas others result in a soft natural language appreciation by a human expert. It is impossible to define the domain knowledge for a real-world complex problem like assessing the performance of security

controls in an exact, mathematical way. The subject matter experts' understanding of the generic rules and constraints, applicable to such a problem, is situated at a qualitative and declarative level, and is typically expressed using vague linguistic terms. This is called a fuzzy level of understanding of the problem. To capture this fuzzy level of understanding we are using fuzzy control statements. These statements associate define for each control a crisp or fuzzy metric and associate with the metric a fuzzy set that describes the expected values for the metric in order for the control to be efficient. The evaluation of a control is then performed through approximate reasoning [Kli95, JSM97].

A classical set is characterized by a clear and unambiguous boundary. Consider a space of objects X; a classical set $A \subseteq X$ can then be defined by its characteristic function $\mu_A(x) : X \to \{0, 1\}$, which defines, for every element $x \in X$, whether it belongs to A ($\mu_A(x) = 1$) or not ($\mu_A(x) = 0$). Classical sets have proven to be an important tool for mathematics, yet do not reflect the fundamentally abstract and imprecise nature of human concepts and thoughts. A fuzzy set is an extension of the classical crisp set, which is not curtailed by a crisp boundary. Its characteristic function, called membership function, maps the elements of X to a membership degree between 0 and 1.

For evaluating the strength of the forces in the MAC triangle using fuzzy metrics and approximate reasoning, we first define the concept of a linguistic metric that is a 5-tuple $(m, M, \mathcal{A}, R, C)$, with:

- m – the name of the metric;
- M – the universe of discourse for that metric;
- $\mathcal{A} = \{A_1, \ldots, A_{N_A}\}$ – the *term set* of m, containing N_A *linguistic values* or *terms*, which can be used to describe m;
- R – a semantic rule which associates with every linguistic value $A_j \in \mathcal{A}$ a meaning in the form of a membership function $\mu_{A_j}(m)$;
- C – the context in which these linguistic terms are applicable.

Each component of a force F shall be defined by a number of linguistic metrics m_i. The evaluation of a metric for a specific situation is performed by evaluating the degree of consistency for the corresponding control clause C_i:

$$C_i : m_i \text{ is } A_{i,C} \tag{1}$$

with $A_{i,C} \in \mathcal{A}_i$ the fuzzy term that expresses the typical values this specific metric should have in order to ensure security.

Let us as an example consider the following metrics:

- The hard crisp metric m_1' represents the average time to handle an incident based on historic measurements. The universe of discourse M_1 for this metric ranges from 0 to ∞. The term set $\mathcal{A}_1$ consists of a single fuzzy term $A_{1,C}$, shown in figure 8, that expresses a subject matter expert's opinion of how acceptable a given value for the average time is for a secure system. The context C of this metric and the associated fuzzy terms is a deployed operational network.

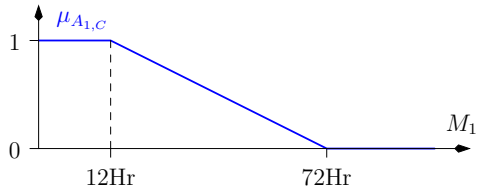


Figure 8: fuzzy term set $\mathcal{A}_1$

- The soft metric m_2 represents the training level of the staff for re-active cyber-operations. The universe of discourse for m_2 covers values from 0, meaning "no training at all", to 1, meaning "fully trained". These values are however not measurable as such. The appreciation of the level of re-active cyber-training of a given military unit will be expressed by a human expert using the pre-defined terms "substandard" ($A_{2,1}$), "average" ($A_{2,2}$), "good level" ($A_{2,3}$), or "expert level" ($A_{2,4}$). The term set $\mathcal{A}_2$ furthermore contains the term $A_{2,C}$ that expresses to what degree a certain training level can be considered sufficient for belonging to the set of secure systems. The membership functions for these fuzzy terms are shown in figure 9. The context for m_2 is identical to the one for m_1.

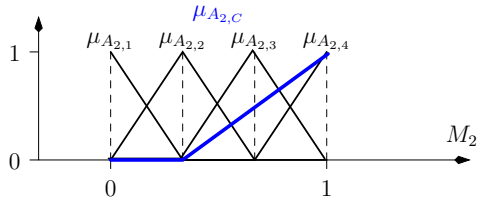


Figure 9: fuzzy term set $\mathcal{A}_2$

The observed facts for the metrics consist of a vector $\overline{\hat{m}}$ with values values $\hat{m}_i$, to be assigned to the variables m_i. The values $\hat{m}_i$ can be fuzzy, characterized by a membership function $\mu_{\hat{m}_i}(m_i)$, or crisp, in which case they will be noted $\hat{m}'_i$. For the moment, we will consider fuzzy facts since crisp values are only a special case of fuzzy values.

The crisp degree of consistency c'_i between a fuzzy metric fact $\hat{m}_i$ and the corresponding fuzzy term A_{Ci} is computed as the height of the intersection of both fuzzy sets:

$$c'_i = \text{height}\left(\hat{m}_i \cap A_{i,C}\right) \tag{2}$$

$$= \sup_{m_i \in M_i} \min\left[\mu_{\hat{m}_i}(m_i), \mu_{A_{i,C}}(m_i)\right] \tag{3}$$

To continue the example of the metrics m_1 and m_2, introduced above, let us consider the following observed values:

- $\hat{m}'_1$ has been computed over the past year and a resulting value of 24Hr was obtained. Applying equation (3) for the crisp $\hat{m}_1$ results in a degree of consistency c'_1 of 0.7, as is shown in figure 10.

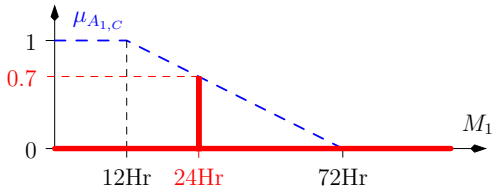


Figure 10: computing c'_1

- $\hat{m}_2$ has been qualified by an expert as "average". Applying again equation (3), a degree of consistency c'_2 of 0.3 is obtained, as is shown in figure 11.

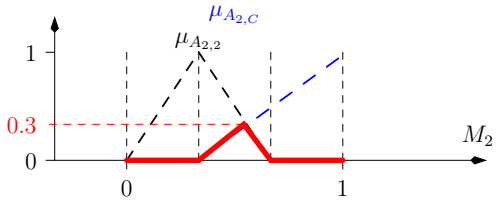


Figure 11: computing c'_2

When one wants to combine information originating from different sources, one needs to aggregate the outputs these sources produce. This is also the case here where different metrics, or more specifically the degrees of consistency c'_i between the observed fuzzy value and the reference fuzzy term for each of the metrics, need to be combined into a single value for a given component of a force.

When a T-norm (for instance implemented using the min() operator) is used as aggregation operator, the "and-ing" allows for no compensation of a single malfunctioning control by other better performing controls. On the other hand, when an S-norm is used (for instance implemented using the max() operator), the "or-ing" would allow a single good security control to maximize the resulting force component.

It is clear that the desired aggregation operator must be situated somewhere in between these two extremes. For that reason, Yager introduced a new aggregation operator, called the "Ordered Weighted Averaging" (OWA) operator [Yag88]. It behaves like a combination of "and-ing" and "or-ing", with a degree of either that can be easily adjusted.

For a force with n components, the aggregated strength is determined by an OWA operator G of dimension n. For an argument n-tuple $C = (c'_1, \ldots, c'_n)$ containing the crisp degrees of consistency for the individual components, the aggregated output is defined as follows:

$$G : [0,1]^n \to [0,1] : \quad G(c'_1, \ldots, c'_n) = w'_1 \; v'_1 + \ldots + w'_n \; v'_n \tag{4}$$

with the crisp order argument vector $V = (v'_1, \ldots, v'_n)$, derived from C, such that

$$v_i \geq v_j \quad \text{if} \quad j > i \tag{5}$$

and with the weighting vector $W = (w'_1, \ldots, w'_n)$, such that

$$\forall i : \quad w'_i \in [0, 1] \tag{6}$$

and

$$\sum_{i=1}^{n} w'_i = 1 \tag{7}$$

The choice of the weights is part of the domain knowledge that is to be provided by the subject matter expert.

In the case of our example with two metrics m_1 and m_2, the order argument vector becomes $V = (0.7, 0.3)$. Let us consider some possible weight vectors:

- $W = (1, 0) \rightarrow G = 0.7$
  This choice of weights corresponds with the maximum operator. It is not a suitable choice since the lower score of 0.3 for the incident handling training level should be taken into account when computing the overall strength of the corresponding component of the force F_C. Indeed, even if incidents are handled rather rapidly, some effects may not be detected and remain hidden due to insufficient expertise.

- $W = (0, 1) \rightarrow G = 0.3$
  These weights lead to a minimum operator for the aggregation. This is clearly too pessimistic since the rapid event handling is still reassuring even if the training level is only considered to be "average".

- $W = (0.3, 0.7) \rightarrow G \approx 0.4$
  This is a conservative choice for the weighting vector, that is probably a good choice to start with. Indeed, the weakest control metric is given a higher weight since it is after all the weakest link in the protection that may be the cause of an incident. Nevertheless the other score is given a certain weight as well since a well developed second security control will still produce a better overall protection than a bad one.

Figure 12 shows the complete processing from observed metrics to an aggregated component strength. The domain knowledge, provided by subject matter experts, is introduced into this project in the following ways:

- the choice of the metrics.

- the term set $\mathcal{A}$ for each of the metrics, which defines a term A_C that expresses to what extent the values of the universe of discourse indicate a secure system. For a fuzzy metric the terms set furthermore specifies the terms A_k that will be used to describe the value of the metric for a given system by a human expert.

- the weight vector W used for the OWA aggregation.

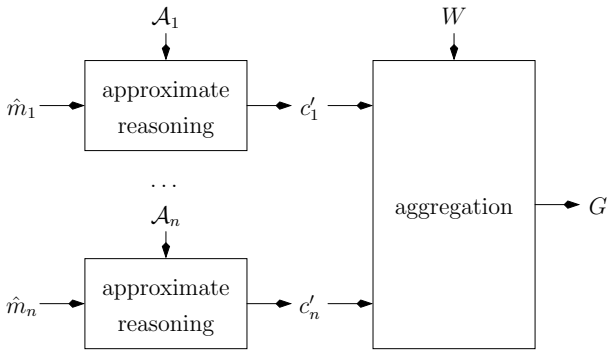


Figure 12: domain knowledge overview

6 Conclusions

This research describes a novel approach for visualising the cyber operational picture in order to improve situation awareness and facilitate the decision-making process. Based on mission-specific characteristics, a multi-modal and multi-level 3D representation is presented that aims to provide, at a simple glance, a baseline assessment of the cyber-situation.

The first view is a 3D visualization that encodes the most important high-level information in an intuitive way, making it possible to easily identify the assets that require a more in-depth analysis. The second level view consists of the "Mission-Attacker-Controls" triangle that depicts for every asset the mission critical aspects in the form of generic forces with a magnitude that is determined by the aggregation of a number of domain-specific low-level metrics.

Finally, the selection and applicability of these low-level metrics was addressed in this paper and some concrete examples were given, followed by an approximate reasoning approach for evaluating and aggregating the metrics using a priori defined domain knowledge. The proposed approach makes it possible to perform a dynamic assessment as the situation evolves based on a real-time feed for the rapidly evolving metrics, for instance by subscribing to information from an external command and control systems. It is also of great interest to analyse the applicability of the "operation assessment framework" within this context.

Finally, the authors realize the practicality principle that must guide the design of solutions to achieve cyber situation awareness and the complexity it entails to put into practice a set of tools to aid military commanders and their staff when they are identifying the course of action that best fulfils a given mission. The scenario can incorporate several missions concurrently. In this case, planners must develop a mission profile that combines capabilities and cyber assets within the 3D overview.

The security controls referred as pro-active, re-active and continuity are quantified by using a group of associated security metrics. Once these mathematical elements are defined, a technical staff can conduct an analysis of which mitigation actions or countermeasures produce better results to reduce the risk to the mission. This kind

of analysis can be performed using the 3D views. The controls regarding the mission received - to restore order in a town in the example of this paper - bring the opportunity to select associated variables and security metrics for cyber deployable assets. Enemy capabilities to disrupt C2, composition of the task force unit in individual vehicles or dismounted patrols, air support to operations and some others are considered as mission relevant elements for planners that may have an impact on the mission. These mission elements are reliant on the network functionalities for mission accomplishment.

References

[Bro] Krag Brotby. Appendix a: Sabsa business attributes and metrics. *Information Security Governance: A Practical Development and Implementation Approach*, pages 163–179.

[CDL+14] Yi Cheng, Julia Deng, Jason Li, Scott A DeLoach, Anoop Singhal, and Xinming Ou. Metrics of security. In *Cyber Defense and Situational Awareness*, pages 263–295. Springer, 2014.

[Div15] Joint Doctrine Analysis Division. Operation assessment. Technical Report 1-15, Joint Doctrine Note, 2015.

[Hec08] Artur Hecker. On system security metrics and the definition approaches. In *2008 Second International Conference on Emerging Security Information, Systems and Technologies*, 2008.

[Jan10] Wayne Jansen. *Directions in security metrics research*. Diane Publishing, 2010.

[JSM97] Jyh-Shing Roger Jang, Chuen-Tsai Sun, and Eiji Mizutani. *Neuro-Fuzzy and Soft Computing*. Matlab Curriculum Series. Prentice Hall, Upper Saddle River, NJ (USA), 1997.

[Kli95] George J. Klir. *Fuzzy Sets and Fuzzy Logic: Theory and Applications*. Prentice Hall, Upper Saddle River, NJ (USA), 1995.

[MD15] Wim Mees and Thibault Debatty. An attempt at defining cyberdefense situation awareness in the context of command & control. In *Military Communications and Information Systems (ICMCIS), 2015 International Conference on*, pages 1–9. IEEE, 2015.

[NIS03a] NIST. 800-53, recommended security controls for federal information systems. 2003.

[NIS03b] NIST. 800-55, security metrics guide for information technology systems. 2003.

[TS10] George P Tadda and John S Salerno. Overview of cyber situation awareness. In *Cyber situational awareness*, pages 15–35. Springer, 2010.

[Yag88] Ronald R. Yager. On ordered weighted averaging aggegration operators in multicriteria decisionmaking. 18:183–190, 1988.