Military Psychology

ISSN: 0899-5605 (Print) 1532-7876 (Online) Journal homepage: https://www.tandfonline.com/loi/hmlp20

Socio-technical communication: The hybrid space and the OLB model for science-based cyber education

Benjamin J. Knox, Øyvind Jøsok, Kirsi Helkala, Peter Khooshabeh, Terje Ødegaard, Ricardo G. Lugo & Stefan Sütterlin

To cite this article: Benjamin J. Knox, Øyvind Jøsok, Kirsi Helkala, Peter Khooshabeh, Terje Ødegaard, Ricardo G. Lugo & Stefan Sütterlin (2018) Socio-technical communication: The hybrid space and the OLB model for science-based cyber education, Military Psychology, 30:4, 350-359, DOI: 10.1080/08995605.2018.1478546

To link to this article: https://doi.org/10.1080/08995605.2018.1478546

Published online: 30 Jul 2018.

MILITARY PSYCHOLOGY
2018, VOL. 30, NO. 4, 350–359
https://doi.org/10.1080/08995605.2018.1478546

Routledge
Taylor & Francis Group

Socio-technical communication: The hybrid space and the OLB model for science-based cyber education

Benjamin J. Knox[a], Øyvind Jøsok[a,d], Kirsi Helkala[a], Peter Khooshabeh[c], Terje Ødegaard[b], Ricardo G. Lugo[b], and Stefan Sütterlin[e,f]

[a]Norwegian Defence Cyber Academy, Defence University College, Lillehammer, Norway; [b]Department of Psychology, Inland University of Applied Science, Lillehammer, Norway; [c]US Army Research Laboratory, Human Research and Engineering Directorate, Los Angeles, California; [d]Child and Youth Participation and Development Research Program, Inland University of Applied Science, Lillehammer, Norway; [e]CHTD Research Group, Oslo University Hospital, Oslo, Norway; [f]Faculty for Health and Welfare Sciences, Østfold University College, Fredrikstad, Norway

ABSTRACT

Lessons from safety-critical sociotechnical systems, such as aviation and acute medical care, demonstrate the importance of the human factor and highlight the crucial role of efficient communication between human agents. Although a large proportion of fatal incidents in aviation have been linked to failures in communication, cognitive engineering provides the theoretical framework to mitigate risks and increase performance in sociotechnical systems not only in the civil sector, but also in the military domain. Conducting cyber operations in multidomain battles presents new challenges for military training and education as the increased importance of psychological factors such as metacognitive skills and perspective-taking both in lower and higher ranking staff, becomes more apparent. The Hybrid Space framework (Jøsok et al., 2016) provides a blueprint for describing the cognitive and behavioral constraints for maneuvering between socio-technical and cyber-physical systems whilst cooperating, coordinating or competing with accompanying cognitive styles in the chain of command. We apply the Hybrid Space framework to communicative challenges in the military cyber domain and suggest a three-phase Orienting, Locating, Bridging model for safe and efficient communication between partners. Based on the educational principles of the Norwegian Defence Cyber Academy, we discuss the required skill-sets and knowledge in which cyber officer cadets are trained and taught early in their education, and how these refer to the theoretical framework of the Hybrid Space and the key principles of communication as defined in cognitive engineering.

ARTICLE HISTORY
Received 31 October 2016
Accepted 11 March 2018

KEYWORDS
Cognitive engineering; hybrid space; sociotechnical system; cyber domain; grounded communication; mental models; multi-domain battle; cyber education

What is the public significance of this article?—The orientating, locating and bridging (OLB) model is a science-based contribution that aims to prevent communication failures arising from individual differences driven by factors such as hierarchy, bias or effort. A pedagogic approach to OLB in cyber education can potentially reduce the cognitive load and ease communication challenges in complex and critical cyberspace operations. This knowledge can easily be applied to civilian applications of cyberspace, such as protection of critical infrastructure, personal privacy protection and informing educators in how to enhance performance and decision-making in the cyber domain.

In this article, we show how we took a cognitive engineering process and applied it to communication activities conducted by military personnel operating in the cyber domain for improved performance.

Communication in sociotechnical systems[1] and its effect on decision-making are a crucial part of modern society influencing safety, efficiency, and performance. Extensive research, particularly in critical civil environments such as medical acute care and aviation, has improved our understanding of the constraints, risk, and possibilities associated with poor communication (e.g., Entin, 2004; Jacobsson, Hargestam, Hultin, & Brulin, 2012; Mills, Neily, & Dunn, 2008). Unsurprisingly, research interest on the effect of communication in the resource-intensive and safety-critical military context is growing rapidly (e.g., Brun et al., 2003; Cannon-Bowers & Salas, 1998; Espevik, Johnsen, & Eid, 2011; Rosen et al., 2008; Letsky, Warner, Fiore, & Smith, 2008; Trejo, Richard, Van Driel, & McDonald, 2015). Consequences arising from misunderstandings and ineffective communication range from undetected suboptimal performance to potentially fatal incidents with both local and international consequences (see Rosen, Fiore, Salas, Letsky, & Warner, 2008). The cyber domain, which consists of interconnected and

CONTACT Benjamin J. Knox bknox@cyfor.mil.no Norwegian Defence Cyber Academy, Defence University College, Lillehammer, Norway.

networked systems and actors represents a new and important domain for studying communication. 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 challenges that span the digital, physical, and the social domain (Jøsok et al., 2016; Von Solms & Van Niekerk, 2013; Whitman & Mattord, 2012). Within the military cyber context, success in the cyber domain requires a new and unique skillset compared to more traditional domains.

The digital context and informational environment has increased mental workloads, shifting demands from physical fitness toward cognitive performance that is novel to military domains. This underlines the importance of versatile preparation of personnel, concepts that go beyond classical military abilities or technological skills, and towards more comprehensive qualifications.

The increased awareness of the multiple social (e.g., cooperation and communication skills) and cognitive demands on cyber officers have been widely acknowledged but are not yet reflected in corresponding empirical research or commonly agreed standards of science-based education and training. The British Ministry of Defence recognized the need for skill development beyond technological domains when it stated that, “The operational commander in 2035 will need to be as focused on cyber as on traditional environmental factors” (Ministry of Defence, 2015). Whereas the US Military Academy at West Point addressed instructor competencies and responsibilities by stating that they have “updated their curriculum and pedagogy so that it now accounts for a cadet’s level of self-development” (Putz & Raynor in Reams, 2005). It is also becoming apparent that educational methods need to correspond to future communication demands placed upon personnel working in all military domains—including those conducting cyber operations.[2] To achieve a change in praxis, officer cadet educational programs should include development of cognitive characteristics such as, “agility, adaptability, and creative and critical thinking” (Tikk-Ringas, Kerttunen, & Spirito, 2014, p. 58). Military cadets who assume more traditional military training practices with clearly defined concepts, templates, and order-based execution may well struggle to fully cope in such an operating environment (Freedberg, 2016; Tikk-Ringas et al., 2014). Future operating environments will require soldiers to communicate effectively with multiple agents and entities in the cyber domain.

To meet some of the challenges that the cyber domain poses, as mentioned above, this article suggests a model for teaching prerequisites for improved communication in the cyber domain. The learning model will support practitioners operating in safety-critical environments by reducing the risk of negative consequences resulting from miscommunication. By implementing measures of cognitive engineering designed to improve communication efficiency in sociotechnical systems, the aim is to mitigate miscommunications that may go undetected or underestimated.

We begin this article by reviewing the current research and practice, detailing the theoretical frameworks established in cognitive engineering research, as well as introducing the Hybrid Space conceptual framework. Then, we propose a three-phase Orienting, Locating, Bridging (OLB) model for teaching and training to improve outcomes via efficient communication. The Norwegian Defense Cyber Academy (NDCA) is used to exemplify the OLB model’s application in a military educational context. Further, we discuss additional applications of the OLB before the article concludes and presents ongoing and future work.

Current research and practice

A novel area of research arising from the formal recognition of cyberspace as a military domain of operations (NATO Cooperative Cyber Defence Centre of Excellence, 2016) is how cognitive engineering can improve communicative challenges in sociotechnical systems. The cyber domain creates a special challenge for efficient communication among military command structures as the digital and the physical domains converge (Tikk-Ringas et al., 2014; Trujillo, 2014). Higher-ranking officers hold the final responsibility for the decisions made. Their routines, command and control activities, and eventual decision-making are most likely rooted in and influenced by their previous experience. However, their situational awareness and decision-making are heavily influenced, if not determined, by the perception, interpretation, and evaluation of a given critical situation by a lower ranking, and often younger officer who comfortably maneuvers in the cyber domain (Røislien, 2015). To promote effective communication, particularly in the cyber domain, there is a mutual need for perspective-taking skills to understand others’ need for information, their mental workload, and a metacognitive awareness concerning one’s own momentary cognitive states and susceptibilities. Common ground theory provides the theoretical framework for understanding the elements of successful social interaction. It is based on cognitive engineering and provides a framework to systematically approach and consequently mitigate risk factors and enhance efficiency and performance in goal-directed communication (Clark, 1996; Monk, 2009; Morrow & Fischer, 2013). Common ground theory stresses the necessity of a mutual understanding, with which both sender and receiver consider the exchanged information as accurate, understood, and related to the shared goal (Searle, 1969). As a result of grounded communication, both partners are able to co-construct a shared mental model that can support "shared consciousness" and "empowered execution" (McChrystal, Collins, Fussell, & Silverman, 2015).

The aspects described above capture the challenge of developing shared mental models in the military domain, where hierarchy and rank structures can impact perspective taking. In particular the emerging nature of the cyber domain adds layers of complexity that further exasperate the challenge of achieving common ground. Approaches capable of finding common ground in the cyber domain need to be considered in the context of networked intelligence (McChrystal et al., 2015; Tapscott, 2014) and multidomain battles (Tan, 2016) as these approaches are heavily dependent upon shared situational awareness for sense-making. For example, multidomain challenges influence communication in military domains by merging the need to empower lower ranks through models of command and control that are context-oriented, rather than reverting them to the norm of restrictive hierarchical communication systems. Communication can be more effective if the actors (i.e., the individuals communicating with one another) can more closely align their mental models in dynamic hybrid operating environments. This will rely upon methods of education and training that aspire to higher levels of consciousness (Joiner & Josephs, 2006; Kegan & Lahey, 2009) in both junior and senior military personnel, as they are expected to undertake mutually beneficial actions of self-orienting and locating each other, to bridge grounded communication.

Because of these new demands, higher-ranking commanders will be required to accept new communication concepts and training for agile maneuvering in the cyber domain. Commanders need to be able to strategically empower lower-ranking soldiers, reduce strict divisions between tactical and strategic personnel, and act to facilitate effective communication that allows for goal-directed and accurate use of information as well as an increased level of openness among involved personnel. The OLB model presented in this article dissects the steps required for successful communication in the Hybrid Space (Jøsok et al., 2016) and provides guidance for both lower and higher ranks to promote grounded communication.

The Hybrid Space framework

A recent theoretical proposal addressed many of the challenges described above by introducing the Hybrid Space conceptual framework (Jøsok et al., 2016) (see Figure 1). The framework represents an individual's range of cognition when involved in tasks that span strategic vs. tactical, or physical (kinetic) vs. cyber operations. Along the spectrum of these dimensions, different cognitive skills are necessary/used, for example, heuristics, social-cognitive perspective-taking, spatial cognition for kinetic, self-regulation for planning, evaluating, and monitoring one's own processes and macrocognition for team performance. The framework acknowledges the new structures and demands by articulating the needs for cognitive flexibility and perspective-taking on an inter- and intra-individual level, which allows for the application of psychological concepts in assessment, in training and action of military cyber personnel. The Hybrid Space not only describes how the individual cognitively maneuvers between dynamic tactical/strategic and cyber-physical/sociotechnical demands, but it also implies the need for objective orientation related to one's own and other communication partner's momentary mental 'location' within these domains. It also reveals the requirements for effective communication bridging to ensure optimal performance levels. This perspective taking is required to co-construct a shared mental model with communication partners.

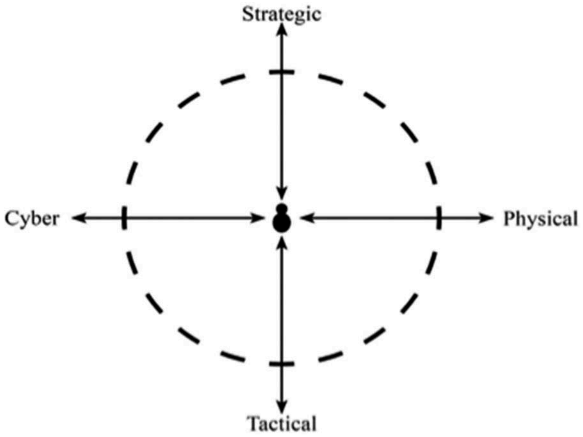


Figure 1. The hybrid space. Reprinted from exploring the hybrid space - theoretical framework applying cognitive science in military cyberspace operations (pp. 181). Ø. Jøsok, B.J. Knox, K. Helkala, R.G. Lugo, S. Sütterlin, & P. Ward. 2016, Foundations of Augmented Cognition: Neuroergonomics and Operational Neuroscience LNCS Volume 9744.

In the military context of the cyber domain, the construction of shared mental models leads to mutual understanding and efficient processing of time-critical information, provides the basis for tactical decisions with potentially large strategic implications, and thus requires the reduction of risk factors that lead to miscommunication. Using the two-dimensional structure of the Hybrid Space rather than adapting or copying existing models allows for more straightforward presentation of the unique characteristics of the human factor in military cyber operations typical in today's multi-domain battles.

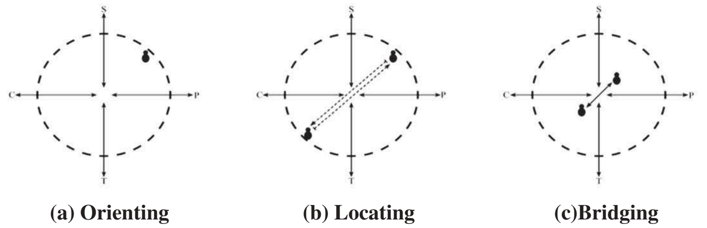
The OLB model: How to educate for grounding of communication in the cyber domain

When co-constructing a shared mental model, communication partners should apply techniques to enhance situational awareness, information-processing resources such as working memory, cognitive flexibility, metacognitive awareness, and perspective-taking (Morrow & Fischer, 2013). The Hybrid Space framework (Figure 1) allows for the introduction of applied cognitive science into cyber domain education. The OLB model is based on this framework and dissects maneuvering within the Hybrid Space into three core phases (see Figure 2). The educational implications are illustrated in Figure 3.

> Phase 1: Orienting—momentary metacognitive awareness of one's cognitive location in the Hybrid Space.
>
> Phase 2: Locating—accurately judge the communication partners' cognitive location in the Hybrid Space.
>
> Phase 3: Bridging—adapting content and style to ensure grounding for appropriate communication to construct a shared mental model of the current situation.

Orienting

A prerequisite for an accurate placement of one's own cognitive location within the Hybrid Space (orienting) is the metacognitive awareness of factors influencing one's momentary mental state and ongoing cognitive processes. In Hybrid Space terms, this refers to the ability to monitor and regulate thinking along the cyber-physical and strategic-tactical dimensions (horizontal and vertical axis, Figure 2a). An example of orienting could be a junior cyber operator preparing to brief or communicate the recognized cyber picture (RCP) to a senior but nontechnical person. If a network intrusion has occurred, a RCP brief should accurately present the severity and potential known or unknown consequences. Good metacognitive awareness allows the operator to visualize the most appropriate mode, method, and content of communication to ensure he/she relays an accurate message that is not only received correctly but also understood. Similarly, a nontechnical commander will need to regulate and monitor his/her own thinking, behavior and be open to extending his/her cognition and modes of communication. This will allow for better understanding and appreciation of critical and quite possibly incomplete information being presented by a junior expert. As the examples above show, failure to orientate prior to receiving an RCP brief could result in a critical communication error occurring. Attempting to orientate to gain mutual understanding or a shared mental model is challenged further when the RCP brief takes place across multiple and heterogeneous communication partners in the



(a) Orienting (b) Locating (c)Bridging

Figure 2. OLB model as a procedure to communicate across the Hybrid Space. (S-strategic, T-tactical, P-physical, C-cyber). (a) Orienting. (b) Locating. (c) Bridging.

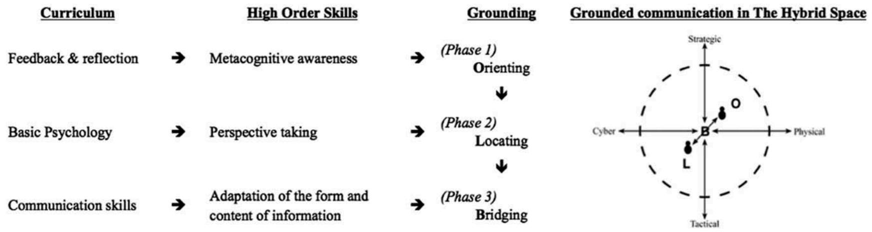


Figure 3. Pedagogic path for OLB – a practice to reduce the cognitive cost of communication in the hybrid space.

Hybrid Space—some face-to-face and others via digital means. This is because the communicator has to be keenly aware of more than one location in the Hybrid Space and be cognizant of the implications for communicating within these different spaces.

Locating

Once an individual has gained metacognitive awareness of his/her location within the Hybrid Space, locating the communication partner constitutes Phase 2 in the OLB model (Figure 2b). Locating specifically involves accurately judging a communication partner's cognitive location in the Hybrid Space. It also involves identifying factors that can impact a partner's interpretation of incoming information. For instance, understanding a partner's knowledge, skills, and emotional state and current cognitive load, as well as cultural background and contextual circumstances (time pressure, external expectation, conflicting task priorities), can help an individual tailor a message to meet their partner's immediate needs and ensure proper understanding.

The act of perspective taking is an important process in the locating phase of the OLB model. Factors such as a partner's expertise, experience with a particular topic, and professional conventions may impact how he or she thinks, talks, and interprets information and can thus be used to establish communal command ground (Monk, 2009). For example, rethinking hierarchical systems to empower lower ranking personnel (Tan, 2016) and thus increase their contextual knowledge could positively affect the lower ranking person's capacity to contribute to effective grounding. Understanding what communities a person belongs to may allow agents to make certain assumptions about existing common ground. They can then use this knowledge to make communication across the hybrid space more effective. In a borderless domain, mediated by electronic communication, this perspective taking might be more relevant than in face-to-face situations where cultural misunderstandings are more easily detected by the use of multiple communication modalities.

Personal common ground gained prior to or during a communication improves the location process further. The personal state of mind such as the level of acute or chronic stress and momentary attentional focus directly influence the quality of grounding and can change at an instant. Individuals who feel observed, monitored, and socially challenged in a conversation within a hierarchical system are more likely to engage in self-monitoring behavior at the cost of their cognitive task performance and ongoing problem-solving or communicative demands. For example, communication failure can occur in a hierarchical system where defensive reasoning flourishes (Argyris, 1991).

Without perspective taking and acknowledging communication partners needs, a junior expert attempting to present the RCP to a nontechnical commander could negatively affect communication flow by incorrect locating and message framing. In this context, interaction may also suffer at the cost of performance outcomes on an individual and team level if the commander is unwilling to locate—through acknowledging the junior experts' needs and requirements—and engage in learning and knowledge creation, to gain critical understanding. The complexity of locating escalates when a RCP has to be delivered via digital communication means to multiple heterogeneous recipients across the Hybrid Space.

Bridging

The final phase, bridging, describes the adaptation of content and style of grounded communication to coconstruct a shared situational model (Figure 2c). When the process of orienting (requiring metacognition) and locating (requiring perspective-taking) has given insight in the relative location of the communication partners, bridging the remaining gap requires an adaptation of the form and content of information provided. This includes a common understanding of the appropriate level of detail, the conventional norms and forms of presentation, knowledge about the degree of tolerated uncertainty, the situationally appropriate level of confidence into one's own judgment or self-criticism, and the openness to admit the need for additional information or simplification. By adapting communicated content and its style in a way that maximizes the overlap of shared cognitive representations, the cognitive distance between two partners within the Hybrid Space is reduced and the risk of misunderstandings and misinterpretations limited. Successful bridging acknowledges the partners' cognitive position along the tactical-strategic and the cyber-physical domain. Preparing the appropriate amount and type of information in a way that acknowledges a partners' cognitive position is key to successful communication in critical situations. For example, bridging for successful communication of a RCP has to be adaptive and able to engage in immediate self-correcting actions in face-to-face communication. In a multidomain context, bridging for good communication of a RCP may require opening multiple lines of communication for adjusted framing of communication. Communicating with more heterogeneous multiple recipients is challenging, as information demands and understandings vary. For this reason, the OLB points out the need for training and development of communication skills to enhance communicating messages simultaneously in face-to-face dyadic mode and in a socio-technical context.

The NDCA approach

The three phases of the OLB model constitute elements fostering grounded communication in a military cyber domain setting. The NDCA emphasizes in their training of cyber officer cadets applied cognitive science and various sub-areas of psychology as a central element of their education program. To facilitate metacognitive awareness for orienting, the NDCA covers topics such as personality psychology, psychophysiological interaction to sensory perception, effects of acute and chronic stress on cognitive performance, group effects on decision-making, and macrocognition. These are combined with practical experience involving regular peer-group and mentor feedback provided in written and oral form. According to the OLB model, forming a realistic perspective of oneself in a complex sociotechnical system is a crucial prerequisite for successfully locating oneself within the Hybrid Space and fostering safe and efficient communication. The NDCA applies the OLB model and aims to enhance individual skills to orientate within the Hybrid Space by the use of reflection logs and frequent feedback. Using reflection and reflective dialogues as a tool to build an evidence base for new perspectives, where a cadet moves from being a detached observer to an involved learner (Brigden & Purcell, 2004), supports the orientation function by enhancing metacognitive awareness. Becoming more aware of yourself through metacognitive training a hybrid-operating environment can provide the necessary scaffolding for success in Phase 2: locating.

Achieving a high level of mutual perspective taking and awareness for communication partners' situational demands in dynamic contexts are central elements of teaching and training at the NDCA. This content is meant to train cadets on the locating phase of the OLB model. A curriculum including subject areas such as intercultural knowledge and international operations acknowledges this need in cyber cadet cohorts. At the NDCA, cadets get exposed to a curriculum equipping them with the knowledge and cultural understanding to mediate their communication efforts in the borderless cyber domain.

In their final year at the NDCA, cadets practice bridging skills by planning activities in complex and varying context, ranging from classroom environments to demanding military exercises. The cadets are expected to lead people—their own cohort and junior cadets—and processes. Teachers and instructors act as facilitators as well as a heterogeneous group of actors within the sociotechnical system. The intent is to encourage cadets to train their skills in adapting the form and content of information being communicated in order to ensure effective bridging. Figure 3 shows how the NDCA applies the model in teaching curriculum.

Furthering understanding and applications of OLB

Other constraints for successful (i.e., efficient and safe) communication—of particular relevance in a military structure—are culture, social norms, conventions, and formal constraints caused by the authority gradient based on formal ranking. These constraints based on an asymmetry of power and agency are commonly associated with the use of indirect speech of a lower ranking person toward someone of higher status, and the tendency to avoid expressions or formulations that could be perceived as critical, disagreeing, impolite, or not sufficiently appreciative (Blum-Kulka, House, & Kasper, 1989; Grice, 1975; Jason, Keys, Suarez-Balcazar, Taylor, & Davis, 2004; Xiao, Seagull, Mackenzie, Ziegert, & Klein, 2003). Conversely, these constraints occur when higher ranking officers incorrectly (consciously or unconsciously) make assumptions about junior officers' level of competence in a particular domain where the junior officer has expertise. This could lead to communication failures (i.e., indirect communication, partial communication or even body language) and result in misinterpretation at the receiving end, having a negative effect for developing shared mental models (DeChurch & Mesmer-Magnus, 2010). Developing (or the emergence of) a shared situational awareness or shared mental model around partially overlapping expertise (probable consequences of action) and responsibilities (tactical and strategic considerations) will be difficult because of the clear role distinctions based on seniority and rank. In this case, higher ranking officers are potentially unaware of factors influencing a young cyber officer's judgment, performance, and goals (Sexton, Thomas, & Helmreich, 2001) thus leading to poor situational awareness and lack of shared mental models. Misinterpretations of critical situations in aviation based on this type of communication failure between pilot and first officer have been termed "monitoring/challenging error" by the National Transportation Safety Board (NTSB, 1994 in Fischer & Orasanu, 2000). This error was found to occur in over 75% of the air traffic accidents reviewed (Morrow &

Fischer, 2013). This type of error has also been acknowledged in acute medical care, where the communication within a surgical team is similarly challenged by differences in social status between nurses and doctors, and a lack of understanding of the external factors influencing the partners' cognitive abilities (Korb, Geißler, & Strauß, 2015).

Explicit procedures such as reading back information to ensure mutual understanding are supposed to facilitate grounding in both aviation and medical care. To avoid misunderstandings caused by the authority gradient and related conventions, research in aviation found positive effects where communication skills allowed for a good balance of informativeness and social appropriateness (Fischer & Orasanu, 2000), and where crew members stated explicitly how the perceived information was interpreted and how they are about to react on it. Although the speaker (e.g., the cyber officer) has to make sure that the intention of his presented information is mutually understood, it is the receiving person's responsibility to signalize his or her level of understanding. A communication style based on mutual reassurance, openness to correction, re-evaluation, negotiation, and adjustment is also needed in the military to minimize barriers to collaboration and communication bottlenecks and to facilitate effective grounding (McChrystal et al., 2015).

OLB for grounded communication

Grounded communication in the context of cyber operations faces particular challenges that result directly from the location of the individual's cognitive focus across the axes of the Hybrid Space (Figure 1), and the cognitive costs of constant movement along them, leading to depletion of attentional resources (Jøsok et al., 2016). An example of the cognitive implications and changes in decision-making processes when being continuously exposed to the cyber domain, arises from the physical, and consequently, emotional distance to this environment that is directly affected via digital means. The decision maker, empowered by the cyber domain, is less directly confronted with the outcomes of the decision. The anticipation of future action's outcomes is more abstract, less detailed, and typically decision-making processes are under time pressure. These circumstances in the decision-making processes in the cyber domain, together with other assumed, but not yet investigated aspects, such as an increased tolerance to uncertainty, increases the cognitive load on decision stakeholders. To ensure grounded communication, the cyber officer has to be aware of the strategic considerations affecting the situational assessment, awareness, and decision-making process of higher ranking officers to whom he or she reporting (e.g., Krulak, 1999; Lemay, Leblanc, & Jesus, 2015; Liddy, 2004; Stringer, 2009). At the same time, his/her own decisions in the cyber domain relating to cyber operations may affect the strategic goals of the mission. The possibility of strategic impact, the implications and the resulting options concerning how to react to these impacts, needs to be communicated accordingly.

OLB for better regulatory behavior

Monitoring and adjusting one's own cognitive location within the Hybrid Space increases cognitive demands considerably. In a time-critical situation, a relatively young/junior cyber operator with appropriate domain understanding and enough knowledge to allow for strategic consideration may lack the skill-set for grounded communication. In this instance, not being "heard" by a higher ranking commander prone to biased judgments can affect the strategic goal due to his/her distant relative location on the Hybrid Space's axes (Jøsok et al., 2016). In this example, communication failure results from insufficient grounding. The former lacked training in OLB processes—not necessarily mental capacity—whilst the latter lacked cognitive regulatory resources and reverted to the hierarchy norm to avoid further increasing the cognitive load.

OLB for grounded communication in multi-domain environments

In the context of multidomain battles, grounded communication becomes essential for team and task maneuvering (i.e., cross-domain cyber operations). Historical and contemporary military norms and practices of communication will not suffice (General D. Perkins in Tan, 2016). Changes in education and training will be necessary to meet the potential consequences of the changing and diverse nature of the battlefield. The increased interconnectivity, reliance, and conjunction of multiple domains translate to heightened operational complexity, and affects leaders, decision makers, operators, and soldiers on the ground (Ministry of Defence, 2015). The extent and complexity of tasks will likely require domain-specific expertise working in collaboration with expertise from other conflicting or complementary domains, in a form of "multidomain problem solving." As earlier research in teams and collaboration shows, it is not enough to put people with a particular expertise or the "right" knowledge together in a group and expect them to work seamlessly (Hackman, 1990; Mathieu, Tannenbaum, Donsbach, & Alliger, 2014). This phenomenon occurs as teams of experts are often hierarchically structured (Brun et al., 2003) and their approach to mastering the complexity of the given environment is to divide the given task into manageable pieces and delegate it to the expert team members (Brun et al., 2003). Brun and colleagues (2003) further pointed to the fact that hierarchical structures may have a negative influence on team communication. In hierarchical teams, performance suffers as the level of communication rises through the chain-of-command (Cannon-Bowers, Salas, & Converse, 1993), and communication is characterized by questions and answers. This is contrary to flat structured teams where peer relationship behavior is directed into finding and offering information based on one's own initiative (Urban, Bowers, Monday, & Morgan Jr., 1995) leading to better communication and performance.

OLB for improved cross cultural team communication

The momentary need for grounded communication is explored in time-framed tasks, often with routine actions and stable competence demands (i.e., a flight plan from A to B; Morrow & Fischer, 2013). This leads to the use of artifact tools, such as checklists or as in read-back strategies to ensure grounded communication. Although relevant, some conclusions have relied heavily on results from US research on US personnel (Brun et al., 2003). This reliance leads to research implications when a similar task includes cultural aspects or cross-cultural collaboration in a complex multidomain sociotechnical cyber-physical system, where teams operate with overlapping schedules and responsibility gets transferred (Morrow & Fischer, 2013). Training metacognitive skills to support improved orientation in cross cultural multidomain operating environments could give an advantage to military personnel as they attempt to locate communication partners. The cyber domain is creating novel communication challenges compared to direct face-to-face communications framed by physical presence. Digital communication and time-lagged interaction poses particular challenges for the communicators both on the sending and the receiving end. Awareness about these sensitivities is therefore increasingly relevant as more digital, indirect, and asynchronous the communication becomes.

Conclusion

In an era of cyber operations and multi-domain battles, new challenges are presented for military training and education. Cognitive engineering can provide theoretical models to understand the conditions of safe and effective communication and design interventions to increase communication skills, which have been shown to be one of the most frequent sources of human failure or under-performance in safety-critical sociotechnical systems both in the civil as well as military domains. As a consequence, teaching and training in the military cyber domain needs to acknowledge the need for knowledge building in psychological functions as represented in enhanced metacognitive skills and mutual perspective-taking.

By applying the Hybrid Space theoretical framework, we locate communication partners within a cognitive space determined by tactical/strategic and cyber-physical/socio-technical dimensions. The proposed three-phase OLB model describes the consecutive and complementary steps that lead to a better grounding of communication in a field of overlapping expertise and separated responsibilities along the authority gradient typical for military context.

In an attempt to meet today's challenges and as a means of taking justified science-based steps toward future teaching doctrines in cyber education, the NDCA aims to enhance future cyber operators' communication skills by training and teaching the aforementioned skills from early stages in their education.

Future work

What remains to be studied is if it is enough to rely on momentary grounding measures or whether teams, working in complex hybrid environments should expend greater effort grounding communication ahead of operations. The NDCA are conducting empirical studies aimed at applying the OLB model in various contexts relevant for military cyber operations and in non-military contexts. This includes communicative challenges on the team level, monitoring communicative processes in real time—the role of cognitive agility for grounded communication and performance assessment—and the influence of personality characteristics and the changing role of leadership in a cyberspace context.

Notes

1. Sociotechnical system is the interaction of people and technology, composed of social, management and technical subsystems (Troxler & Lauche, 2015).
2. Cyber operations is defined as the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace (Schmitt; Tallinn Manual, 2013).

References

Argyris, C. (1991). Teaching smart people how to learn. *Harvard Business Review*, *69*, 3.

Blum-Kulka, S., House, J., & Kasper, G. (1989). Cross-cultural pragmatics: Requests and apologies. *Advances in Discourse Processes*, *31*. Norwood, NJ: Ablex Publishing Corporation.

Brigden, D., & Purcell, N. (2004). *Focus: Becoming a reflective practitioner*. York, UK: Higher Education Academy. [Online] Available at: http://www.heacademy.ac.uk/resources/detail/subjects/medev/Focus-_Becoming_a_reflective_practitioner

Brun, W., Ekornås, B., Kobbeltvedt, T., Pallesen, S., Hansen, A., Laberg, J. C., ... Johnsen, B. H. (2003). Betydningen av felles mentale modeller for beslutningstaging i operative team. *Norwegian Military Journal*, *11*(3), 22–27.

Cannon-Bowers, J. A., Salas, E., & Converse, S. (1993). Shared mental models in expert team decision making. In N. J. Castellan Jr. (Ed.), *Individual and group decision making: Current issues* (pp. 221–246). Hillsdale, NJ: Lawrence Erlbaum Associates.

Cannon-Bowers, J. A., & Salas, E. E. (1998). *Making decisions under stress: Implications for individual and team training*. Washington, DC: American Psychological Association.

Clark, H. H. (1996). *Using language*. Cambridge, UK: Cambridge University Press.

DeChurch, L. A., & Mesmer-Magnus, J. R. (2010). The cognitive underpinnings of effective teamwork: A meta-analysis. *Journal of Applied Psychology*, *95*(1), 32–53. doi:10.1037/a0017328

Entin, E. E. (2004). Communications and Coordination Across Low and High Fidelity Simulation Environments. Retrieved April 20, 2016, from http://www.dodccrp.org/events/2000_CCRTS/html/pdf_papers/Track_4/027.pdf?ref=Guzels.TV

Espevik, R., Johnsen, B. H., & Eid, J. (2011). Communication and performance in co-located and distributed teams: An issue of shared mental models of team members? *Military Psychology*, *23*(6), 616–638. doi:10.1080/08995605.2011.616792

Fischer, U., & Orasanu, J. (2000). Error-challenging strategies: Their role in preventing and correcting errors. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *44*(1), 30–33. doi:10.1177/154193120004400109

Freedberg, S. (2016 October 05). Miserable, disobedient & victorious: Gen. Milley's future US soldier. *Breaking Defense, Air, Intel & Cyber, Land, Sea, Strategy & Policy*. Retrieved from http://breakingdefense.com/2016/10/miserable-disobedient-victorious-gen-milleys-future-us-soldier/

Grice, H. P. (1975). Logic and Conversation. In P. Cole & J. Morgan (Eds.), *Syntax and semantics* (Vol. 3, pp. 41–58). New York, NY: Academic Press.

Hackman, J. R. (Eds.). (1990). *Groups that work (and those that don't): Creating conditions for effective teamwork*. San Francisco, CA: Jossey-Bass.

Jacobsson, M., Hargestam, M., Hultin, M., & Brulin, C. (2012). Flexible knowledge repertoires: Communication by leaders in trauma teams. *Scandinavian Journal of Trauma, Resuscitation and Emergency Medicine*, *20*(1), 44. doi:10.1186/1757-7241-20-44

Jason, L. A., Keys, C. B., Suarez-Balcazar, Y. E., Taylor, R. R., & Davis, M. I. (Eds.). (2004). *Participatory community research: Theories and methods in action*. Washington, DC: American Psychological Association.

Joiner, W. B., & Josephs, S. A. (2006). *Leadership agility: Five levels of mastery for anticipating and initiating change*. San Francisco, CA: John Wiley & Sons.

Jøsok, O., Knox, B. J., Helkala, K., Lugo, R. G., Sütterlin, S., & Ward, P. (2016). Exploring the hybrid space - theoretical framework applying cognitive science in military cyberspace operations. In Schmorrow, D. D. D., Fidopiastis, C. M. M. (Eds.) *Foundations of augmented cognition: Neuroergonomics and operational neuroscience* Lecture Notes in Computer Science, 9744, (pp. 178–188). New York, NY: Springer.

Kegan, R., & Lahey, L. L. (2009). *Immunity to change: How to overcome it and unlock potential in yourself and your organization* (1st ed.). Boston, MA: HBR Press.

Korb, W., Geißler, N., & Strauß, G. (2015). Solving challenges in inter-and trans-disciplinary working teams: Lessons from the surgical technology field. *Artificial Intelligence in Medicine*, *63*(3), 209–219. doi:10.1016/j.artmed.2015.02.001

Krulak, C. C. (1999). The strategic corporal: Leadership in the three block war. *Marine Corps Gazette*, *83*(1), 18–22.

Lemay, A., Leblanc, S. P., & Jesus, T. D. (2015). *Lessons from the strategic corporal: Implications of cyber incident response*, Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research (pp. 61-66), SIGMIS-CPR '15, Newport Beach, CA.

Letsky, M. P., Warner, N., Fiore, S., & Smith, C. A. P. (Eds.). (2008). *Macrocognition in teams: Theories and methodologies*. London, England: Ashgate.

Liddy, L. (2004). The strategic corporal: Some requirements in training and education. *Australian Army Journal*, *2*(2), 139–148.

Mathieu, J. E., Tannenbaum, S. I., Donsbach, J. S., & Alliger, G. M. (2014). A review and integration of team composition models: Moving toward a dynamic and temporal framework. *Journal of Management*, *40*(1), 130–160. doi:10.1177/0149206313503014

McChrystal, S. A., Collins, T., Fussell, C., & Silverman, D. (2015). *Team of teams: New rules of engagement for a complex world*. New York, NY: Penguin.

Mills, P., Neily, J., & Dunn, E. (2008). Teamwork and communication in surgical teams: Implications for patient safety. *Journal of the American College of Surgeons*, *206* (1), 107–112. doi:10.1016/j.jamcollsurg.2007.06.281

Ministry of Defence (2015, December 14). *Strategic Trends programme: Future operating environment 2035*. Retrieved from https://www.gov.uk/government/publications/future-operating-environment-2035

Monk, A. (2009). *Common ground in electronically mediated conversation*. San Rafael, CA: Morgan & Claypool Publishers.

Morrow, D. G., & Fischer, U. M. (2013). Communication in socio-technical systems. In J. D. Lee & A. Kirlik (Eds.), *The Oxford handbook of cognitive engineering* (pp. 178–199). New York, NY: Oxford University Press.

NATO Cooperative Cyber Defence Centre of Excellence, (2016). *NATO Recognises cyberspace as a 'domain of operations' at warsaw summit*. Retrieved from https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html

Putz, M., & Raynor, M. (2004). *Integral leadership: Overcoming the paradox of growth*. In J. Reams (2005). What's integral about leadership? A reflection on leadership and integral theory. *Integral Review*, *1*, 118–131.

Reams, J. (2005). What's integral about leadership? A reflection on leadership and integral theory. *Integral Review*, *1*, 118–131.

Røislien, H. (2015). When the generation gap collides with military structure: The case of Norwegian cyber officers. *Journal of Military and Strategic Studies*, *16*(3), 23–44.

Rosen, M. A., Fiore, S. M., Salas, E., Letsky, M., & Warner, N. (2008). Tightly coupling cognition: Understanding how communication and awareness drive coordination in teams. *International Journal of Command and Control*, *2*(1), 1–30.

Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge, England: Cambridge University Press.

Searle, J. R. (1969). *Speech acts: An essay in the philosophy of language*. Cambridge, England: Cambridge University Press.

Sexton, J. B., Thomas, E. J., & Helmreich, R. L. (2001). Error, stress, and teamwork in medicine and aviation: Cross sectional surveys. *Journal of Human Performance in Extreme Environments*, *6*(1), 5–11. doi:10.7771/2327-2937.1019

Stringer, K. D. (2009, September-October). Educating the strategic corporal: A paradigm shift. *Military Review*, *89*(5), 87–95.

Tan, M. (2016, October 3). The multi-domain battle. *Defense News Weekly*. Retrieved from http://www.defensenews.com/articles/the-multi-domain-battle

Tapscott, D. (2014). *The digital economy anniversary edition: Rethinking promise and peril in the age of networked intelligence*. New York, NY: McGraw-Hill.

Tikk-Ringas, E., Kerttunen, M., & Spirito, C. (2014). Cyber security as a field of military education and study. *Joint Forces Quarterly*, *75*(4), 57–60.

Trejo, B. C., Richard, E. M., Van Driel, M., & McDonald, D. P. (2015). Cross-cultural competence: The role of emotion regulation ability and optimism. *Military Psychology*, *27*(5), 276–286. doi:10.1037/mil0000081

Troxler, P., & Lauche, K. (2015, July 15), *Assessing creating and sustaining knowledge culture in organisations*. Retrieved from http://www.academia.edu/1964062/Assessing_Creating_and_Sustaining_Knowledge_Culture_in_Organisations

Trujillo, C. (2014). The limits of cyberspace deterrence. *Joint Forces Quarterly*, *75*(4), 43–52.

Urban, J. M., Bowers, C. A., Monday, S. D., & Morgan Jr., B. B., Jr. (1995). Workload, team structure, and communication in team performance. *Military Psychology*, *7*(2), 123–139. doi:10.1207/s15327876mp0702_6

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. doi:10.1016/j.cose.2013.04.004

Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Boston, MA: Course Technology.

Xiao, Y., Seagull, F. J., Mackenzie, C., Ziegert, J., & Klein, K. J. (2003, October). Team communication patterns as measures of team processes: Exploring the effects of task urgency and shared team experience. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *47*(12), 1502–1506. Los Angeles, CA: SAGE Publications. doi:10.1177/154193120304701228