Macrocognition Applied to the Hybrid Space: Team Environment, Functions and Processes in Cyber Operations

Øyvind Jøsok[1,4(✉)], Benjamin J. Knox[1], Kirsi Helkala[1], Kyle Wilson[3], Stefan Sütterlin[2,5], Ricardo G. Lugo[2], and Terje Ødegaard[2]

[1] Norwegian Defence Cyber Academy, Lillehammer, Norway
{ojosok, bknox}@cyfor.mil.no, khelkala@mil.no
[2] Department of Psychology, Inland Norway University of Applied Sciences, Lillehammer, Norway
{Stefan.Sutterlin, Ricardo.Lugo, Terje.Odegaard}@inn.no
[3] The Applied Cognition and Cognitive Engineering (AC2E) Research Group, University of Huddersfield, Manchester, UK
K.Wilson@hud.ac.uk
[4] Child and Youth Participation and Development Research Program, Inland Norway University of Applied Sciences, Lillehammer, Norway
[5] Center for Clinical Neuroscience, Oslo University Hospital, Oslo, Norway

Abstract. As cyber is increasingly integrated into military operations, conducting military cyber operations requires the effective coordination of teams. This interdisciplinary contribution discusses teams working in, and in relation to the cyber domain as a part of a larger socio-technical system, and the need for a better understanding of the human factors that contribute to individual and team performance in such settings. To extend an existing macrocognitive model [19] describing functions and processes into a conceptual framework that maps cognitive processes along cyber-physical and tactical-strategic dimensions (the Hybrid Space; [4]) to gain a better understanding of environmental complexity, and how to operate effectively in a cyber team context. Current experience from conducting cyber network defence exercises at the Norwegian Defence Cyber Academy and implications for future education and training are discussed.

Keywords: Macrocognition · Cyber domain · Team · Cognitive engineering · Hybrid space · Human factors · Socio technical system · Cyber · Military · Operations

1 Introduction

Across multiple domains teams are being increasingly called upon to perform complex problem identification and problem-solving tasks in novel contexts and situations [1, 71]. This is revealed in the military context, where formal recognition of the cyber domain as a domain of operations [2], presents significant team challenges due to its

D.D. Schmorrow and C.M. Fidopiastis (Eds.): AC 2017, Part II, LNAI 10285, pp. 486–500, 2017.
DOI: 10.1007/978-3-319-58625-0_35

emergent nature and novelty in the conflict arena [4–6, 65]. Cyber is the enabler of networked operations[1], allowing enhanced information flow to support humans in planning, command and control activities [7]. But it also escalates nonlinearity, complexity and unpredictability [8, 10], creating an environment too rapid and complex for human cognitive abilities to handle [12].

While the focus of research and development within the area of military cyber operations has been technology centered [13, 14], a growing amount of researchers have identified that the introduction of cyber as an operational domain places enhanced demands on teams [4, 10, 15, 16] and effective team coordination appears to be necessary for good cyber defence [17]. Combined with the integration of cyber operations into lower levels of military hierarchical structures [20, 21], this could lead to a significant shift in team dynamics, as roles, task demands and command functions are subsequently affected. [4, 10, 22]. The result is: *"Personnel operating in the cyber domain represent a group of actors facing work that is characterized by a unique pattern of human-technological interaction bearing cognitive and physical challenges across the digital, physical, and the social domain."* [22, p. 3]. How these demands manifest across team performance remains unexplored, which presents a challenge for education and training of individuals and teams within the area of cyber operations, as no common best practices or guidelines currently exist [3, 23].

While research on cyber operations has tended to investigate the possibility of enhancing performance by means of augmented cognition (e.g. aiding humans through the means of technology), there remains a case that the human element might be one of the greatest untapped sources of cyber defence effectiveness [14, 16, 17]. Currently, there is no consensus on how to assess the performance of teams in a cyber operation context [17]. This may be due to limited understanding of team processes in the complex problem solving environment of the cyber domain, when they are assessed against existing 'team' research that is generally considered to have flaws and limitations [1, 18]. For this reason, this paper assumes that good team performance cannot be assessed simply based upon the team who captured the flag first. Instead we argue that there is a need to investigate team processes in cyber defence training exercises as a path to assessing team and judging performance.

This paper first introduces the macrocognitive model by Schraagen et al. [19] and the Hybrid Space framework ([4]; Fig. 1) as conceptual tools for improving team performance in cyber operations. The paper will then look at team macrocognition in a cyber operations environment before finally describing contextual viewpoints from the perspective of cyber defence exercises conducted at the Norwegian Defence Cyber Academy (NDCA). Functions and processes that can be fostered in education and training will be discussed.

[1] Network enabled operations, definitions and maturity specifications see e.g.; [7, 9, 11].

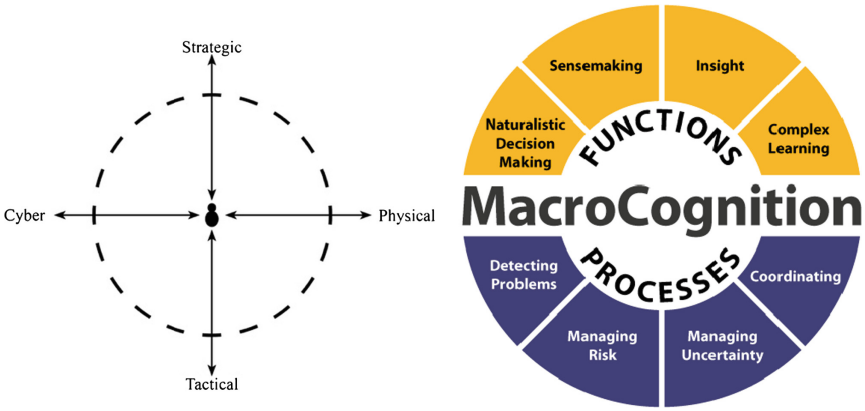

Fig. 1. The Hybrid Space conceptual framework [4] and macrocognition - functions and processes [19, 63].

2 Macrocognition and the Hybrid Space Framework Applied to Cyber Defence Teams

Located within the field of cognitive engineering [25] and empirically grounded in naturalistic decision making studies [24, 26, 27], the term macrocognition emerged from a need to address the broad variety of cognitive processes in a natural setting [1, 28, 70]. Macrocognition is subject to a variety of definitions that resemble each other by the commonality of explaining cognition in natural environments and later as 'the adaptation to complexity' [26, 28–32].

Macrocognition provides a framework (see Fig. 1) to study cognitive processes as they affect real-world task performance, and is addressed as a complement rather than a competitor to microcognition[2] [33, 70]. These processes include a range of internal and external cognitive activities [30] that are interoperable across team members for developing a set of alternative solutions [34]. The strength of this approach is that it encompasses both individual and team processes: *"Macrocognition is defined as the internalized and externalized high level mental processes employed by teams to create new knowledge during complex, one of a kind, collaborative problem solving."* [25, p. 7].

The Hybrid Space framework (see Fig. 1) can be used to map cognitive processes and to present a multidomain environment where cyber - as the key enabler - reduces distance between established hierarchical structures and formal rank and knowledge power relations [4, 22]. This occurs as decision makers and teams have to acknowledge and understand how to prioritize multiple assets based on known and unknown vulnerabilities and risks [4]. Mastering an environment where cognitive and physical challenges occur simultaneously across many situational dynamics and between several

[2] Klein et al. [30] coins the term microcognition for the purposes of explaining macrocognition. Microcognition refers to the study of cognition in controlled environments aiming at investigating the building blocks of cognition [30].

domains of interest [22, 35, 36] will rely on unprecedented levels of understanding [37, 69]. These higher levels of cognitive development are yet to be fully understood and require research to support agile manoeuvres in the information age [8].

The Hybrid Space conceptual framework primarily focuses on describing a cognitive landscape and the individual's perspective and perception of this [4]. However its applicability is not limited to individual actions; *"At all operational levels agents*[3] *can affect and are affected by abstraction levels of team and individual performance"* [4, p. 7]. Knox et al. [22] utilise the versatility of the Hybrid Space framework when addressing the issue of communication in socio-technical systems. They demonstrate the importance of the human factor by inferring from research in other safety-critical socio-technical systems such as acute medical care and aviation. A logical expansion of this contribution is to consider team processes in military socio-technical systems from the perspective of cyber defence units, where multiple operators are expected to act simultaneously as well as communicate and share knowledge.

The Hybrid Space adds a new dimension to observe and understand macrocognition functions and processes as they interact in a cyber-physical system. The macrocognition model, when applied to the cyber context does not account for vertical plane considerations as presented by the Hybrid Space. For example; the power dynamics in a team between tactical and strategic have direct impacts on team communication and coordination for functions and processes contributing to better performance.

3 Macrocognition in the Hybrid Space

In addressing cyber defence team issues, three possible factors that contribute to the breakdown of performance have been identified; team structure, team communication and information overload [38]. The conjunctions and reciprocal influence of these factors are not discussed in detail, but observed repeatedly in training as; *"…a group of individuals working independently with little to no communication or collaborative effort with team members."* [38, p. 221]. Even if research in this area is not mature enough to infer conclusively, this behaviour can be partly attributed to high cognitive load and partly to organizational policies [38]. However, analysts often spend a lot of time and effort searching the web for information that is often held by other members of the team, and simple communication efforts could fulfil the information need [16]. This indicates that the analysts' actions may actually be contributing to increased cognitive load. This leads to a decrease in communication and collaboration effort and as a result levels of overall understanding (individual and team) might suffer. This insight suggests that the individual and team dynamics are reciprocal cognitive processes, and understanding team dynamics in cyber defence teams can be approached from a naturalistic decision making research perspective through macrocognitive frameworks [26, 32, 69].

[3] In this context an agent can be both human and non-human [4].

3.1 Environment

Even though teamwork is a well researched construct, focus has been primarily on behavioural coordination in known tasks, and less on collaborative performance in novel situations [1, 38]. The macrocognitive functions that support teamwork in the Hybrid Space have to be viewed as processes that occur all of the time, often simultaneously, and some functions may serve as strategies to support the execution of additional novel functions [30]. Despite the interconnectivity of the functions, they can serve to support cognitive task analysis in naturalistic environments [31].

In discussing the macrocognitive environment, Klein et al. [30] identify a series of distinguishing features that form the context in which naturalistic decision making normally takes place [31]. These features are amongst others: ill-defined goals and ill-structured tasks; uncertainty, ambiguity, and missing data; shifting and competing goals; dynamic and continually changing conditions; action-feedback loops (real-time reactions to changed conditions); time stress; high stakes; multiple players; organizational goals and norms; experienced decision makers [31]. This list of features resembles the prerequisites for the Hybrid Space conceptual framework, where multiple agents in multiple domains interact and bring their own goals and assets into play. In the same way that Jøsok et al. [4] identify metacognitive skills as vital for performance in the Hybrid Space; research on macrocognitive constructs could bridge gaps between cyber team-members working in a hybrid environment that is defined by high stakes, ill-defined goals and tasks, information load, uncertainty and dynamic conditions [13, 14, 17, 38].

3.2 Structure

The role of cyber security teams is to protect assets that can be harmed via the cyber domain or in the cyber domain [39]. Within the area of team research it is generally accepted that a team needs to have a purpose and a goal, defined roles and a level of interdependence, as well as the fact that efficiency relies on team members' task- and team relevant knowledge and their understanding of these factors [40]. The current environmental issues in cyber defence teams make it difficult to meet these needs. Empowerment of lower ranks and cognitive readiness[4] to adapt to change is currently emerging as a requirement to perform successfully in the modern battlespace [4, 10, 22].

The tension between team goals and procedures, compared to organizational norms is a problem in this space [4]. At both inter and intra team level, one of the main contributing factors is that today's network and communications systems enable information to be shared and gathered in real-time, speeding up and blurring the interaction of agents, increasing the number of interactions between components dramatically, resulting in an inability to predict with confidence the consequences, (especially long term consequences) when parts of the system are altered by human actions [10].

[4] *"Cognitive readiness is the mental preparation (including skills, knowledge, abilities, motivations, and personal dispositions) an individual needs to establish and sustain competent performance in the complex and unpredictable environment of modern military operations"* [43, p. I-3].

Figure 2 encompasses a team with individually distributed responsibility and workload across the Hybrid Space. The leader will try to establish lines of communications to keep up to speed with the evolving situation, interacting with both the environment and team-members, engaging in a form of knowledge building process connecting pieces of information and aggregate these into higher levels of understanding [10]. In a military structure, the leader will also be expected to brief on the current situation to ranking officers or other stakeholders based on the current situational awareness of the total team knowledge and understanding. A logical action will be to position himself in an overarching role, with low levels of 'hands-on' and more context-related sensemaking. While this team concept model should work in relatively stable contexts in the physical world, the attributes of cyber make this difficult (e.g. ill-defined borders, concepts of time and space, absence of ground truth, the lack of law and policies, ambiguous ethical dilemmas etc.). However, hierarchical structuring of teams may have a negative impact on communication [41]. As several research contributions show, putting a team of experts together does not equal effective team performance. Factors ranging from a lack of organizational need or support, managemental errors or interindividual issues [42, 44–46] can all affect performance. This is somewhat addressed in the cyber defence team context when team coordination is identified as one of the main obstacles to performance. For example; internal team division of responsibility and established lines of communication during an incident were often brought into question [38]. In our view, this can also be described as a 'growing pain' [7] for military operations in the context of cyber operations. In a military context the contrarian asymmetries resulting from 'authority gradient' (leader: high; operator: low) and technical competence (leader: low; operator: high) distorts the common conception of a team. The leader's source of input is filtered by a complete information processing cycle on lower ranking expert levels; they rephrase, summarize and simplify before the collection of several complementary acting team members - at operator level - provide the informational input for the leader. This situation of contrarian asymmetrics probably needs entirely new ways of team development efforts, because of the special coordination and communication requirements needed in such a context [22]. Figure 3 provides a more accurate representation of the division of labor, coordination and communication demands that manifests itself in an operational context where any person can be the leader any given time.

3.3 Communication

The way team members are located across the space to cover the entire operational context has been acknowledged in the Orienting, Locating, Bridging (OLB) model [22]. This model is based on the assumption that one domain alone is not sufficient to make sense of the actions taken and the transferability of meaning to another domain. Using the OLB model, the interaction between members will be emergent and based on the current individual need to advance in the problem solving effort. The team would also be empowered to self-organize during problem solving if the traditional conceptions applied does not work, or had to be revised as the goals are reconceptualized

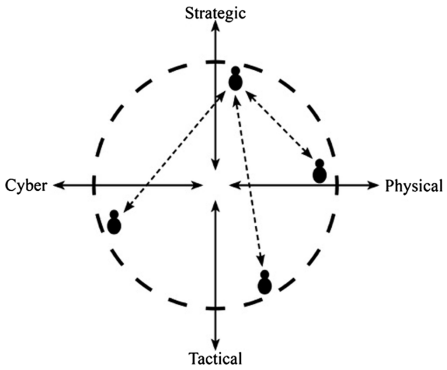

Fig. 2. Hierarchical structure, complicated relations

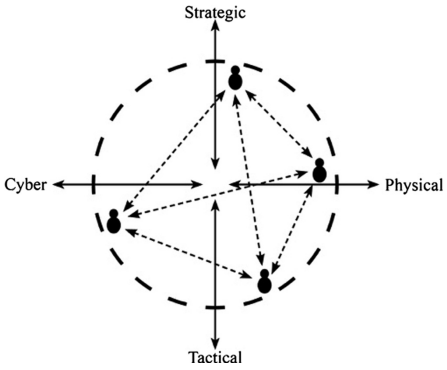

Fig. 3. Hierarchical structure, complex relations

based on improved understanding, or changing conditions in the environment. Klein [47] argues that complex settings require a more adaptive philosophy that breaks with fixed goals and fixed roles and task paradigms. Not just adapting to the goal, and changing the course of action, but changing the goals because of discoveries made during execution [47, 67]. Klein [47, 48] calls for a flexible execution that appreciates the process of setting goals, learning and discovery through planning and eventually redefining goals based on new insight into newly discovered, earlier invisible, relationships and dependencies. This will often lead to deeper understanding of the problem rather than to a solution [48]. Without a formal hierarchy, team members are free to share information as they wish [18]. Hence communication and coordination can be categorized as positively-complex between all team members. An example of this can be found among engineers working who demonstrated great team-work and cognitive flexibility to support their understanding of the STUXNET malware [53]. They analysed the code, and attempted to make sense of it individually and as a collaborative effort. They shared ideas across domains (i.e., not only looking at the

code). In the end, for the code to make sense, they needed greater insight and had to start paying attention to the world around them and the geopolitical situation [49]. This multi-domain, coordinating and detecting process was achieved through complex learning functions and demonstrates macrocognition in action, in a Hybrid Space environment.

While sensemaking is considered a process in macrocognition [30], in the cyber context it relies on a state of cyber situational awareness. Obtaining and presenting an agreed recognized cyber picture is a contested area in the military, and a number of scientific papers are concerned with *aspects* related to situational awareness that are in fact only sub components (i.e. sensors, recognized cyber picture, strategic picture, physical operations etc.) leaving the overall situational awareness unmentioned [23]. Consequently some argue the cyber situational awareness is just a part of the overall situational awareness, and that cyber information needs to be combined with other information from other domains in order to make sense [23]. In practical terms this suggests that team members as well as operator and commander, need mutual appreciation towards each other's perspective in order to communicate efficiently to support each other's sensemaking [22].

Terms like the 'strategic corporal' [50–52] try to address the symptoms of this change, the solution however is disputed. To enhance team communication and coordination efforts, team members must be empowered to share knowledge and make decisions based on the current shared team knowledge, reducing the perception of the leader as a command and control mechanism. This means that the attitude of each team member is important; as each team member is required to maintain effort towards building individual knowledge, whilst also engaging in uninterrupted sharing based on own and team insight relating to the current context and problem space. In researching naturalistic decision making, Klein [26] observed that experts were not necessarily searching for the optimal choice, but looking to find an action that was workable, timely and cost effective [31]. While this is probably workable in a tactical situation in the physical domain, this approach may not be good enough in an operational cyber setting. These 'experts' heavily relied on the recognition of patterns in their environment for decision making. However, the often complex and intangible relationships in cyber, confront teams with previously unknown factors that influence the decision making process. Therefore they would probably have to engage in what Klein describes as "complex recognition primed decision making strategy" [31], where the precondition is that the situation does not match the experts' prior experiences. Hence the expert cannot apply recognition primed decision making directly, meaning they are required to engage in learning and discovering new knowledge and exploring new and adaptable ways to tackle the current issue. This shifts the goalposts for team research; from performance and efficiency, to, adaptability and appreciation of learning and sharing. In this situation, the 'all capturing' Hybrid Space framework is appropriate to gain insight into cyber-physical understanding, consideration for multiple domains, and interpretation of information emerging from different channels; all leading to greater appreciation for different domain perspectives within a learning team. Klein et al. [54] claim that any human sensemaking of events will start with some kind of framework, even if the framework is minimal. However some events in cyber operations may be counter-intuitive, and hence require more effort to make sense of, as seemingly logical

reasoning may lead to faulty conclusions [55]. In conditions such as these, the adaptive characteristics of the Hybrid Space demonstrate how 'fit for purpose' it is for framing macrocognitive functions and processes in a new and complex field.

3.4 Information Load

Often in cyber operations the context complexifies the decision making process as the communication flow can be distorted by high cognitive load and information saturation [4, 12, 22, 38]. While the general, domain independent, assumption has been that more information available equals better decisions, there is still little known about how information sharing actually contributes to cyber situational awareness [23]. As long as humans are required to perceive and process information, there will be a point at which information overload becomes a reality. This leads to diminishing positive effects of information sharing due to reduced situational awareness [7].

In expert teams, individuals with specialized competence must actively acquire knowledge from the environment and each other to agree upon a full understanding of a problem space [18]. This dynamic form of problem-solving in a team can essentially be that of a 'moving-target' as processes are parallel, interdependent and continuous [1]. As for the Hybrid Space context, one could imagine the space itself sliding or moving along its axis, shifting the focus of the team to a more distant part of the space. This is a common problem recognized by several macrocognitive researchers in trying to understand complex socio-technical systems, and presents the researcher with 'moving target complications' in measurements [27, 64]. As experienced by military commanders [10], changes in both real-world scenarios and technology requires resilience and adaptability in work [27]. As the complexity of relations are augmented by technology *"...work cannot be adequately understood in terms of simplistic causal chain decomposition"* [56, p. 15].

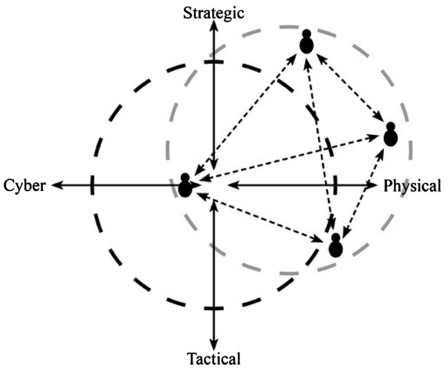

Fig. 4. Sliding space

As complexity increases [12] at an individual level, strategies of oversimplification are often applied [57]. At a team level, an often used strategy is distribution of workload and division of responsibility across an hierarchical team of domain experts [41, 46].

Both oversimplification (meaning also filtering out a lot of information before communicating it, limiting the recipient's information base for his/her decisions) and workload distribution are also an additional burden for communication capabilities. The process of gaining information is never ending, and in the Hybrid Space the attribution of attacks is difficult and making sense of intent and impact between domains can be confusing. The relationship between uncertainty and risk is also somewhat intangible, but still interconnected as i.e. acknowledgment of uncertainty would be to taking risk into account or to prepare to avoid or confront risks [58]. This is recognized in the Hybrid Space [4] when stating that: *"Assets and their vulnerabilities are interconnected. If an asset is lost, this loss has an effect on other assets and their vulnerabilities"* [4, p. 178].

It is well documented that inability to detect problems is the cause of many accidents [59], and in the Hybrid Space context the question of problem detection is particularly interesting (e.g. problem detection in the cyber domain relies on a unique human computer interaction and understanding; problems can emerge in one or several domains at different times, but still be interconnected; the effect of attacks might not be kinetic, but only have a cognitive impact i.e. lead to unthoughtful decisions that reduce operational freedom of own forces). While previous attempts to understand problem detection has been more incremental towards a threshold of detection, more complex domains seem to take advantage of higher level cognitive skills like re-conceptualization [59, 61].

Where the Hybrid Space conceptual framework [4] describes the environment in which cyber teams operate, the macrocognitive framework [19] adds understanding to the functions and processes that individuals and teams engage in within this space. Knowledge gained from observing and studying cognition in naturalistic settings in a cyber operation context [65], shed light on the current problems that have to be tackled to ensure that individuals and teams receive proper education and training [60] to operate in this complex multi-domain environment.

4 Research Based Cyber Defence Education - NDCA Context

The Norwegian Defence Cyber Academy (NDCA) conducts cyber defence exercises as part of a three year education cycle for officer cadets training to lead and operate in the cyber domain. Learning to operate in an environment where macrocognition shapes critical decision making supports exercising troops develop increased appreciation for team structures, grounded communication and the hazards of information overload.

The exercises are designed to ensure a positive learning environment for motivating, developing and nurturing the necessary and evolving individual and team skill-sets required to lead adaptively [68], and function as effective members in cyber teams. Fundamentally this requires creating an adaptable operative learning environment, that replicates multiple levels of complexity and cross domain dynamics [66]. In these conditions it becomes straightforward to expose trainees to novelty, as well as to the emerging nature of macrocognition in a cyber domain team context. Founded upon real world conflicts, exercise scenarios are holistic and capture the dynamics of the Hybrid Space by encompassing both cyber-physical problems as well strategic-tactical tension [4], ensuring naturalistic complexity. Context sensitive real world scenarios allow novices and practitioners to engage in authentic sensemaking based on available

newsfeeds, online information and own mental frameworks. The complexity of the scenarios requires the teams engage in learning activities to gain understanding of detected problems, to coordinate in order to decide on the best course of action as well as communicate risk, limitations and uncertainties to the designated operational commander. The objective is to create an environment where standard operation procedures cannot be applied and teams have to continually adapt to complexity and novelty. No frameworks are imposed upon exercising personnel regarding team configuration. They are encouraged to self-synchronize and are supported rather than assessed by their appointed expert mentor. As they learn to manage the broad spectrum of team demands required to operate effectively, they themselves discover and develop a deeper appreciation for the functions and processes of macrocognition (see Fig. 1) in a cyber critical team context. As they iterate through increasingly complex cyber attacks - that arrive in their network as part of larger geo-political scenario - their individual and team dynamics are trained, tuned and tested.

The cyber defence exercises apply the Hybrid Space framework as a means of grounding communication partners within a cognitive space that is influenced by tactical/strategical and cyber-physical/socio-technical dimensions. Participants' ability to consciously apply macrocognitive functions is built upon the three-phase OLB model [22]. For example; to create a learning environment that exposes these competencies, students attending a cyber defence exercise in 2016 were tasked to design and create their own 'recognized cyber picture'. This demanded they present information relevant for building cyber situation awareness as part of the wider operational and strategic scenario. The product needed to be versatile enough that data could be verbally and visually presented to a non-technical strategic level commander. The purpose was to ensure the teams were able to increase the commander's understanding of how the cyber situation affects the physical context, and needs to be integrated into decision making.

Critically and possibly uniquely, the research team is an integrated part of the exercise planning team. This allows observing for decision making and team processes in a naturalistic way as the 'exercise becomes the lab', meaning research methods can be applied, triangulated formatively and summatively and cognitive load can be managed in order to ensure information overload leads to positive learning outcomes among participants. All the while, researchers and experts mentor and encourage metacognitive process as well as observe for macrocognitive functions. Applying the Hybrid Space framework as both a tool to encourage metacognition in cadets, as well as a tool for researchers to gather data on, for example; team workload [62], establishing training, education and performance metrics for individuals and teams working in the cyber domain becomes less intangible.

5 Conclusion and Future Work

In this paper we gave a brief introduction of macrocognitive concepts and the Hybrid Space framework, and discussed their applicability for improving team performance in cyber operations. As an educational example, we discussed how the NDCA uses macrocognitive processes and the Hybrid Space framework in research-based cyber defence education.

Despite attempts by teams to self-evaluate improvements in their performance, or judgements based upon 'capture the flag type' competitions, there does not exist a well-defined definition for good performance in cyber defence. The development of objective and valid criteria of success in cyber defence, the operationalization of individual and team performance, and finally the isolation of predictors for performance are challenges for future research. The placement of macrocognitive processes within the Hybrid Space acknowledges the cognitive dimensions of tactical versus strategic considerations and the hybridity of environmental events encompassing cyber events and physical correspondents and thus provides an adaptation of the macrocognitive model in a cyber defense context. Current conceptions of team organisation, team leadership and team interaction might have to be re-conceptualized due to the impact of the cyber domain.

Acknowledgements. The authors would like to thank the Ving 69 at the NDCA for the contributions to this article.

References

1. Fiore, S.M., Rosen, M.A., Smith-Jentsch, K., Salas, E., Letsky, M., Warner, N.: Toward an understanding of macrocognition in teams: predicting processes in complex collaborative contexts. Hum. Fact.: J. Hum. Fact. Ergon. Soc. **52**, 203–224 (2010)
2. NATO: Warsaw Summit Communiqué (2016, press release). http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en
3. NATO: Cyber Defence Pledge (2016, press release). http://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en
4. Jøsok, Ø., Knox, Benjamin J., Helkala, K., Lugo, Ricardo G., Sütterlin, S., Ward, P.: Exploring the hybrid space - theoretical framework applying cognitive science in military cyberspace operations. In: Schmorrow, Dylan D.D., Fidopiastis, Cali M.M. (eds.) AC 2016. LNCS (LNAI), vol. 9744, pp. 178–188. Springer, Cham (2016). doi:10.1007/978-3-319-39952-2_18
5. Tikk-Ringas, E., Kerttunen, M., Christopher, S.: Cyber security as a field of military education and study. Joint Force Q. **75**, 57–60 (2014)
6. Williams, B.T.: The joint force commander's guide to cyberspace operations. Joint Force Q. **73**(2nd quarter), 12–19 (2014)
7. Buchler, N., Fitzhugh, S.M., Marusich, L.R., Ungvarsky, D.M., Lebiere, C., Gonzalez, C.: Mission command in the age of network-enabled operations: social network analysis of information sharing and situation awareness. Front. Psychol. **7**(937) (2016). doi:10.3389/fpsyg.2016.00937
8. Alberts, D.S., Haynes, R.E.: Power to the Edge. Command and Control in the Information Age. DoD Command and Control Research Program: Department of Defence (2003). (ISBN 1-893723-13-5)
9. Alberts, D.S., Huber, R.K., Moffat, J.: NATO NEC C2 maturity model. DTIC Document (2010)
10. McChrystal, S., Collins, T., Silverman, D., Fussell, C.: Teams of Teams: New Rules of Engagement for a Complex World. Penguin, New York (2016)
11. Wilson, C.: Network centric operations: background and oversight issues for congress (2007)

12. Zachary, W., Rosoff, A., Miller, L.C., Read, S.J.: Context as a cognitive process: an integrative framework for supporting decision making. Paper presented at STIDS (2013)
13. Knott, B.A., Mancuso, V.F., Bennett, K., Finomore, V., McNeese, M., McKneely, J.A., Beecher, M.: Human factors in cyber warfare: alternative perspectives. Paper presented at Proceedings of Human Factors and Ergonomics Society Annual Meeting (2013)
14. Mancuso, V.F., Christensen, J.C., Cowley, J., Finomore, V., Gonzalez, C., Knott, B.: Human factors in cyber warfare II emerging perspectives. Paper presented at Proceedings of Human Factors and Ergonomics Society Annual Meeting (2014)
15. Gutzwiller, R.S., Fugate, S., Sawyer, B.D., Hancock, P.: The human factors of cyber network defence. Paper presented at Proceedings of Human Factors and Ergonomics Society Annual Meeting (2015)
16. Rajivan, P., Janssen, M.A., Cooke, N.J.: Agent-based model of a cyber security defence analyst team. Paper presented at Proceedings of Human Factors and Ergonomics Society Annual Meeting (2013)
17. Forsythe, C., Silva, A., Stevens-Adams, S., Bradshaw, J.: Human Dimension in Cyber Operations Research and Development Priorities. Paper presented at International Conference on Augmented Cognition (2013)
18. Grand, J.A., Braun, M.T., Kuljanin, G., Kozlowski, S.W.J., Chao, G.T.: The dynamics of team cognition: a process-oriented theory of knowledge emergence in teams. J. Appl. Psychol. **101**(10), 1353–1385 (2016). doi:10.1037/apl0000136
19. Schraagen, J.M., Klein, G., Hoffman, R.R.: The Macrocognition Framework of Naturalistic Decision Making. Ashgate Publishing Limited, Aldershot (2008)
20. Army, U.: Integration of cyberspace capabilities into tactical units. US Army Cyber Command (2016)
21. Tan, M.: The multi-domain battle. Def. News Weekl. (2016). http://www.defencenews.com/articles/the-multi-domain-battle
22. Knox, B.J., Jøsok, Ø., Helkala, K., Khooshabeh, P., Ødegaard, T., Sütterlin, S.: Socio-technical communication: the hybrid space and the OLB-Model for science-based cyber education. J. Mil. Psychol. (2017, submitted)
23. Franke, U., Brynielsson, J.: Cyber situational awareness–a systematic review of the literature. Comput. Secur. **46**, 18–31 (2014)
24. Letsky, M.P.: Macrocognition in teams: macrocognition in collaboration and knowledge interoperability. Paper presented at Panel Presentation at 51st Annual Meeting of the Human Factors and Ergonomics Society, Baltimore MD (2007)
25. Letsky, M., Warner, N., Fiore, S.M., Rosen, M., Salas, E.: Macrocognition in complex team problem solving. DTIC Document (2007). http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA481422
26. Klein, G.: Naturalistic decision making. Hum. Fact.: J. Hum. Fact. Ergon. Soc. **50**(3), 456–460 (2008)
27. Hoffman, R., Klein, G., Miller, J.: Naturalistic investigations and models of reasoning about complex indeterminate causation. Inf. Knowl. Syst. Manag. **10**(1–4), 397–425 (2011)
28. Hoffman, R.R., McNeese, M.D.: A history for macrocognition. J. Cogn. Eng. Decis. Mak. **3** (2), 97–110 (2009)
29. Kahneman, D., Klein, G.: Conditions for intuitive expertise: a failure to disagree. Am. Psychol. **64**(6), 515 (2009)
30. Klein, G., Ross, K.G., Moon, B.M., Klein, D.E., Hoffman, R.R., Hollnagel, E.: Macrocognition. IEEE Intell. Syst. **18**(3), 81–85 (2003)
31. Klein, G., Klinger, D.: Naturalistic decision making. Hum. Syst. IAC Gatew. **2**(1), 16–19 (1991)

32. Klein, G., Wright, C.: Macrocognition: from theory to toolbox. Front. Psychol. **7**(54) (2016). doi:10.3389/fpsyg.2016.00054
33. Klein, D.E., Klein, H.A., Klein, G.: Macrocognition: linking cognitive psychology and cognitive ergonomics. Paper presented at Proceedings of 5th International Conference on Human Interactions with Complex Systems, University of Illinois at Urbana-Champaign, Urbana-Champaign (2000)
34. Deshmukh, A.V., McComb, S.A., Wernz, C.: Agents as collaborating team members. In: Letsky, M.P., Warner, N.W., Fiore, S.M.F., Smith, C.A.P. (eds.) Macrocognition in Teams: Theories and Methodologies. Ashgate Publishing Ltd., Aldershot (2008)
35. Kegan, R., Lahey, L.L.: Immunity to Change: How to Overcome It and Unlock Potential in Yourself and Your Organization. Harvard Business Press, Boston (2009)
36. Joiner, W.B., Josephs, S.A.: Leadership Agility: Five Levels of Mastery for Anticipating and Initiating Change, vol. 307. Wiley, New York (2006)
37. Defence, M.O.: Future Trends Programme - Future Operating Environment 2035, United Kingdom (2015). https://www.gov.uk/government/publications/future-operating-environment-2035
38. Champion, M.A., Rajivan, P., Cooke, N.J., Jariwala, S.: Team-based cyber defence analysis. Paper presented at 2012 IEEE International Multi-disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (2012)
39. von Solms, R., van Niekerk, J.: From information security to cyber security. Comput. Secur. **38**, 97–102 (2013)
40. Fiore, S.M., Ross, K.G., Jentsch, F.: A team cognitive readiness framework for small-unit training. J. Cogn. Eng. Decis. Mak. **6**(3), 325–349 (2012)
41. Brun, W., Ekornås, B., Kobbeltvedt, T., Pallesen, S., Hansen, A., Laberg, J.C., Johnsen, B. H.: Betydningen av felles mentale modeller for beslutningstaging i operative team. Nor. Mil. J. **11**(11–03), 22–27 (2003)
42. Dyer, W.G., Dyer, J.H., Dyer, D.: Team Building: Proven Strategies for Improving Team Performance. Wiley, New York (2013)
43. Morrison, J.E., Fletcher, J.D.: Cognitive readiness (2002)
44. Hackman, J.R.: Why teams don't work. In: Scott Tindale, R., Heath, L., Edwards, J., Posavac, E.J., Bryant, F.B., Suarez-Balcazar, Y., Henderson-King, E., Myers, J. (eds.) Theory and research on small groups, pp. 245–267. Springer, Heidelberg (2002)
45. Hackman, J.R.: Groups That Work and Those That Don't. Jossey-Bass, San Francisco (1990)
46. Urban, J.M., Bowers, C.A., Monday, S.D., Morgan Jr., B.B.: Workload, team structure, and communication in team performance. Mil. Psychol. **7**(2), 123–139 (1995). doi:10.1207/s15327876mp0702_6
47. Klein, G.: Flexecution as a paradigm for replanning, part 1. IEEE Intell. Syst. **22**(5), 79–83 (2007)
48. Klein, G.: Flexecution, part 2: understanding and supporting flexible execution. IEEE Intell. Syst. **22**(6), 108–112 (2007)
49. Gibney, A.: Zero Days. World War 3.0. Magnolia Pictures (2016)
50. Krulak, C.C.: The strategic corporal: leadership in the three block war. Mar. Mag (1999). http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA399413
51. Liddy, L.: The strategic corporal: some requirements in training and education. Education, training and doctrine. Aust. Army J. **2**, 139 (2004)
52. Lemay, A., Leblanc, S.P., De Jesus, T.: Lessons from the strategic corporal: implications of cyber incident response. Paper presented at Proceedings of 2015 ACM SIGMIS Conference on Computers and People Research (2015)
53. Lindsay, J.R.: Stuxnet and the limits of cyber warfare. Secur. Stud. **22**(3), 365–404 (2013)

54. Klein, G., Moon, B., Hoffman, R.R.: Making sense of sensemaking 2: a macrocognitive model. IEEE Intell. Syst. **21**(5), 88–92 (2006)
55. Lugo, R.G., Sütterlin, S., Knox, B.J., Jøsok, Ø., Helkala, K., Lande, N.M.: The moderating influence of self-efficacy on interoceptive ability and counterintuitive decision making in officer cadets. J. Mil. Stud. (2016)
56. Hoffman, R.R., Patterson, E., Miller, J.: Some challenges for macrocognitive measurement. In: Macrocognition Metrics and Scenarios: Design and Evaluation for Real-World Teams, pp. 11–28 (2009)
57. Fiore, S.M.F., Rosen, M., Salas, E., Burke, S., Jentsch, F.: Agents as collaborating team members. In: Letsky, M.P., Warner, N.W., Fiore, S.M.F., Smith, C.A.P. (eds.) Macrocognition in Teams: Theories and Methodologies. Ashgate Publishing Ltd., Aldershot (2008)
58. Lipshitz, R., Strauss, O.: Coping with uncertainty: a naturalistic decision-making analysis. Org. Behav. Hum. Decis. Process. **69**(2), 149–163 (1997)
59. Klein, G., Pliske, R.M., Crandall, B., Woods, D.: Features of problem detection. Paper presented at Proceedings of Human Factors and Ergonomics Society Annual Meeting (1999)
60. Arnold, T., Harrison, R., Conti, G.: Towards a career path in cyberspace operations for army officers. Small Wars J. 18 August 2014. http://smallwarsjournal.com/jrnl/art/towards-a-career-path-in-cyberspace-operations-for-army-officers. Accessed 4 Jan 2017
61. Hoffman, R.R., Shattuck, L.G.: Should we rethink how we do OPORDs? Mil. Rev. **86**(2), 100 (2006)
62. Lugo, R.G., Jøsok, Ø., Knox, B.J., Helkala, K., Sütterlin, S.: Team workload demands influence on cyber detection performance. Paper submitted for review at 13th International Conference on Naturalistic Decision Making 2017, Bath, UK (2017)
63. MacroCognition LLC. http://www.macrocognition.com
64. Rosen, M.A., Fiore, S.M., Salas, E., Letsky, M., Warner, N.: Tightly coupling cognition: understanding how communication and awareness drive coordination in teams (2008)
65. D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., Roth, E.: Achieving cyber defence situational awareness: a cognitive task analysis of information assurance analysts. Paper presented at Proceedings of Human Factors and Ergonomics Society Annual Meeting (2005). http://journals.sagepub.com/doi/abs/10.1177/154193120504900304
66. Jones, R.M., O'Grady, R., Nicholson, D., Hoffman, R., Bunch, L., Bradshaw, J., Bolton, A.: Modeling and integrating cognitive agents within the emerging cyber domain. Paper presented at Proceedings of Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) (2015)
67. LePine, J.A.: Adaptation of teams in response to unforeseen change: effects of goal difficulty and team composition in terms of cognitive ability and goal orientation. J. Appl. Psychol. **90** (6), 1153–1167 (2005). doi:10.1037/0021-9010.90.6.1153
68. London, M., Sessa, V.I.: The development of group interaction patterns: How groups become adaptive, generative, and transformative learners. Hum. Resour. Dev. Rev. **6**(4), 353–376 (2007)
69. Sawyer, B.D., Finomore, V.S., Funke, G.J., Mancuso, V.F., Funke, M.E., Matthews, G., Warm, J.S.: Cyber vigilance effects of signal probability and event rate. Paper presented at Proceedings of Human Factors and Ergonomics Society Annual Meeting (2014)
70. Wilson, K.M., Helton, W.S., Wiggins, M.W.: Cognitive engineering. Wiley Interdiscipl. Rev.: Cogn. Sci. **4**(1), 17–31 (2013)
71. Salas, E., Cooke, N.J., Rosen, M.A.: On teams, teamwork, and team performance: discoveries and developments. Hum. Fact.: J. Hum. Fact. Ergon. Soc. **50**(3), 540–547 (2008)