Exploring the Hybrid Space

Theoretical Framework Applying Cognitive Science in Military Cyberspace Operations

Øyvind Jøsok[1](✉), Benjamin J. Knox[1], Kirsi Helkala[1], Ricardo G. Lugo[2], Stefan Sütterlin[2], and Paul Ward[3]

[1] Norwegian Defence, Cyber Academy, Lillehammer, Norway
ojosok@cyfor.mil.no, {f-bknox,khelkala}@mil.no
[2] Department of Psychology, Lillehammer University College, Lillehammer, Norway
{Ricardo.Lugo,Stefan.Sutterlin}@hil.no
[3] The Applied Cognition & Cognitive Engineering (AC2E) Research Group, University of Huddersfield, Manchester, UK
P.Ward@hud.ac.uk

Abstract. Operations in cyberspace are enabled by a digitized battlefield. The ability to control operations in cyberspace has become a central goal for defence forces. As a result, terms like cyber power, cyberspace operations and cyber deterrence have begun to emerge in military literature in an effort to describe and highlight the importance of related activities. Future military personnel, in all branches, will encounter the raised complexity of joint military operations with cyber as the key enabler. The constant change and complexity raises the demands for the structure and content of education and training. This interdisciplinary contribution discusses the need for a better understanding of the relationships between cyberspace and the physical domain, the cognitive challenges this represents, and proposes a theoretical framework - the Hybrid Space - allowing for the application of psychological concepts in assessment, training and action.

Keywords: Cyberspace · Physical domain · Cyber-physical system · Cyber security · Socio-technical system · Hybrid space · Human factors

1 Introduction

"The future commander needs to be as focused on cyber as on other environmental factors" [1]. This statement summarizes the current dilemma of contradictory task profiles and cognitive demands for military personnel, which result in challenges that present themselves across the social, physical and cyber domains. The complexity of cognitive work associated with human-technological interaction with multiple interdependent, interconnected and networked environments is compounded [2], as these human and technological agents consequently bring their own assets and goals (e.g., informational, social, physical, cyber [3–5]) into the operating and decision making space. Moreover, activity in this space is further complicated or complexified as each agent needs to secure their own assets, in order to maintain freedom of movement [17].

D.D. Schmorrow and C.M. Fidopiastis (Eds.): AC 2016, Part II, LNAI 9744, pp. 178–188, 2016.
DOI: 10.1007/978-3-319-39952-2_18

Examining asset protection from a security perspective is important to ensure security is not compromised, all assets need to be protected from current and future threats, both internal and external to the system. Simultaneously, vulnerabilities inherent within the entire socio-technical system (STS) have to be managed [5]. According to Whitman and Mattord [3] an asset is a protected organizational resource. Therefore, prioritizing these resources is achieved by weighting assets based on values ranging from: criticality, profitability, replacement or protection expenses, and embarrassment or loss of liability factor if the asset is revealed [3]. Assets and their vulnerabilities are interconnected. If an asset is lost, this loss has an effect on other assets and their vulnerabilities.

Expanded digitization and global network coverage [6] will connect people and physical infrastructure to cyberspace and to other physical entities via cyberspace. In turn, this will reveal novel and unforeseen connected vulnerabilities that requires human cognition to self-regulate and transform[1]. Several authors have identified a lack of understanding regarding how the connectivity of agents has negative consequences for decision making and action, especially relating to third party infrastructure [8]. We argue that today's decision makers have to acknowledge and understand how to prioritize multiple assets based on known and unknown vulnerabilities and risks. Achieving this level of understanding within a contradictory and hybrid landscape requires cognitive flexibility to control the multiple situational dynamics that can occur simultaneously between assets in the physical domain, the social domain and cyberspace.

In a military context, these hybrid conditions create challenges for efficient decision making as final responsibility lies with ranking officers whose past experience and current practice, including key command and control activities such as sensemaking and decision making, are rooted in and influenced by factors in the physical domain [7, 8]. Despite their affinity for the physical over cyber media, increasingly, officer understanding and decision making is being guided by information perceived, interpreted, evaluated and communicated to them by lower ranking, and often younger, officers who operate comfortably in this domain [10]. Agents equipped with the necessary capabilities to translate phenomena originating in cyberspace into the physical domain can potentially provide the crucial knowledge bridge required to influence far reaching military and political decision making.

The conjunction of age, rank and experience reveals a didactic shift in command responsibility and decision making. This can be addressed through better understanding of competencies or better definitions of competencies. The arrival of 'cyber' has revealed evidence that suggests more understanding of skill-sets and agile leadership [12] can contribute to defining human competencies as requisites for performance in contemporary military operations.

Huge investments have been made to develop and implement state-of-the-art technologies across sectors to improve human efficiency. Digitization has increased

[1] Kegan and Lahey [2] define the self-transforming mind as: "able to step back and reflect on the limits of our own ideology or personal authority; see that any one system or self-organization is in some way partial or incomplete; be friendlier toward contradiction and opposites; seek to hold on to multiple systems rather than projecting all but one onto the other" [2, p. 17].

information flow and interdependability of technological systems [13]. Efforts to leverage human performance have been answered by new technologies [15], yet the results seem only to increase cognitive demand [14, 16]. The cognitive workload placed on humans in this context exceed those in most common contexts [14]. Making the right decisions in Computer Network Operations (CNO) has added value given the potential for unknown or unintended consequences [17].

Several authors argued that there is a current lack of understanding of the human factors necessary to operate effectively, safely and securely in this complex space [9, 11, 18, 19]. This is revealed through the inability to adequately integrate CNO into contemporary military operations [17, 20], a pressing need for cyber related study materials at all command levels [8, 21], and insufficient career structures for cyber personnel [22]. The Hybrid Space approach acknowledges these factors as points of departure for continuing research that integrates situational dynamics in cyberspace and the physical domain, with individual cognitive skill-sets, psychological determinants of action and communicative aspects, within a merging socio-technical and cyber-physical system.

2 The Hybrid Space Framework

The Hybrid Space (Fig. 1) frames the interconnection between cyberspace and the physical domain, whilst simultaneously demonstrating the tension between tactical and strategic goals in decision making and action (compression of command-levels) in a future operating environment context. Individual domain specific competencies, experience and rank determine performance levels and behaviours in a organisational and institutional landscape that necessitate the integration, or at least complementary juxtaposition, of cyber and physical domains (henceforth, hybrid). Understanding the processes and actions required to enhance and accelerate these capabilities may hold the key to releasing the tension between command levels when attempting to project military power.

This framework acknowledges the Cyber-Physical System (CPS) and the effects of automation through cyber-based technological operations on the physical world. CPS research has been predominantly focused on the left side (Fig. 2a) of the horizontal axis and has been defined as "…the close interaction of computing systems and physical objects…" [24, p. 3]. With some exceptions (e.g., [37]), research in the area of STS - defined as; "…taking both social factors and technological factors into consideration" [25, p. 720] - resides primarily on the right of our horizontal axis (Fig. 2b). Going forward, we view the field of STS research exploring how people will cope and perform in a digitizing society.

In a pre-cyber landscape, the vertical axis has divided doctrine into three levels; tactical, operational and strategic [23]. The intent of the vertical axis in the Hybrid Space framework is to transfer conventional knowledge of military command levels and situate this doctrine into a present day context. This novel approach is representative of today's digitized context; where cyber pervades all aspects of military planning and leadership [23]. Cyber is shaping how traditional command levels are responding. It has resulted in the compression of command levels [10] as a means of adaptation for coping and

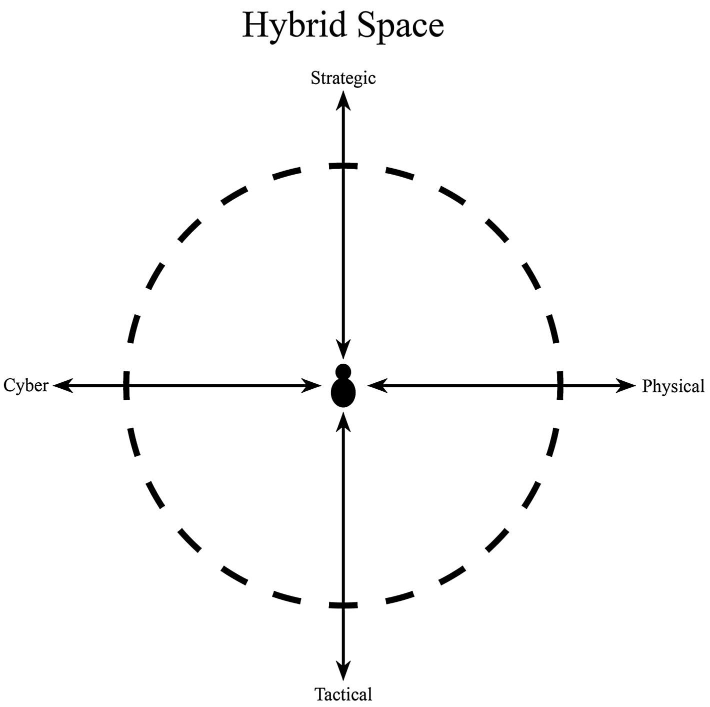

Fig. 1. The hybrid space framework

performance. In turn, bisecting the vertical axis with the horizontal axis reveals a convergence of complexity. The purpose of the Hybrid Space is to open the space for exploration in competencies, human behavior and cognitive processes [19] that occur, or need to occur, in and around this point of convergence.

Viewing this complex terrain through the lense of the Hybrid Space - where human and macrocognitive factors play a significant role [19] - can serve to bridge the expertise gap between cyberspace and the physical domain. Cyberspace operations merge in-depth tactical knowledge with strategic appreciation, which can create tension at different command levels as it challenges traditional military doctrine, education models and cultures [8, 16]. Inconsistencies in tactical and strategic operations across organizations result in difficulties in collaborative sensemaking with respect to core aspects of defining cyber and, as such, present significant barriers for CPS and STS interoperability [8]. Establishing clarity in this Hybrid Space is needed, not only to ensure effective intra and inter-organisational communication, cooperation and coordination, but to ensure national and international asset security.

2.1 Horizontal Axis

As indicated, the horizontal axis shown in Fig. 2 of the Hybrid Space framework acknowledges earlier research in CPS and STS. CPS research acknowledges the

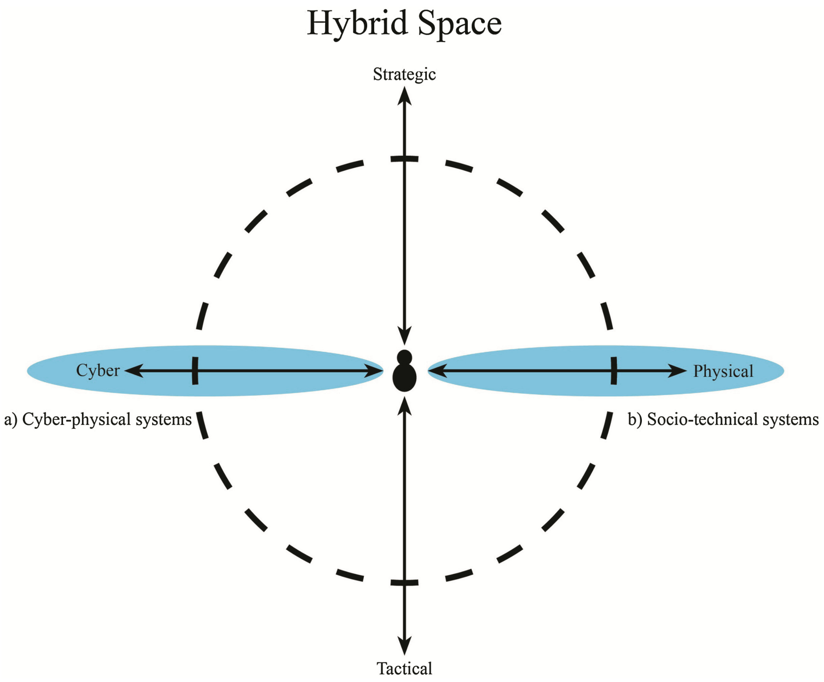

Fig. 2. The hybrid space framework in relation to CPS: "…the close interaction of computing systems and physical objects…" [24, p. 3] and STS: "…taking both social factors and technological factors into consideration" [25, p. 720].

integration of the cyber domain with the physical world [26, 27], but current frameworks describing CPS and cyber attack categorization are mostly technology-centric and tend to neglect the human factor [9, 19]. On the other hand, STS situates a human in the center and is composed of social, management and technical subsystems [28], but in most research conducted to date, STS has not fully embraced the role of cyberspace, as the technical subsystem only provides the necessary functions to meet the roles of the human [28]. We argue that including all environmental factors solely in an additive manner does not satisfy the level of complexity facing individuals and teams operating within these overlapping fields.

In the Hybrid Space framework, we extend the notion of STS to include cyber operations as well as the coordinating operations that result from its integration. As a result, the cognitive work in which humans engage, and the systems themselves, are increasingly complex [14]. Work is highly interactive and comprised of humans, agents and artifacts. Information may be novel, deceptive, and/or limited, and is typically distributed across space and time; Tactical goals (i.e., how to deal with a specific new threat) are frequently ill-defined, and there is often a need for conflict resolution between strategic goals (e.g., protect against a known state threat actor) and lower-order goals that are both dynamic and emergent. Much of this requires significant preparation, planning and replanning, as well as a considerable degree of domain-specific skill (such as situation assessment, sensemaking, and decision making skills within STS and CPS). A key feature is the requirement for proficiency at handling novelty, so that humans can adapt on the fly to changing demands. To complicate matters further, the stakes are almost always high, and uncertainty, time-constraints and stress are seldom absent. Moreover, tactics and strategy that dictate how work should unfold are typically constrained by broader professional, organizational, and institutional practice and policy [29]. The macrocognitive demand characteristics placed on young personnel when operating in the Hybrid Space exceeds those in most common contexts. Making the right decisions in the Hybrid Space has added value given the potential for unknown or unintended consequences [30].

The horizontal axis in the Hybrid Space model acknowledges the simultaneous presence and incongruent needs of cyberspace and the physical domain. Attacks in cyberspace do not differ from conventional attacks insofar as they generate effects beyond the intended domain of interest [9, 17]. However, they do differ in the way that consequences might be unintended or hidden, revealed in unconventional timeframes or affect third party interests. This incongruency necessitates a range of skill sets including highly developed technical skills (e.g., coding, programming, analysis, etc.), considerable macrocognitive skills (perception, interpretation, evaluation) and effective interpersonal and psychological skills (perspective taking, communicative skills, for instance to convey mission impact information to a commander). This axis highlights the need for a new category of personnel with a wide variety of social and technical expertise [1, 8, 11, 17, 20].

2.2 Vertical Axis

The vertical trajectory of the Hybrid Space framework visualizes the compression of command levels whilst simultaneously recognizing the institutional need to maintain such structures. The compression of command levels has been widely recognized in contemporary military doctrines and goes by the acronym of the Strategic Corporal [10]. Tactical decisions made by military personnel must take into account the strategic realities that used to be purview of the higher levels in the chain of command [10], as the distinction between tactical and strategic impact is becoming increasingly blurry [10]. In a CNO context, these decisions and actions performed by an operator, can have geopolitical consequences.

Lemay and colleagues [10] give a variety of plausible situations where a cyber operator is forced to decide and act on Advanced Persistent Threat (APT) incidents that may affect the strategic scope of the organization. Cyber operations are marked by unconventional timeframes (ranging from years to seconds in a both a future and historical timeline) that result in cognitive complexity and pressure when attempting to avoid negative consequences. Thus, a high level commander can easily miss out on decisions affecting the strategic goal due to his/her relatively distant placement on the Hybrid Space's horizontal axis. Consequently, strategic sensemaking and decision-making can suffer. When this is combined with concerns relating to adversary intent and attribution [10] young personnel need to understand the strategic picture in order to communicate events and respond accurately to uncertainty. This requires a model of leadership that is mature, agile and appropriate to context [8]. Lamay et al. [10] conclude that in this new context, the strict division between tactical and strategic personnel cannot hold as it potentially constrains and prevents leadership of cyber operators. They elaborate that it is unlikely that a manager with an IT background will keep up with technology development, and technical personnel spending all their time updating themselves, might lose track of the bigger picture. Having one supervisor for every cyber operator is not an answer, and given the time constraint and time available to make decisions [10] it narrows down the possible pathways ahead. As Lemay et al. [10] argue; enhanced training, understanding the commander's intent and decentralized decision making have been brought forward as possible solutions. However, this process will require instruction and training methods followed by evaluation to determine whether or not decentralized decision-making generally works.

So for now, incident handlers are strategic agents, often without being aware of it [10], and often without their operational and strategic levels of command being aware of it. If the current gap of technological skills and knowledge between managers/ commanders and technical personnel [10] is viewed upon in the Hybrid Space framework, the implications for leadership training that can leverage mastery of the 'understand function' [1] through cognitive-technical and cognitive-psychological competencies becomes evident.

To the best of our knowledge, the Hybrid Space conceptualization is the first to fully acknowledge that investing in new technologies - to leverage human performance [31, 32] - has not accounted for what people view as important and given them strategies for organizing that information. The Hybrid Space acknowledges specific features that appear through a shift in contemporary military leadership. As knowledge agents (human and technical) are required to 'lead' commanders and senior military planners who experience heightened anxiety as their perceived self-efficacy and control beliefs are threatened due to the ambiguity and asynchronous nature of the digital battlefield [8].

The Hybrid Space framework simultaneously stresses how human agents are required to move between tactical and strategic considerations to master the understand function [1] and operate effectively within the complexity of merging CPS and STS landscapes. The Hybrid Space explains a novel state of being and opens up space for critical research that can guide practices capable of facilitating the necessary learning pathways for human performance in digitization.

3 Metacognition and Navigation Within the Hybrid Space

As command levels compress and systems converge, operating within the Hybrid Space requires agents take conscious control of assets and responsibility for improving their cognitive flexibility to move freely. This cognitive process builds on the Generation Y learning paradigm of perception, emotional involvement, intuitive and experience based practice [11, 33]; whilst also complimenting current pedagogical trends where learners are encouraged to develop their cognitive and metacognitive skills, as pathways to better performance and self-insight [35]. For military personnel, this learning process facilitates mastery of the future operating environment whilst also implying the need for systematic and autonomous application of adaptive reflection [36] to build self-regulatory processes and self-efficacy. Agents who are capable of mirroring the dynamism [34] of the complex developing Hybrid Space landscape, will demonstrate leadership qualities founded upon the power of knowledge-based abstractions, rather than being constrained by institutional norms of military command experience or rank. This cyber leadership 'art' chances that current military norms and solutions relating to command, control and understanding of leadership models, only present barriers and limit expectations [8].

Human factors focuses on the "fit" between the user, system, and the situational demands in a hybrid space between cyber and physical domain. The Hybrid Space model defines military personnel as located at the interface between CPS and STS and that both systems incorporate the human "in the loop". Events in the cyberspace, as perceived by the human agent, have not only direct effects on decisions made in the physical domain, but also influence human decision-making via indirect psychological effects. In a similar vein, circumstances in the physical domain can affect the interaction with and thus events within the cyberspace. Reacting adequately to constantly changing environmental needs requires efficient navigation within the Hybrid Space, i.e., between cyber- and physical domain (horizontal axis) as well as monitoring one's relationship towards current tactical and strategic goals and demands (vertical axis).

Metacognition refers to 'thinking about thinking' and includes the components knowledge of one's abilities, situational awareness, and behavioral regulation strategies [38]. Individuals with high metacognitive skills have more accurate and confident judgment of their own performance in relation to the demands and are better able to accurately describe their strengths, weaknesses, and their potential to improve. Thus, high metacognitive awareness of one's cognitive processes (planning, monitoring, evaluations) facilitates one's localisation within the Hybrid Space, a judgment on its appropriateness and initiation of change of cognition or action. As an example, individuals who recognize emotional impacts of events in one of the domains (e.g., a failure or sub-optimal performance in cyber) affecting their performance in the physical domain (e.g., distraction leading to impaired concentration and reduced physical or cognitive performance), can counter-regulate and apply emotion-regulation strategies.

An individual with a particular accurate judgment of his/her own performance level (high metacognitive awareness) will recognise a potential threat in cyberspace exceeding his/her technical abilities and consider to activate additional personal or technical resources in the physical domain. A person being aware that the outcomes of previous actions were taken under immense time pressure to serve short-term goals served primarily tactical purposes can readjust short-term goals earlier to put strategic goals back into the focus. The ability to be metacognitively aware of one's own performance without underestimation of own capacities or inappropriate over-confidence is considered a relatively stable personality trait that can be quantified and made subject to training and improvement. A crucial role for improvement of metacognitive skills is played by leaders, trainers, and all persons designing training and giving feedback.

As an example for the application of cognitive science in the Hybrid Space model serves the Recognition/Metacognition model [39] for tactical decision-making that involves the ability to recognize situations and supplement with processes of verification and optimal solution resolvement that is relevant to the Hybrid Space. The R/M approach identifies and outlines factors that can be trained to help deal with novel situations that may arise (see [39] for in-depth description). At the meta-recognition stage, agents will need to become aware of evidence-conclusion relationships, critically analyse the arguments that support a conclusion, correct any beliefs through external (collecting more data) and internal (attention shifting or regulating the recognitional process) actions, and quick testing the critical-analysis/correctional process. The meta-recognition component of the model provides information on the metacognitive factors so that it can monitor and evaluate the recognitional process to modify behavior efficiently. This process is dependent on expertise understanding of the Hybrid Space as well as an understanding of the physical demands and psychosocial processes needed (metacognitive skills) to function in it.

4 Future Research

Several authors suggest that cyber officers need a varied skill-set [10, 11]. We agree with these finding and see the Hybrid Space as a tool capable of framing the complex environment that both defines and reveals this skill-set. This is a framework that reflects the novel demands of the future operating environment.

The integration of cyber power into joint warfare presents a research gap that concerns more than just understanding CNO from a technological or human factors view. It requires us to understand the significance of these factors through their interdependency and the reciprocal processes that occur for functioning effectively in the Hybrid Space. At all operational levels agents can affect and are affected by abstraction levels of team and individual performance. Thus, by learning how to support performance in the Hybrid Space we hope to develop efficacy through multiple performance pathways. Research that embraces and leverages cross discipline collaboration is required to establish a pedagogic methodology concerning how to educate, train and accelerate the requisite skills that will enable responsible personnel to operate with superior cognition in the Hybrid Space.

This framework has the potential to reveal the cognitive and metacognitive processes required to conduct future military operations. By categorizing the relevant agents, prioritizing the critical assets and finding novel approaches to measuring adaptation can lead us to better understand the competencies, relationships and processes that occur in the Hybrid Space.

References

1. Ministry of Defence, United Kingdom: Future Trends Programme - Future Operating Environment 2035, 1st edn. First Published 14 December 2015. https://www.gov.uk/government/publications/future-operating-environment-2035
2. Kegan, R., Lahey, L.: Immunity to Change. Harvard Business School Publishing Corporation, Boston (2009)
3. Whitman, M., Mattord, H.: Principles of Information Security, 4th edn. Cengage Learning, Boston (2012)

4. NERC, Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets (2015) http://www.nerc.com/docs/cip/sgwg/Critcal_Cyber_Asset_ID_V1_Final.pdf
5. von Solms, R., van Niekerk, J.: From information security to cyber security. Comput. Secur. **38**, 97–102 (2013)
6. Andrews, J., Buzzi, S., Choi, W., Hanly, S.V., Lozano, A., Soong, A.C.K., Zhang, C.J.: What will 5G be? IEEE J. Sel. Areas Commun. **32**(6), 23–44 (2014)
7. Trujillo, C.: The Limits of Cyberspace Deterrence. JFQ 74, 3rd Quarter 2014 (2014)
8. Tikk-Ringas, E., Kerttunen, M., Spirito, C.: Cyber Security as a Field of Military Education and Study. JFQ 74, 3rd Quarter 2014 (2014)
9. Mancuso, V.F., Strang, A.J., Funke, G.J., Finomore, V.S.: Human factors of cyber attacks: a framework for human-centered research. In: Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting – 2014, pp. 437–441 (2014)
10. Lamay, A., Leblanc, S., De Jesus, T.: Lessons form the strategic corporal - implications of cyber incident response. In: SIGMIS-CPR 2015, 4–6 June 2015. ACM, Newport Beach (2015). ISBN 978-1-4503-3557-7/15/06
11. Røyslien, H.: When the generation gap collides with military structure: the case of norwegian cyber officers. J. Mil. Strateg. Stud. **16**(3), 1065–1082 (2015)
12. Joiner, B., Josephs, S.: Leadership Agility, Five Levels of Mastery for Anticipating and Initiating Change. Wiley, San Francisco (2007)
13. Zanenga, P: Knowledge eyes, nature and emergence in society, culture, and economy. IEEE (2014). 978-1-4799-4735-5/14
14. Paterson, D.M.: Work domain analysis for network management revisited: infrastructure, teams and situation awareness. In: IEEE International Inter-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA). IEEE (2014). 978-1-4799-3564-2/14
15. Sawilla, R.E., Wiemer, D.J.: Automated computer network defence technology demonstration project (ARMOUR TDP). IEEE (2011). 978-1-4577-1376-7/11
16. Zhong, C., Yen, J., Liu, P., Erbacher, R., Etoty, R., Garneau, C.: ARSCA: a computer tool for tracing the cognitive processes of cyber-attack analysis. In: IEEE International Inter-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA) (2015). 978-1-4799-8015-4/15
17. Williams, B.T.: The joint force commander's guide to cyberspace operations. JFQ 73, 2nd Quarter 2014. Major General Brett T. Williams, USAF, is the Director of Operations, J3, for U.S. Cyber Command (2014)
18. Proctor, R.W. Chen, J.: The role of human factors/ergonomics in the science of security: decision making and action selection in cyberspace. Hum. Factors J. Hum. Factors Ergon. Soc. **57**(5), 721–727 (2015)
19. Gutzwiller, R.S., Fugate, S., Sawyer, B.D., Hancock, P.A.: The Human Factors of Cyber Network Defense. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting. vol. 59, no. 1, pp. 322–326. SAGE Publications, September 2015
20. Bonner, L.E.: Cyber Power in 21st Joint Warfare. JFQ 74, 3rd Quarter 2014. Lieutenant Colonel E. Lincoln Bonner III, USAF, is Director of Operations at the Space Operations Squadron Aerospace Data Facility–Colorado (2014)
21. NATO MC 0616: NATO Cyber Defence Education and Training Plan. 6th Draft MC 0616. NATO UNCLASSIFIED (2015)
22. Arnold, T., et al.: Towards A Career Path in Cyberspace Operations for Army Officers. J. Art. Aug. **18**(10), 37am (2014)
23. Dombrowski, P., Demchak, C.C.: Cyber war, cybered conflict, and the maritime domain. Naval War Coll. Rev. **67**(2), 70 (2014)

24. Hu, F.: Cyber-Physical Systems: Integrated Computing and Engineering Design. CRC Press, Boca Raton (2013)
25. Coghlan, D., Brydon-Miller, M. (eds.): The SAGE Encyclopedia of Action Research. Sage, London (2014)
26. Ahmed, S.H., Kim, G., Kim, D.: Cyber physical system: architecture, applications and research challenges. In: Wireless Days, 2013 IFIP. IEEE (2013). doi:10.1109/WD.2013.6686528
27. Sanislav, T., Miclea, L.: Cyber-physical systems – concepts challenges and research areas. CEAI **14**(2), 28–33 (2012)
28. Troxler, P., Lauche, K.: Assessing Creating and Sustaining Knowledge Culture in Organisations (2014). http://www.academia.edu/1964062/Assessing_Creating_and_Sustaining_Knowledge_Culture_in_Organisations
29. Hoffman, R.R., Ward, P., Feltovich, P.J., DiBello, L., Fiore, S.M., Andrews, D.: Accelerated Expertise: Training for High Proficiency in a Complex World. Psychology Press, New York (2014). http://www.psypress.com/books/details/9781848726529
30. Farwell, J., Rohozinski, R.: The new reality of cyber war. Survival (00396338) **54**(4), 107–120 (2012). Academic Search Complete, EBSCOhost
31. Oltromani, A., Noam, B.-A., Cranor, L., Bauer, L., Christin, N.: General requirements of a hybrid-modeling framework for cyber security. In: Military Communications Conference (MILCOM). IEEE (2014)
32. Bennet, K.B.: Ecological interface design: military C2 and computer network defence. In: IEEE 2014 International Conference on Systems, Man, and Cybernetics, 5–8 October 2014, San Diego, CA, USA (2014)
33. Sookermany, AMcD: What is a skillful soldier? An epistemological foundation for understanding military skill acquisition in (post) modernized armed forces. Armed Forces Soc. **38**(4), 582–603 (2012)
34. Castells, M.: Information Technology, Globalization and Social Development. UNRISD Discussion Paper no. 114, Geneva, UNRI (1999)
35. Baas, D., Castelijns, J., Vermeulen, M., Martens, R., Segers, M.: The relation between assessment for learning and elementary students' cognitive and metacognitive strategy use. Br. J. Educ. Psychol. **85**(1), 33–46 (2015)
36. Hannah, S.T., Avolio, B.J.: Ready or not: how do we accelerate the developmental readiness of leaders? J. Organ. Behav. **31**(8), 1181–1187 (2010)
37. Woods, D.D., Hollnagel, E.: Joint Cognitive System: Patterns in Cognitive Systems Engineering. CRC Press, Boca Raton (2006)
38. Jacobs, J.E., Paris, S.G.: Children's metacognition about reading: Issues in definition, measurement, and instruction. Educ. Psychol. **22**, 255–278 (1978)
39. Cohen, M.S., Freeman, J.T., Thompson, B.: Critical thinking skills in tactical decision making: a model and a training strategy. In: Making Decisions Under Stress: Implications for Individual and Team Training, pp. 155–190 (1998)