An attempt at defining Cyberdefense Situation Awareness in the context of Command & Control

Wim Mees and Thibault Debatty
Royal Military Academy
Brussels, Belgium
Email: wim.mees@rma.ac.be

***Abstract*—In this paper we present an overview of the most important views on situation awareness in literature. We then go on to apply these concepts to cyberdefense.**

The main contribution of the paper lies in bringing together different decision making models and proposing a unified cyberdefense situation awareness model, that covers the different levels of abstraction from raw data to understanding, as well as the different topics that are relevant for building situation awareness.

I. Introduction

Accurate situation awareness is essential for decision making in all military command & control situations. cyberdefense is not different in that respect. Achieving a sufficient level of situation awareness remains however a major challenge, as well in kinetic warfare as in cyber operations.

In section II we present a brief bibliography on situation awareness, followed by an application of the concept of situation awareness to cyberspace in section III. As we will show, cyberdefense situation awareness (CDSA) as a stand-alone concept is not very useful. It is always strongly coupled with other aspects of the global situation awareness of the military commander and his staff. As CDSA is however a widely adopted term, we will use it as well but define it as "the cyberdefense part of the global situation awareness".

We will bring together the most important decision making models and propose a reference for CDSA with respect to Boyd's OODA loop, Endsley's decision making model and the cognitive hierarchy on the one hand, and the different topical components of the operation picture on the other.

II. Situation awareness

In a military environment, decision making is most often studied in the context of command & control. A typical operational-level command & control process is the *operational planning process* (OPP), shown in figure 1.

The OPP is an iterative process with an orientation phase, consisting of an analysis of the mission by the commander and his staff, that is followed by a concept development phase, where a number of *"courses of action"* (COA) are identified by the staff and the most appropriate one is selected by the commander. Developing a COA requires accurate situation awareness about the environment, about friendly forces as well as about the opposing forces, and finally the ability to project into the future the inter-dependent, possible and most probable actions of both sides. The final step consists in transforming the selected concept of operations into an operational plan.

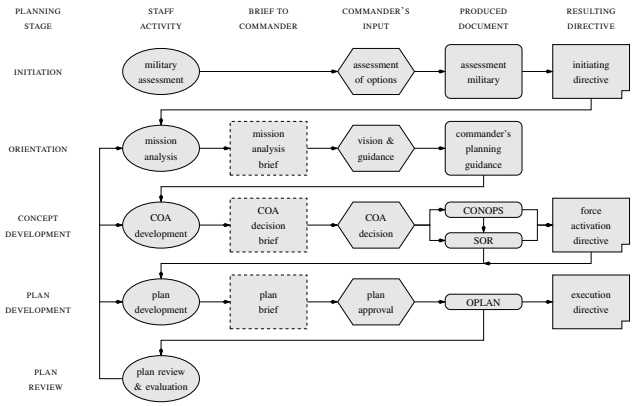

Fig. 1. The operational planning process

At a tactical level, an interesting model for representing the decision making process is Boyd's *"observe - orient - decide - act"* (OODA) loop [1], shown in figure 2.

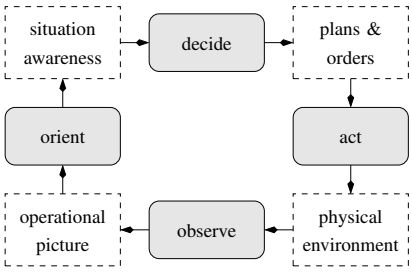

Fig. 2. The observe - orient - decide - act loop

The *"observe"* process of the OODA loop acquires data and information about the environment, and produces an *"operational picture"* (OP). The *"orient"* process in turn interprets the situation depicted in the operational picture and produces *"situation awareness"* (SA). Boyd emphasized the fact that this SA results from many-sided, implicit cross-referencing projections, empathies, correlations, and rejections, and is furthermore shaped by the interplay of genetic heritage, cul-

tural tradition, previous experiences, unfolding circumstances, etc. The *"decide"* process identifies the possible courses of action, selects the most appropriate one based on the SA, and translates it into a set of *"plans and orders"*. Finally, the *"act"* step consists of applying the decision through an interaction with the *"physical environment"*.

When different entities operate in a combined operation, it is important to coordinate, or at least de-conflict, their command & control processes. This requires a *"common operational picture"* (COP), which Conti et al [2] define based on the US military doctrine [3] as "a single identical display of relevant information shared by more than one command that facilitates collaborative planning and assists all echelons to achieve situation awareness." Based on the same reference they define SA as "the requisite current and predictive knowledge of the environment upon which operations depend – including physical, virtual, and human domains – as well as all factors, activities, and events of friendly and adversary forces across the spectrum of conflict." What is particularly interesting about these definitions is the clear link with the cognitive hierarchy [4], with the positioning of the OP at the *information* level on the one hand and the SA at the *knowledge* level within this hierarchy at the other.

A number of definitions of situation awareness can be found in the literature. Cumiford for instance defines SA in a generic way as "the ability to rapidly and effectively address incoming stimuli with appropriate responses" [5], which corresponds with the course of action development and selection of the OPP, and is indeed on the edge between the orient and the decide stages of the OODA loop. Rousseau et al on the other hand state that for most researchers and practitioners SA means "a body of knowledge together with a set of processes for developing and updating that knowledge" [6]. Again SA is clearly situated at the knowledge level of the cognitive hierarchy.

One of the most widely accepted definitions for situation awareness is the more specific one by Endsley: "the perception of elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future." [7]. Endsley's work initially

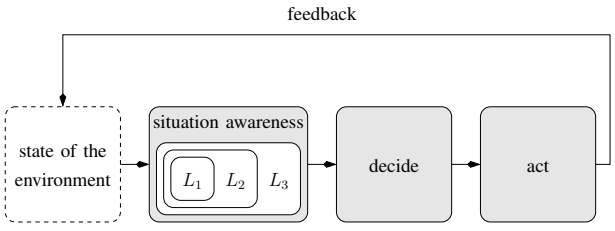

Fig. 3. Endsley's decision making model

focused on avoiding loss of SA by aircraft pilots, so it comes as no surprise that her decision making model, shown in figure 3, consists of a loop that is similar to the OODA loop. The model makes no distinction between OP and SA, but rather captures everything in a single SA entity. Within this single entity however three levels of situation awareness are defined [8], with the results of the higher levels depending on the success of achieving the lower ones. Level 1 SA, called *"perception"*, is the direct equivalent of the OODA observe process, while level 2 SA, called *"understanding"*, corresponds with the OODA orient process. Level 3 SA, called *"projection"*, however, has no direct equivalent in the OODA loop. It can be considered as a combination of the higher level knowledge produced by the orient process, that makes it possible to project into the future, and the COA development that is part of the decide process.

Cumiford [5] identifies the same three levels of SA as Endsley, and stresses the fact that the appropriateness of a COA depends on its success in accomplishing a given goal. He furthermore emphasizes the importance of the notion of time for situation awareness. It is important to know the time at which events occur in the environment, in order to identify for instance sequences, trends, simultaneous or overlapping events, as well as to for instance take into account deadlines. Cumiford finally also addresses the importance of selective attention. The SA must make it possible to direct the focus of the orientation and of the planning processes in order to dynamically respond to changes in the environment in a timely fashion.

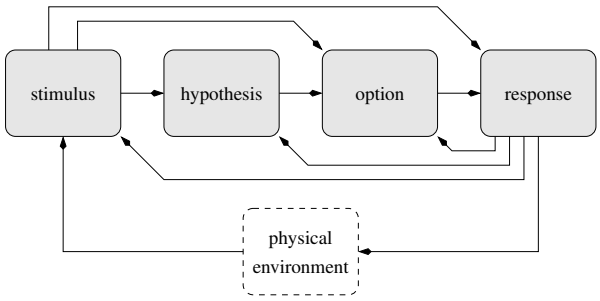

Fig. 4. Wohl's stimulus - hypothesis - option - response model

Another decision-making model is Wohl's *"stimulus - hypothesis - option - response"* (SHOR) model [9], shown in figure 4. In the *"stimulus"* step data is gathered, filtered, correlated, and aggregated. This step can therefore be considered as the equivalent of the "observe" step of the OODA loop together with a first part of the "orient" process. In the *"hypothesis"* step, hypotheses are created, evaluated and then selected or rejected, which corresponds with the higher stages of the OODA "orient" process. The *"option"* step consists of identifying possible response options, evaluating them and finally selecting the one to be adopted. The last step is the *"response"* step which consists of preparing plans, organizing the operations and executing them. This would be the "act" step of the OODA loop. A number of authors have criticized the OODA model for lacking a *"planning"* step [10]. The SHOR model answers this concern since it clearly distinguishes hypothesis development and evaluation for building situation awareness on the one hand and "option" or "course of action" identification and evaluation to prepare the decision making process on the other. McGuinness et al extend in the same way Endsley's model by adding an explicit "resolution" level that addresses selecting the best path to follow in order to achieve the desired outcome [11].

In Endsley's view, situation awareness is achieved using *"mental models"*, illustrated in figure 5, and defined by Rouse and Morris as "mechanisms whereby humans are able to generate descriptions of system purpose and form, explanations of system functioning and observed system states, and predictions

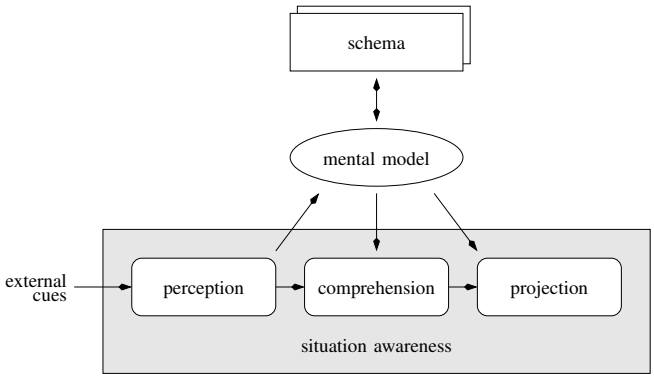

Fig. 5. Mental model and schema

of future states" [12]. These mental models are built ad hoc by activating one or more *"schemata"*, which are prototypical states of mental models, that make it possible to easily match a perceived situation with a number of well-known and recognized classes of situations, preloaded in memory, and as a result provide comprehension and projection as a single step. Endsley furthermore defines the notion of *"scripts"* associated with a schema, which are predefined sequences of actions that define what to do in the cases that are represented by the schema, and therefore allow for very rapid decision making.

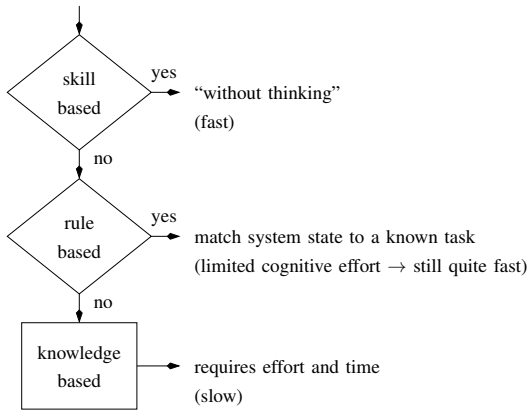

Fig. 6. Rasmussen's three-level model

This combination of rapid, short-cut based decision making when available, and more resource intensive, model-based reasoning when required, is reflected in Rasmussen's three-level model [13], illustrated in figure 6. According to this model, a decision maker first tries to identify signals in the data that enable him to take action at the lowest, *"skill-based"* level of reasoning, almost "without thinking". If this skill-based solution fails, the decision maker will apply a *"rule-based"* reasoning, trying to match the system state to a known task that he can execute. This requires a limited cognitive effort, yet is still quite fast and fits well in the military *"tactics, techniques and procedures"* (TTP) approach. If rule-based reasoning fails, for instance when there is no template that matches the current situation, the decision maker will have to proceed with a purely *"knowledge-based"* reasoning approach, which requires more effort and time.

It is often assumed that decision makers make purely rational decisions. In practice however, researchers have observed that expert decision makers tend to reject decision support systems that enforce a purely rational decision making based approach upon them. This resulted in a research field called *"naturalistic decision making"* (NDM). Klein [14] proposed the *"recognition-primed decision model"* (RPD) to describe the way in which human experts use their experience of previous incidents to match every new situation with a previous prototype, that is then associated with a preferred course of action. This corresponds with Endsley's "schema" and Rasmussen's "rule-based" approach. Klein furthermore ties the notions of goals, cue salience, expectations, and the identification of typical actions to SA.

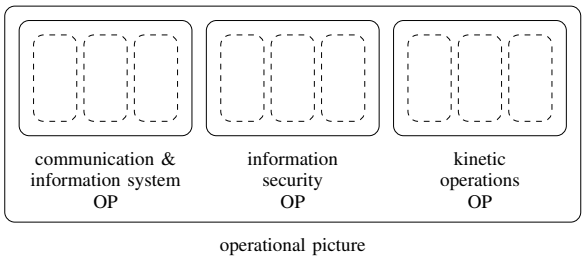

Fig. 7. Cyberdefense part of the operational picture

III. Cyberdefense situation awareness (CDSA)

In the 1990s, command posts at all levels switched from physical maps and acetate overlays to computerized displays, that have since then evolved into state-of-the-art digital multi-echelon command & control systems. These systems have traditionally revolved around physical and material assets and reconnaissance and now need to be adapted to incorporate cyber command and control tasks, resources, and requirements [15], and this change has not yet been achieved [2]. Computer network and information service monitoring does already occur in government and industry *"network operation centres"* (NOC), that nowadays evolve into or are complemented by *"cyber security operations centres"* (CSOC). These NOCs or CSOCs possess however only limited physical domain awareness, and are primarily defensive, lacking offensive operational planning capabilities [2].

Current day NOCs and CSOCs focus mainly on a dynamically updated technical description of networks and systems, their real-time status, as well as information about known hostile activities. As was shown in section II, this is not sufficient for supporting the planning and decision making process. Indeed, this information is rather situated at the level of the OP and must therefore first be interpreted in the context of the mission as well as the current institutional, political, social, and behavioural situation in order to achieve SA [5]. An example hereof is the recent *"Situational Awareness of Critical Infrastructure and Networks"* (SACIN) framework [16], that aims at developing a COP and leaves the development of higher-level CDSA from the COP to the human analysts.

Figure 7 shows the main components of the OP that are required as input for the "orient" process in order to achieve an adequate cyberdefense component of the SA, which we will hereafter refer to as CDSA. Figure 8 shows some of the elements that are part of the *"communication & information system"* (CIS) part of the OP. Current day network

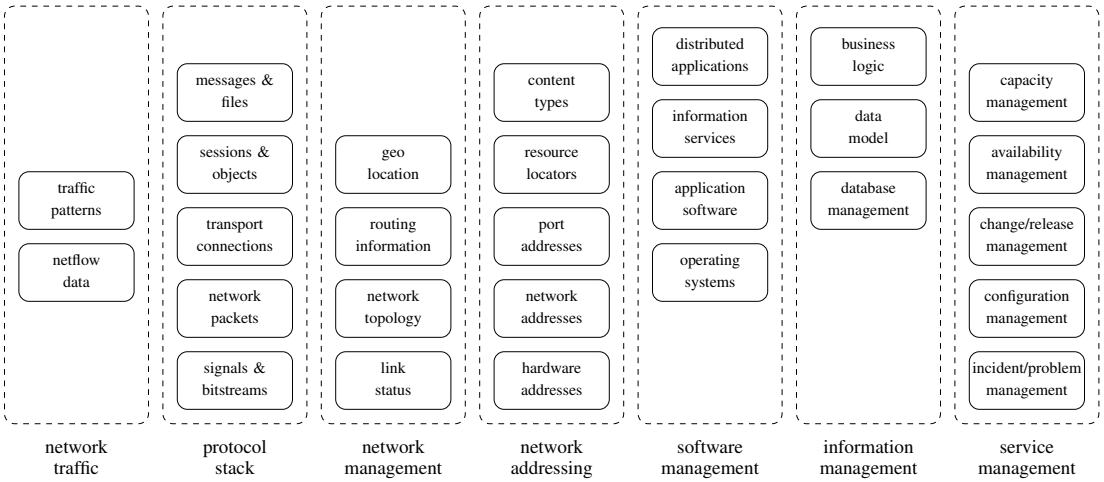

Fig. 8. Communication & information system part of the operational picture

topologies evolve rapidly over time, hosts are frequently added or removed, software configurations change, etc. Especially in a military operational context, where we have federated mission networks, combined with converged mobile tactical networks, built up of low-bandwidth, high-latency, intermittent links, the CIS part of the OP will evolve constantly. Yet the accurateness of this information is essential for understanding the current situation, its impact on the mission and projecting the evolution of this impact into the future. Therefore it should be updated automatically as much as possible. The types of information that will be part of the CIS OP obviously depend on the organization and its mission. The elements depicted in 8 are just meant to illustrate the levels of abstraction at which information is considered for the OP, they are certainly not a complete catalogue of possible categories.

Figure 9 shows some elements of the *"information security"* (INFOSEC) part of the OP. In the area of risk management, new vulnerabilities are frequently discovered, attackers' capabilities and strategies evolve, and therefore automatic updating is required here as well. This can be realized in part by subscribing to publicly available catalogues like the *"Common Attack Pattern Enumeration and Classification"* (CAPEC) [17].

Where intrusion detection is concerned, it should be noted that an *"Intrusion Detection System"* (IDS) is a sensor that only identifies an event that may be part of an attack. It does not recognize the attack [18] itself. The events and alerts that are generated by active network components, hosts, and security controls, are often uncertain or incorrect. It is therefore important to be aware of the quality of the collected information, which can for instance reflect the truthfulness, trustworthiness, completeness, and freshness of that information, and to track this meta-information attribute when processing the information into higher-level knowledge [18]. An example hereof is for instance the use of attack graphs in combination with Bayesian networks [19], [20], or the use of Dempster-Shafer evidence theory [21].

Given furthermore the large numbers in which security events are generated, solutions are needed for efficiently filtering and aggregating them [22]. It is also one of the findings of the NATO cyberdefense exercise *"Locked Shields 2012"* that a human beings alone, acting without the support of intelligent software, cannot possibly process the massive amounts of events that are produced in a real-world setting [23].

When considering insider threat, traditional approaches for anomaly detection produce even higher false positive rates. Indeed, insiders have more opportunities and accessible resources than outside attackers, such as legitimate accounts with authorized access to target systems, more extensive knowledge of the network environment, etc. Regular users on the other hand are not always at expert level, and their actions may not always be optimal and rational [24], making it very difficult to distinguish innocent from malicious activities.

In practice, the aggregation of events and alerts is often based on a priori defined attack plans, expert knowledge about the monitored networks, etc., and is therefore prone to obsolescence and error. For this reason novel solutions are needed that do not require a priori knowledge about a given network architecture or rely on static attack templates [25].

Deriving qualified risks from identified threats requires associating a value with each information asset, which is a complex task due to the asset's intangible qualities [26]. In a military context the intangible value of information most often far exceeds its tangible economic value. A coarse first estimate is typically available in the form of the asset's classification level, but this still needs to be matched with the impact on the specific mission [27].

When offensive capabilities are available, the goal will be to deliver precision effects. Cyberspace operations can create cross-domain effects of the D-family type (deter, deny, disrupt, deceive, dissuade, degrade, destroy, and defeat), that extend beyond the traditional warfighting domains of land, sea, air, space, and can include for instance diplomatic or economic effects. Measuring the precise effect of a cyber operation still relies to a large extent on an analyst's intuitive estimate, that depends in large part on his experience and expertise [28]. There is furthermore the risk of cyber fratricide, due to the stragegic blindspot caused by the fact that an area of operation is incomplete and ineffectual in cyberspace [29], which is why the "geo location" component in the CIS COP is important.

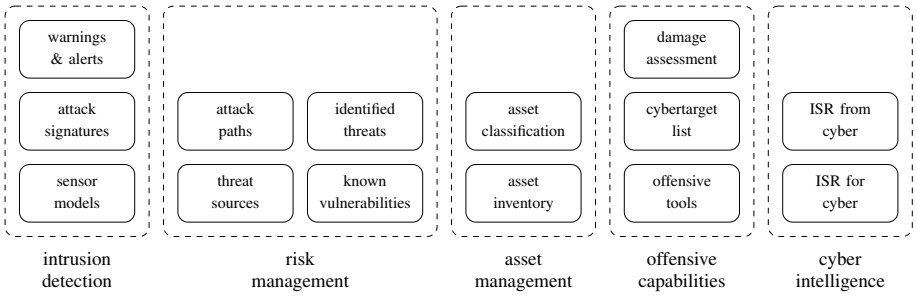

Fig. 9. Information security part of the operational picture

Another part of the INFOSEC part of the OP is the information obtained from *"Intelligence, Surveillance, and Reconnaissance"* (ISR) activities. Here we need to distinguish "ISR *from* cyber", where information is obtained by combing cyberspace for any information of intelligence value that is available, be it on an adversary's network or as open source, from "ISR *for* cyber" which is all-source intelligence required for the planning and execution of cyberspace operations [30].

The kinetic operations part of the OP will not be discussed here. A very complete and detailed data model is available in the *"Joint Consultation, Command & Control Information Exchange Data Model"* (JC3IEDM) that is used by the *"Multilateral Interoperability Programme"* (MIP) [31]. It is for instance in the context of CDSA important to know which signals units provide which parts of the circuits, networks, or services in an operation, as well as which clients depend on which network and information system services. It is also important to know which changes or movements by providers or clients have been planned, which missions the clients are involved in, and how important their role is in the global concept of operations, since this information is required for maintaining a relevant, dynamic, and mission-specific set of qualified risks, that are to be addresses by the decision making process.

Figure 10 shows an attempt at uniting Boyd's OODA loop model and Endsley's decision making model, incorporating the by a number of authors suggested improvement of a separate planning stage. On the left a map of the CDSA is drawn. We have followed Endsley's approach of having the CDSA cover the entire range from the low-level raw data acquisition processes up to the synthesis of a deeper understanding of the cyber aspects of the operation. We do however still distinguish within that SA the elements that make up the OP since this will typically be that information that is managed and exchanged by the already existing NOCs or CSOCs, as well by the existing operational Command & Control Information Systems (CCIS). Three different information flows are indicated by numbered arrows in figure 10:

(1) Information enters the CDSA at different levels of the cognitive hierarchy. At the lowest levels it is for instance raw sensor data, like netflow data or firewall logs, a level higher it can be processed information that is exchanged between friendly forces in the context of a COP, while at the highest levels it can consist of operational or strategic intelligence reports.

(2) A lot of information enters the CDSA, much of which is volatile and only relevant for a short period of time and can thereafter be "forgotten". The part that is relevant for a longer period of time migrates from the "volatile" to the "persistent" part of the CDSA.

(3) The ultimate goal of developing CDSA is to support the decision making process by making it possible in the planning stage to identify and evaluate COAs. It is therefore important to process the lower levels into higher level CDSA, be it through the "manual labour" of human analysts or through automated processing, using signal processing, pattern recognition, correlation and aggregation, information fusion, artificial intelligence, security analytics, ...

Paul et al [32] studied the mental models of cybersecurity analysts responsible for large networks and produced a taxonomy that is useful for CDSA tool development. Because the analysts were only responsible for intrusion detection related activities, the taxonomy is mainly focused on that area:

- *event detection:* matches the observe process of the OODA loop and produces "information" level events in the OP. Three aspects play a role in event detection:
  - network baseline: a model of the normal network behaviour,
  - change detection: compare states of the network to identify differences and trends,
  - network activity: the shift from "normal" to "abnormal" network activity triggers the start of a focused in-depth analysis.
- *event orientation:* matches the orient process of the OODA loop, producing insight into an identified event, in other words the higher levels of CDSA that make it possible to predict what will most probably happen during the wargaming activity that is part of COA development. This typically involves the following activities:
  - identification: detailed analysis of an event to identify who, what, when, where, and why and attack is occurring, possibly linking it to similar events in the past,
  - mission impact: judge the severity of the impact of the event on operations in order to prioritize the incident response,
  - damage assessment: understand the full effect of the event on the internal network and sys-

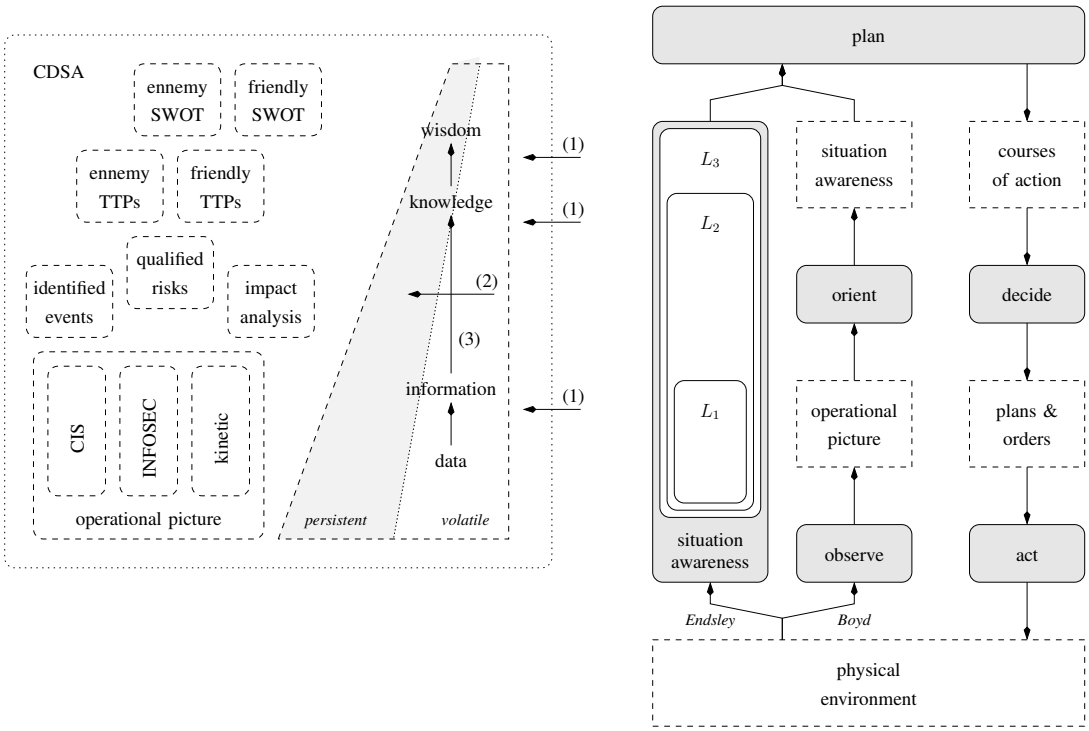

Fig. 10. The cognitive hierarchy and CDSA in the context of the decision making loop

tems.

One aspect of building the higher levels of understanding of the CDSA consists of analysing known vulnerability dependencies for a given network configuration and developing possible attack paths into this network [33]. Jajodia et al developed such a "topological vulnerability analysis" approach [34] and identified the need for aggregating attack graphs at higher levels of abstraction to aid interpretation by the analyst. In [35] they present Cauldron, an integrated framework for automated attack modelling using multi-step network vulnerability paths, intrusion alert correlation with the vulnerability paths, mission impact analysis, and attack mitigation based on mission workflow. Godefroy et al try to automatically derive correlation rules from attack scenario specifications and a knowledge base with the system cartography and with sensor information [36]. Another approach by Yang et al [37] uses high-level information fusion for building network specific information exposure graphs, enabling contextual reasoning and situation assessment that can be used for COA development.

These developments aim at partially automating the higher levels of the CDSA, building knowledge and wisdom that make it possible to develop and assess possible courses of action during the planning phase in figure 10. This will make it possible to - using Boyd's representation of the decision making challenge - loop faster through the decision loop than the opponent, as a result to have the initiative, and in the end to win the battle.

In order to allow for situation tracking, part of the CDSA is persistent and another part is volatile and changes with every iteration of the loop, as is depicited in figure 10. This situation tracking makes it possible to be aware of adversary behaviour within a situation rather than just being aware of the situation itself. This part of the CDSA is called *"situation comprehension"* by Barford at al [18], and also includes being aware of what lead to the current situation, which includes causality analysis (via back-tracking) and forensics.

At the highest level of the CDSA is a deeper understanding or wisdom about the friendly and enemy *"Tactics, Techniques, and Procedures"* (TTP), and from these an assessment of the *"Strengths, Weaknesses, Opportunities and Threats"* (SWOT) for both sides.

The CDSA must also be able to represent cyber battle damage assessment of self and friendly systems, as well as of enemy systems [5].

The upstream processing on the left-hand side of the loop can be partially automated, especially at the lower levels of the SA. The decision part on the right-hand side of the loop however is currently a purely human responsibility.

Because of the speed at which events unfold in cyberspace, it is in practice difficult for the CDSA building process to keep up with the tempo of the operations [5]. Howes [38] shows in this context that a hierarchical organization of decision making, relying on situation reports going up the chain of command for decision making and then orders coming back down the chain of command to implement these decisions, does not work well for cyberdefense because incidents take place in the seconds to minutes range whereas kinetic warfare battles occur in the hours to days range. Liu et al [39] therefore propose a *"cyber-physical-social system"* (CPSS) based solution, using a "chaotic control mechanism" to achieve self-synchronization. They replace a centralized command & control by a distributed command & control organization that is both self-organizing and self-adaptive in response to changes in the battlefield,

focusing in this way on the harmony of a system of systems.

A number of authors claim that the speed at which decisions and actions are required in cyberspace is such that it simply requires automated solutions [2]. Unfortunately the complexity of the real-world interconnected information systems is such that automated decisions will in the near future be limited to very specific, well-defined threats, similar to the kinetic world automated terminal defense systems against anti-ship missiles like the Phalanx or the Goalkeeper [40], that address very specific threats in the physical world. The Canadian ARMOUR Technology Demonstration Project (TDP) is an example of an ongoing research effort to develop fully automated Computer Network Defence (CND) capabilities for a wider range of cyber threats [41]. There will nevertheless still be an important role for loosely interacting teams of humans and computers[18], and solutions will be needed for establishing team-CDSA in such mixed teams of humans and computers [42]. Computers and humans must then also have a shared understanding of the goals so they can identify the optimum set of tasks that lead to achieving these goals. This requires that the mental models of the human analysts and the computer models used by the computers represent the same or at least compatible cognitive models [43]. Haack et al present a mixed-initiative hierarchical framework of humans and software agents, in which the software agents share the decision-making power with the humans, handling most of the real-time decisions autonomously but enabling human involvement at all levels [44]. In order to train these mixed teams, simulators that combine the kinetic and the cyber environments offer interesting opportunities [45].

Indeed, from the work of Hayden [46], Cumiford [5] derives the need for building discernment and an associated spontaneity into the reasoning capability of a CDSA system. Hayden emphasizes that complex systems such as that of terrorism exhibit emergence, meaning that system properties cannot be predicted a priori and that the cause and effect relationships only become evident in retrospect. Therefore, traditional reasoning, purely based on templates, schema, or frames in the traditional sense, would result in a fairly low quality of SA. The system would always be a few steps behind the curve, since it would not be able to predict or respond to novel situations. This type of reasoning could at best be used as a starting point for a human analyst determining an appropriate response but would not be sufficient in itself, especially in cyberspace where threats and countermeasures are unpredictable and evolve very rapidly.

One should furthermore not forget that there is an intrinsic link with the traditional kinetic operations. Indeed, the CDSA is on the one hand used for managing the cyber operations, but is on the other hand also essential for providing information system support to the physical counterpart [5]. Knowledge about the dependencies between cyber assets, their users and missions is indispensable to assess the impact of cyber attacks. There is however no systematic method for mapping these relationships. Furthermore, knowledge of these same dependencies is also required for staff officers and commanders to understand which cyber assets are critical to the execution of their operations [47]. Developing a solution for modelling these dependencies and automatically populating the model from commonly available network data sources, is precisely the goal of the *"Cyber Assets, Missions and USers"* (CAMUS) project [48].

At the highest levels of CDSA, where the human analyst is the main actor, appropriate visualizations can also play an important role in establishing the link between the physical operations and the cyber situation, as is illustrated by the geographic approach for representing security data, presented by Angelini et al [49], the STARMINE system by Hideshima et al [50] which integrates a geographical, temporal, and logical view of the cyber threat in 3D space, the *"Visual Analytics Suite for Cyber Security* (VACS) developed by Fischer et al [51] in the context of the *Visual Analytic Representation of Large Datasets for Enhancing Network Security"* (VIS-SENSE) project, or the SemanticPrism system from Chen et al [52]. Other visualizations target the more abstract aspects of the CDSA, like the relationships between decision goals, sub-goals, decisions, information requirements, and data sources [53]. The effectiveness of the different visualization solutions in improving CDSA must however still be evaluated using a representative group of human analysts and a set of sufficiently complex and relevant scenarios [54]

Cybersecurity will typically be managed in CSOCs that are distributed across the globe. Situation awareness must therefore be shared not only within a team, but also between teams operating in different operations centres, and must be preserved during shift changes from one team to the next, etc. [55]. It must furthermore be possible to perform truth maintenance [5] in such a shared CDSA environment, in other words to identify the facts that are no longer valid at a given time. This also implies that there must be a traceability in order to retract any inferences or decisions that were derived from these invalid facts.

Finally, CDSA requires a collaborative effort between the public and the private sector. Indeed, although a country certainly has the right to control its borders, including those in cyberspace [56], the government cannot handle cybersecurity all by itself [57]. Information about an attack will for instance first be available to the organization being attacked. Unless the government is itself the target of the attack, a government organization managing cybersecurity will have to rely on information provided by the victim of the attack and feed that into its national situation awareness solution. Unfortunately, the private sector, representing for instance 85% of the critical infrastructure, is often reluctant to share information with the government for fear of regulatory action, lawsuits, or bad press [58]. For that reason some authors urge that a combination of incentives and penalties be put in place that push organizations to put themselves through the necessary forms of examination, like vulnerability assessment and penetration testing, in order to minimize the cyber risk that ultimately affects all citizens [59]. There is furthermore always the risk that the opponent injects fake reports about events that are difficult to verify, which would reduce the CDSA of the defenders [60].

The fact that sharing information between public and private sectors leads to improved situation awareness was confirmed by the findings from the *"Multinational Experiment 7"* (MNE) Cyber Situational Awareness *"Limited Objective Experiment"* (LOE), conducted in 2012 in the UK [61]. They also found that establishing trust was a critical enabler to infor-

mation sharing, but that the participants found many reasons not to share. They finally also concluded that visualisation technology can significantly increase the ability of decision makers to absorb and process the information they receive.

IV. Conclusions

At all levels of command, situation awareness is essential for optimal decision making. When different actors participate in the same operation, it is furthermore essential to coordinate their command & control processes. This is handled by synchronizing information between the different command & control information systems in order to ensure a common operational picture, that will then lead to a shared situation awareness.

With the increasing importance of cyber space as one of the dimensions of the theatre of operations that needs to be addressed by the commander and his staff, the cyberdefense part of their situation awareness becomes increasingly critical for the success of the mission. For that reason we have proposed in this paper a unified model of situation awareness, that combines Boyd's OODA loop with Endsley's decision making model and proposes an all-encompassing situation awareness that contains as its lower level the classic operational picture.

We have positioned cyberdefense situation awareness with respect to the cognitive hierarchy to show how it reaches from low-level data to very abstract understanding and insight, and examined the different types of information that are to be covered, to show how communication & information system information and information security information is to be combined with the classic kinetic operations part of the operational picture.

We have furthermore described how the rapidly changing network and information system situation, together with the speed at which cyber attacks are executed, requires very rapid cycling through the decision loop. This implies that the situation awareness building should be fully or at least to a large extent automated. This remains in practice however still a very big challenge, even though a number of research initiatives are trying to automate to a certain extent the process of creating and maintaining cyberdefense situation awareness, identifying possible defensive countermeasures and selecting the most appropriate one.

We have also shown that a number of problems still need to be resolved related to the situation awareness building, such as the fact that a lot of the information that is received from security devices is incomplete, uncertain, erroneous, etc., and therefore information processing methods need to be adopted that preserve this aspect of the information as it finds its way to the higher levels.

We have finally addressed the combination of automatic processing with a human specialist, as a team that share situation awareness, as well as with respect to the visual interface between the information and the human user.

References

[1] J. R. Boyd, "Organic design for command and control," *A discourse on winning and losing*, 1987.

[2] G. Conti, J. Nelson, and D. Raymond, "Towards a cyber common operating picture," in *Cyber Conflict (CyCon), 2013 5th International Conference on*, pp. 1–17, IEEE, 2013.

[3] D. Dictionary, "Joint publication 1-02, dod dictionary of military and associated terms 08 november 2010, as amended through 15 february 2012."

[4] R. L. Ackoff, "From data to wisdom," *Journal of applied systems analysis*, vol. 16, pp. 3–9, 2010.

[5] L. D. Cumiford, "Situation awareness for cyber defense," tech. rep., DTIC Document, 2006.

[6] R. Rousseau, S. Tremblay, and R. Breton, "Defining and modeling situation awareness: A critical review," *A cognitive approach to situation awareness: Theory and application*, pp. 3–21, 2004.

[7] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors*, vol. 37, no. 1, pp. 32–64, 1995.

[8] M. R. Endsley *et al.*, "Theoretical underpinnings of situation awareness: A critical review," *Situation awareness analysis and measurement*, pp. 3–32, 2000.

[9] J. G. Wohl, "Force management decision requirements for air force tactical command and control," *Systems, Man and Cybernetics, IEEE Transactions on*, vol. 11, no. 9, pp. 618–639, 1981.

[10] T. Grant and B. Kooter, "Comparing ooda & other models as operational view c2 architecture topic: C4isr/c2 architecture," *ICCRTS2005, Jun*, 2005.

[11] B. McGuinness and L. Foy, "A subjective measure of sa: the crew awareness rating scale (cars)," in *Proceedings of the first human performance, situation awareness, and automation conference, Savannah, Georgia*, 2000.

[12] W. B. Rouse and N. M. Morris, "On looking into the black box: Prospects and limits in the search for mental models.," *Psychological bulletin*, vol. 100, no. 3, p. 349, 1986.

[13] J. Rasmussen, "Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models," *Systems, Man and Cybernetics, IEEE Transactions on*, no. 3, pp. 257–266, 1983.

[14] G. A. Klein, *Sources of power: How people make decisions*. MIT press, 1999.

[15] R. F. Erbacher, "Extending command and control infrastructures to cyber warfare assets," in *Systems, Man and Cybernetics, 2005 IEEE International Conference on*, vol. 4, pp. 3331–3337, IEEE, 2005.

[16] J. Timonen, L. Laaperi, L. Rummukainen, S. Puuska, and J. Vankka, "Situational awareness and information collection from critical infrastructure," in *Cyber Conflict (CyCon 2014), 2014 6th International Conference On*, pp. 157–173, IEEE, 2014.

[17] A. Schaeffer-Filho, D. Hutchison, *et al.*, "Attack pattern recognition through correlating cyber situational awareness in computer networks," in *Cyberpatterns*, pp. 125–134, Springer, 2014.

[18] P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning, *et al.*, "Cyber sa: Situational awareness for cyber defense," in *Cyber Situational Awareness*, pp. 3–13, Springer, 2010.

[19] P. Xie, J. H. Li, X. Ou, P. Liu, and R. Levy, "Using bayesian networks for cyber security analysis," in *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on*, pp. 211–220, IEEE, 2010.

[20] J. Li, X. Ou, and R. Rajagopalan, "Uncertainty and risk management in cyber situational awareness," in *Cyber Situational Awareness*, pp. 51–68, Springer, 2010.

[21] F. Lan, W. Chunlei, and M. Guoqing, "A framework for network security situation awareness based on knowledge discovery," in *Computer Engineering and Technology (ICCET), 2010 2nd International Conference on*, vol. 1, pp. V1–226, IEEE, 2010.

[22] J. Goodall, W. Lutters, and A. Komlodi, "The work of intrusion detection: rethinking the role of security analysts," 2004.

[23] F. Schuetz and S. Burschka, "Locked shields: Nato cyber defense exercise 2012. exercise report," tech. rep., DTIC Document, 2012.

[24] K. Tang, M. Zhao, and M. Zhou, "Cyber insider threats situation awareness using game theory and information fusion-based user behavior predicting algorithm," *Journal of Information & Computational Science*, vol. 8, no. 3, pp. 529–545, 2011.

[25] S. R. Byers and S. J. Yang, "Real-time fusion and projection of network intrusion activity," in *Information Fusion, 2008 11th International Conference on*, pp. 1–8, IEEE, 2008.

[26] M. V. Van Alstyne, "A proposal for valuing information and instrumental goods," in *Proceedings of the 20th international conference on Information Systems*, pp. 328–345, Association for Information Systems, 1999.

[27] M. R. Grimaila, R. F. Mills, and L. W. Fortson, "An automated information asset tracking methodology to enable timely cyber incident mission impact assessment," tech. rep., DTIC Document, 2008.

[28] K. Jabbour, S. Adams, M. Gorniak, T. Humiston, P. Hurley, H. Klumpe, P. Ratazzi, P. Repak, B. Sessler, J. Sidoran, *et al.*, "The science and technology of cyber operations," tech. rep., DTIC Document, 2009.

[29] S. Liles and J. Kambic, "Cyber fratricide," in *Cyber Conflict (CyCon 2014), 2014 6th International Conference On*, pp. 329–338, IEEE, 2014.

[30] M. M. Hurley, "For and from cyberspace: Conceptualizing cyber intelligence, surveillance, and reconnaissance," tech. rep., DTIC Document, 2012.

[31] A. Tolk, "Moving towards a lingua franca for m&s and c3i–developments concerning the c2iedm," in *European Simulation Interoperability Workshop*, pp. 268–275, 2004.

[32] C. L. Paul and K. Whitley, "A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness," in *Human Aspects of Information Security, Privacy, and Trust*, pp. 145–154, Springer, 2013.

[33] M. Albanese, S. Jajodia, A. Pugliese, and V. Subrahmanian, "Scalable analysis of attack scenarios," in *Computer Security–ESORICS 2011*, pp. 416–433, Springer, 2011.

[34] S. Jajodia and S. Noel, "Topological vulnerability analysis," in *Cyber Situational Awareness*, pp. 139–154, Springer, 2010.

[35] S. Jajodia, S. Noel, P. Kalapa, M. Albanese, and J. Williams, "Cauldron mission-centric cyber situational awareness with defense in depth," in *MILITARY COMMUNICATIONS CONFERENCE, 2011-MILCOM 2011*, pp. 1339–1344, IEEE, 2011.

[36] E. Godefroy, E. Totel, M. Hurfin, and F. Majorczyk, "Automatic generation of correlation rules to detect complex attack scenarios," in *International Conference on Information Assurance and Security (IAS 2014)*, p. 6, IEEE, 2014.

[37] S. J. Yang, A. Stotz, J. Holsopple, M. Sudit, and M. Kuhl, "High level information fusion for tracking and projection of multistage cyber attacks," *Information Fusion*, vol. 10, no. 1, pp. 107–121, 2009.

[38] N. R. Howes, M. Mezzino, and J. Sarkesain, "On cyber warfare command and control systems," tech. rep., DTIC Document, 2004.

[39] Z. Liu, D.-s. Yang, D. Wen, W.-m. Zhang, and W. Mao, "Cyber-physical-social systems for command and control," *IEEE Intelligent Systems*, vol. 26, no. 4, pp. 92–96, 2011.

[40] W. Bradford, "The theoretical layered air-defence capability of a ship engaged against multiple anti-ship capable missile attacks," tech. rep., DTIC Document, 1992.

[41] R. E. Sawilla and D. J. Wiemer, "Automated computer network defence technology demonstration project (armour tdp): Concept of operations, architecture, and integration framework," in *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*, pp. 167–172, IEEE, 2011.

[42] L. Motus, M. Meriste, and J. Preden, "Towards middleware based situation awareness," in *Military Communications Conference, 2009. MILCOM 2009. IEEE*, pp. 1–7, IEEE, 2009.

[43] M. M. Kokar and M. R. Endsley, "Situation awareness and cognitive modeling," *IEEE Intelligent Systems*, vol. 27, no. 3, pp. 91–96, 2012.

[44] J. N. Haack, G. A. Fink, W. M. Maiden, D. McKinnon, and E. W. Fulp, "Mixed-initiative cyber security: Putting humans in the right loop," in *The First International Workshop on Mixed-Initiative Multiagent Systems (MIMS) at AAMAS*, 2009.

[45] A. F. Machado, A. B. Barreto, and E. T. Yano, "Architecture for cyber defense simulator in military applications," tech. rep., DTIC Document, 2013.

[46] N. Hayden, "The complexity of terrorism: Social and behavioral understanding trends for the future," *Information Age Warfare Quarterly*, vol. 1, no. 2, 2006.

[47] A. D'Amico, L. Buchanan, J. Goodall, and P. Walczak, "Mission impact of cyber events: Scenarios and ontology to express the relationships between cyber assets, missions, and users," tech. rep., DTIC Document, 2009.

[48] J. R. Goodall, A. D'Amico, and J. K. Kopylec, "Camus: automatically mapping cyber assets to missions and users," in *Military Communications Conference, 2009. MILCOM 2009. IEEE*, pp. 1–7, IEEE, 2009.

[49] G. S. M. Angelini, D. De Santis, "Toward geographical visualizations for hierarchical security data," in *VizSEC*, (Paris, France), November 2014.

[50] Y. Hideshima and H. Koike, "Starmine: A visualization system for cyber attacks," in *Proceedings of the 2006 Asia-Pacific Symposium on Information Visualisation-Volume 60*, pp. 131–138, Australian Computer Society, Inc., 2006.

[51] F. Fischer and D. A. Keim, "Vacs: Visual analytics suite for cyber security," in *IEEE VIS 2013: VAST Challenge Presentations*, (Atlanta, Georgia, USA), 2013.

[52] V. Y. Chen, A. M. Razip, S. Ko, C. Z. Qian, and D. S. Ebert, "Multi-aspect visual analytics on large-scale high-dimensional cyber security data," *Information Visualization*, p. 1473871613488573, 2013.

[53] C. Horn and A. D'Amico, "Visual analysis of goal-directed network defense decisions," in *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, p. 5, ACM, 2011.

[54] N. A. Giacobe, *Measuring the effectiveness of visual analytics and data fusion techniques on situation awareness in cyber-security*. PhD thesis, The Pennsylvania State University, 2013.

[55] C. A. Bolstad and M. R. Endsley, "Shared mental models and shared displays: An empirical evaluation of team performance," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 43, pp. 213–217, SAGE Publications, 1999.

[56] O. K. Upton, "Asserting national sovereignty in cyberspace: the case for internet border inspection," Master's thesis, Naval Postgraduate School, Monterey, California, June 2003.

[57] F. Hare, "Borders in cyberspace: can sovereignty adapt to the challenges of cyber security?," *The Virtual Battlefield: Perspectives on Cyber Warfare*, 2009.

[58] G. P. Coldebella and B. M. White, "Foundational questions regarding the federal role in cybersecurity," *J. Nat'l Sec. L. & Pol'y*, vol. 4, p. 233, 2010.

[59] T. Kellerman, "Cyber-threat proliferation: today's truly pervasive global epidemic," *Security & Privacy, IEEE*, vol. 8, no. 3, pp. 70–73, 2010.

[60] R. Ottis, "From pitchforks to laptops: volunteers in cyber conflicts," in *Conference on Cyber Conflict. Proceedings*, pp. 97–109, 2010.

[61] A. Viita-aho and A. Koskinen-Kannisto, "Multinational experiment 7 cyber domain outcome 3. cyber situational awareness. limited objective experiment report," tech. rep., DTIC Document, 2013.