# Technical Maturity of Human Network Cognitive Systems

Norbou Buchler

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

www.sto.nato.int

# Cognitive Warfare: The Future of Cognitive Dominance

First NATO scientific meeting on Cognitive Warfare (France) – 21 June 2021.
Symposium organized by the Innovation Hub of NATO-ACT and ENSC,
with the support of the French Armed Forces Deputy Chief of Defence,
the NATO Science and Technology Organization / Collaboration
Support Office, and the Region Nouvelle Aquitaine.

Scientific Editors
B. Claverie, B. Prébot, N. Buchler and F. Du Cluzel.

# Chapter 6 – TECHNICAL MATURITY OF HUMAN NETWORK COGNITIVE SYSTEMS

**Dr. Norbou Buchler**[1]

*"Human collaboration and team leadership structure are critical to managing complex technical systems and coordinating effective responses to threats. The notion of maturity of technological solutions for human use (Human Readiness Levels: HRLs) is essential in this context."*

## 6.1 TRENDS IN NETWORK DEVELOPMENT

A first trend is the development of the networked organization. Advances in information and network technologies are significantly transforming the way human organizations operate and communicate. These networked organizations are at the heart of the social, political, military, or economic fabric of the 21st century. Managing and safeguarding the systematic convergence of people, information, and technology is one of the key challenges of our time.

This transformation to distributed network operations is quite recent and has occurred rather rapidly. For military organizations, it took place at the turn of the century, around 2003 for North American countries and their NATO allies, and has impacted many of us, profoundly changing the specialties and even the careers of specialists.

Socially, networked operational environments are massively collaborative: the number of potential collaborations is virtually unlimited. However, they have potential disadvantages such as increasing complexity, and the deluge of information in these networked environments can quickly overwhelm human cognitive abilities. The ongoing challenge is to get the right information to the right person at the right time.

The second trend is one of increasing autonomy: the nature of work is constantly changing due to the blistering pace of technological change. This includes tools and systems of Artificial Intelligence and Automatic Assistance technologies (AI/AA) that are increasingly capable of operating on their own and in concert with human operators.

In military organizations, a major focus remains the interaction of human operators and their tools. Some key aspects underlying this transformation of the Human-Autonomous Agent (HAT) team are calibrating trust levels of the relationship and its transparency, especially with respect to underlying assumptions, uncertainty, and reasoning processes.

Both humans and machines have their strengths and weaknesses. Ultimately, a key marker of the success of this combination is that levels of performance are being achieved through human/machine collaboration that could not previously be achieved without a full and complementary human/machine partnership. One of our concerns remains that the rapid development and complexity of modern artificial intelligence limits our ability to intuit and imagine the future impacts of using new technologies. We still need a lot of experience and experimentation to succeed in this.

The third trend is "Cognitive Warfare" which leverages cyber-attacks, Big Data, and social media for destabilization purposes. Cyber security threats are based on malware, Trojans, and botnets. The convergence

[1] Norbou Buchler holds a PhD in experimental psychology researcher, specialized in cognitive neuroscience (functional MRI) and computational modeling. He works at the Human Systems Integration Division of the U.S. Army Combat Capabilities Development Command (DEVCOM) Analysis Center – Aberdeen Proving Ground, Maryland USA.

of cyber, physical, and social environments is also a place of weakness, with massive attacks on a large scale that specifically target the seams and boundaries of these cyber, physical, and social networks.

The impact of artificial intelligence that leverages large databases and social networks is a major threat. It enables Cognitive Information Warfare (CogIW) on an unprecedented scale to destabilize democracies and undermine alliances. The stealth of attacks, lack of attribution of cause or perpetrator, deception and consequent distrust undermine the social fabric.

The NATO-ACT paper by Cole and Le Guyader (2020) draws our attention to the AI-supported "human domain" (future monitoring and surveillance of allies), sounding an early warning against the destabilization of CogIW campaigns. A broader theme might be about safeguarding digital democracy and bringing cyber-social safeguards such as online authentication of citizens for participation in digital democracy.

## 6.2 THE INSTITUTIONAL DECISION-MAKING PROCESS

This question echoes some of the work of Dr. Alex Kott, Director of Science at the U.S. Army Research Laboratory, entitled "Breakdown of Control." His thesis draws on Control Systems theory and uses historical examples to argue that deception and mistrust within an organization forces compartmentalization and verification measures that significantly slow and impede action and decision making, causing a "breakdown" in organizational decision making (Kott, 2007). These include late decisions (delays), changes in decision thresholds in information warfare, excessive inhibition (timidity) or aggression – low or high gain, self-reinforcing errors, as in feedback loops. See also Kott (2008), Kott and Alberts (2017), Kott and Linkov (2021), Theron, Kott et al., (2019).

The second question concerns our own coalition's decision-making imperative to mitigate the previous threat. How can a well-designed, equipped, and trained organization avoid being hit by such an attack? With its own equipment, this organization can anticipate and respond decisively. Two complementary dimensions are defined here, which are on the one hand the contributions of training and technology, and on the other hand predictive models, human mental models or programmed digital models.

One conceptualization of the military decision-making cycle is known as the "OODA loop" for Observe – Orient – Decide – Act. Also known as Boyd's cycle (1976), it defines a time-competitive process by which an individual or organization observes and orients itself in an operational environment and repeatedly and iteratively makes decisions in light of dynamic events, while acting effectively. It is a useful framework for thinking about organizational functions, workflows and supporting technologies.

We can comment on four different technical areas that support the issue of human decision making and organizational effectiveness (Figure 6-1). These areas ultimately support mission effectiveness.

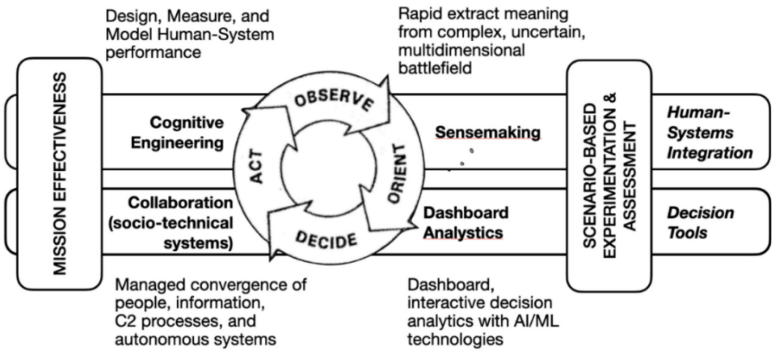


**Figure 6-1: Human Decision Making and Organizational Effectiveness Aligned to the Military Decision-Making Cycle (OODA Loop).**

One can point to the importance of cognitive engineering and human-systems integration. Nevertheless, the majority of this chapter will focus on collaboration and more specifically, the cognitive dimension of networked human systems.

## 6.3 FROM TRL TO HRL OR "HUMAN READINESS LEVELS"

The U.S. Army Combat Capabilities Developmental Command (DEVCOM), and within it the Analysis Center, are interested in ensuring that technology development is well aligned with the needs of the soldier. This means ensuring the maturity of the adaptation of technologies to human users (see Figure 6-2).

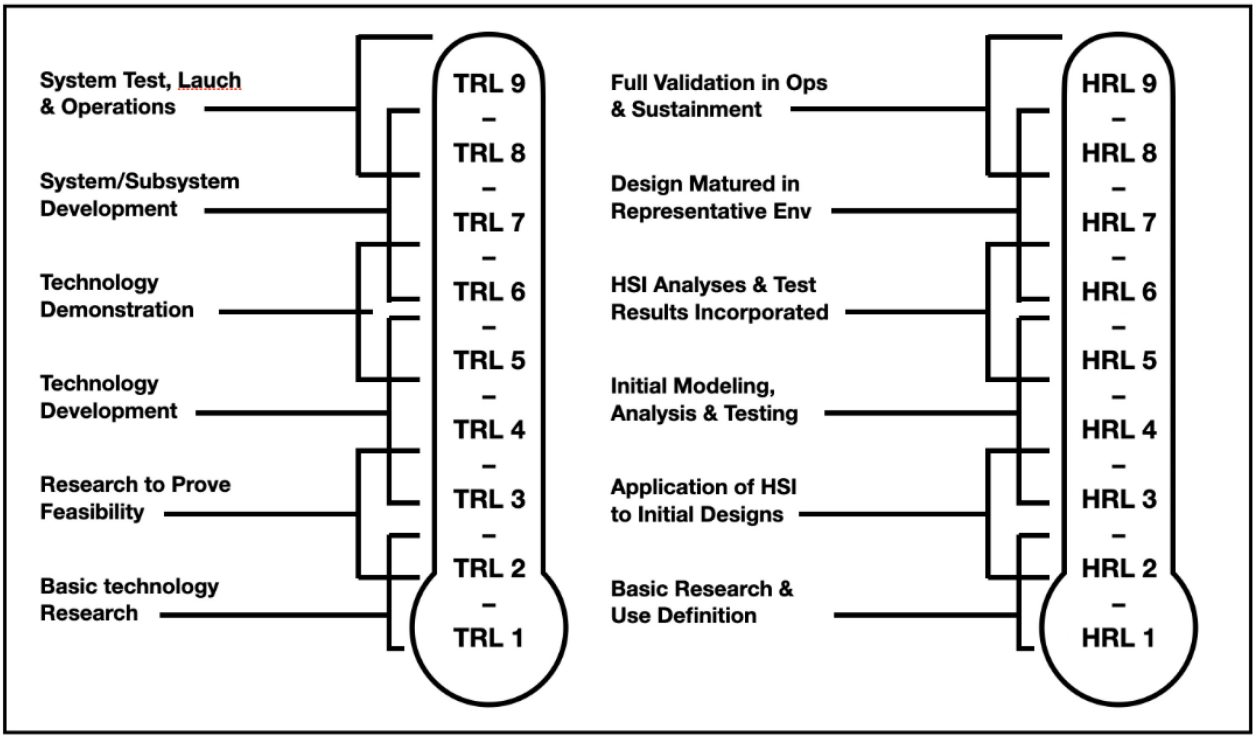


**Figure 6-2: Equivalence Between the Two Scales of Technological Maturity (TRL) and Maturity of Technological Solutions for Human Uses (HR).**

The term TRL, or Technology Readiness Level, has been around since the 1970s, and refers to the level of technological maturity of a given piece of equipment or software, ranging from the first level of concept development through development and operational testing to prototyping (ISO, 2013). One of the key challenges in developing technology is to ensure that it takes into account the human and organizational dimensions of their use; and this is particularly the case for artificial intelligence and complex systems to support Cognitive Warfare.

Dr. Pamela Savage-Knepshield (Savage et al., 2015) is developing the use of the notion of Human Readiness Levels (HRLs) that mirror the logic of TRLs for an easy understanding of human-system integration maturity (Handley and Savage-Knepshield, 2021). This index provides a single number for assessing communication readiness for human use. For each level, there are both input and output criteria.

HRL applies universally, from technology science programs to systems acquisition. This ranges from early identification of human performance-based requirements to user interface design and refinement, through successive user evaluations and full operational testing by humans (Savage-Knepshield et al., 2021). In 2021,

the American National Standards Institute (ANSI) and the Human Factors and Ergonomics Society (HFES) accepted Human Readiness Levels (HRL) as a current standard, made available at (https://www.hfes.org/Publications/Technical-Standards).

The HRL scale provides questions that serve as triggers to consider applicability of multiple human-system integration topics throughout design and development. Ultimately, the HRL scale supports iterative evaluation of human-centered domain principles and provides a single 'human readiness' number to support program decision-makers.

## 6.4 BEHAVIORAL OBSERVATIONS LOGGING TOOLKIT

In terms of Cognitive Engineering, the analysis center is also moving towards the digitization of surveys and behavioral observation data.

A digital toolkit has been developed for the study of all behavioral observation data. It is called the Behavioral Observations Logging Toolkit or BOLT.

The BOLT system is based on a four-step logic (see Figure 6-3). It provides a technological leap in Human-System Integration (HSI) analysis over current mainstream technologies that, even when using handheld devices such as smartphones or tablets, require transcription, are not real-time, do not aggregate data from multiple observers, and do not provide global visibility to leaders of current operations. The logic of the BOLT system is to provide an online representation that allows for the evaluation of training, technology, and operations by supporting all human expert observers, streamlining data collection, tracking, and analysis of information without delay (Garneau et al., 2020).

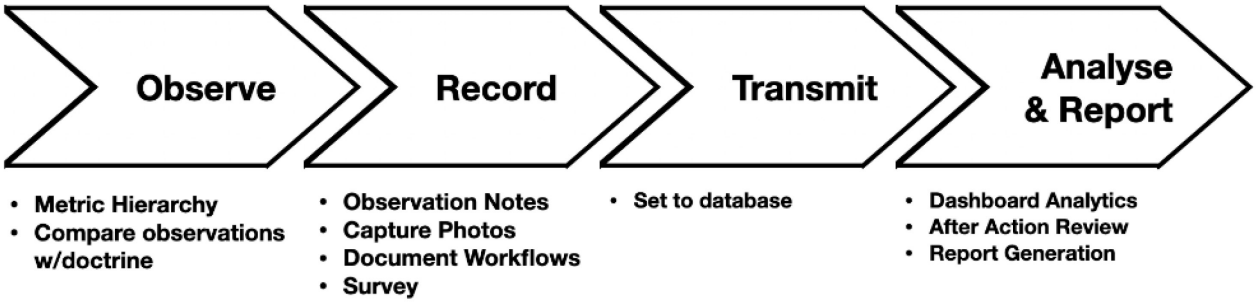


**Figure 6-3: Principles of the BOLT Digital Tablets (Behavioral Observations Logging Toolkit).**

## 6.5 COGNITIVE NETWORKS AND THE COGNITIVE WARFARE AS NETWORK SCIENCE

As in the Wachowskis' movie "Matrix," we can choose the blue pill, and see nothing, or the red one to open our eyes and explore the world as a series of interconnected networks.

Figure 6-4 is from the U.S. Army Field Manual FM 3-13 "Inform and Influence Activities" (2016). It shows six types of networks that span the Political, Military, Economic, Social, Infrastructural, and Informational (PMESSI) domains Individual nodes can represent people, places, or equipment.

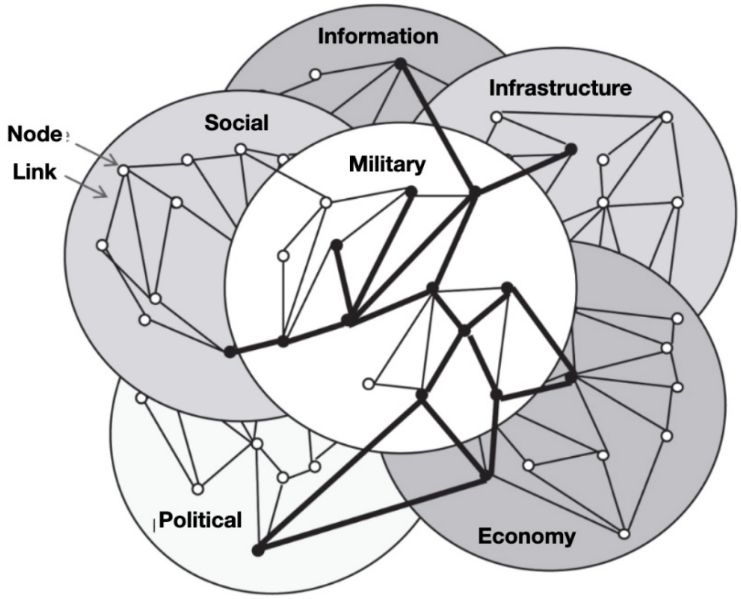


**Figure 6-4: Enhance Capabilities of Soldiers and Commanders to Leverage and Safeguard the PMESII Dimensions to Inform and Influence an Increasingly Complex and Interconnected Operational Environment (from U.S. Army Field Manual, FM 3-13 – Inform and Influence Activities).**

Cognitive Warfare involves mapping all of these different types of networks and exploiting the critical interdependencies that exist between them. For example, in 2015, a Russian sought to destabilize the Ukrainian capital of Kiev with a multi-layered attack. A cyber-attack knocked out critical electricity infrastructure, leaving 200,000 Ukrainians without power in predominantly Russian neighborhoods, and was quickly followed by a disinformation campaign blaming the outage on the Ukrainian government. This hybrid attack was carried out on 3 networks: Infrastructure, Social, Information.

More specifically, our applied work focuses on how to map and understand three of these networks – the military, cognitive/social, and informational networks.

The military transformation of the United States and NATO countries has taken place within a conceptual framework known as "Network-Enabled Operations" (NEO) developed by Alberts et al. (2004). It provides a relevant conceptual framework for understanding human cognition, collaboration, and organizational effectiveness in the military domain. It includes four main principles:

- A strong networking force improves information sharing and collaboration.
- Such sharing and collaboration improves both the quality of information and shared situation awareness.
- In turn, this improvement allows for additional self-synchronization and improves the sustainability and speed of command.
- The combination of these factors significantly increases mission effectiveness.

This framework is cumulative, so communication and information sharing act as a positive feedback loop. Increased information sharing leads to greater shared situation awareness. This, in turn, promotes organizational adaptations such as self-synchronization that ultimately increases overall mission effectiveness. (Alberts and Garstka, 2004).

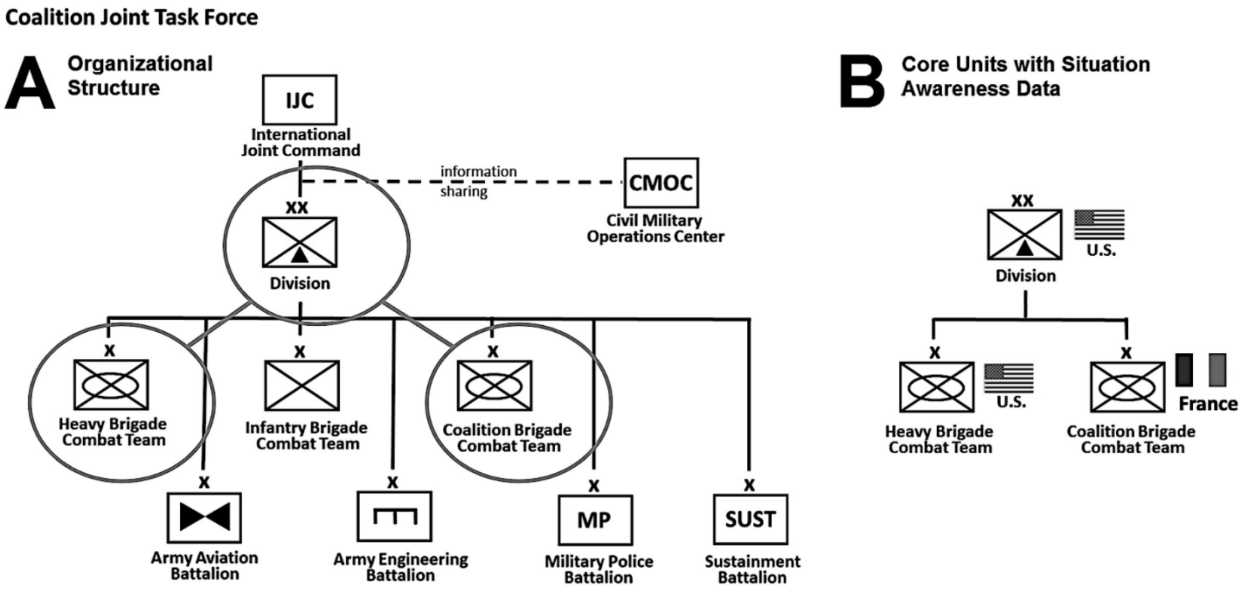


**Figure 6-5: (A) Organizational Structure of the Coalition Joint Task Force During the Experiment. The network organization spans several levels, from the Joint Command to the Division, including the brigade and support battalions. (B) Units practiced: division Mission Command, and two subordinate brigades.**

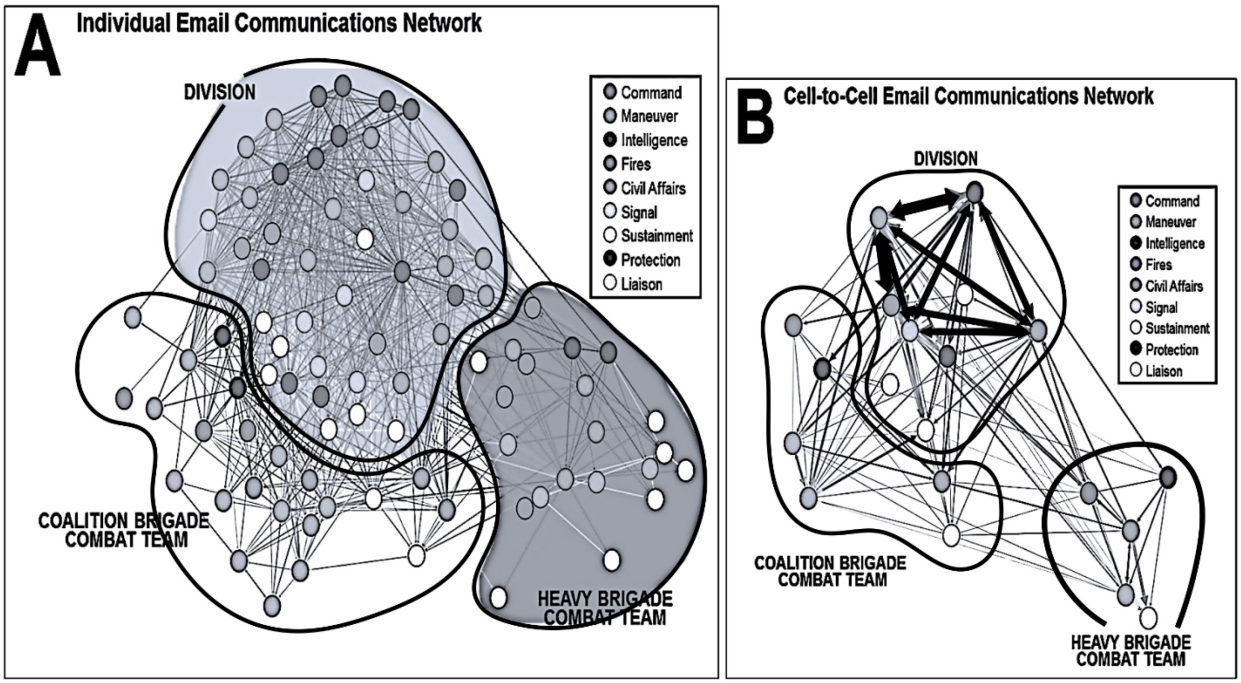


**Figure 6-6: Intra and Inter-Unit Communication Network (Three Structures in Figure 6-5). The color of the cells indicates the functional roles and the thickness of the lines indicate the functional cell of the sender and the volume of the message.**

## 6.5 FORT LEAVENWORTH

In 2016, we focused specifically on the first two principles (Buchler et al., 2016). We examined information sharing and situation awareness during a large-scale military exercise at the Mission Command Battle Laboratory at Fort Leavenworth, KS-USA. A network science approach based on graph theory of collected communications was applied to the entire coalition joint task force organization.

The hypothesis was that "increased information sharing leads to increased situation awareness." The experiment was conducted during a two-week Mission Command Training Exercise (MCBL: Fort Leavenworth, KS).

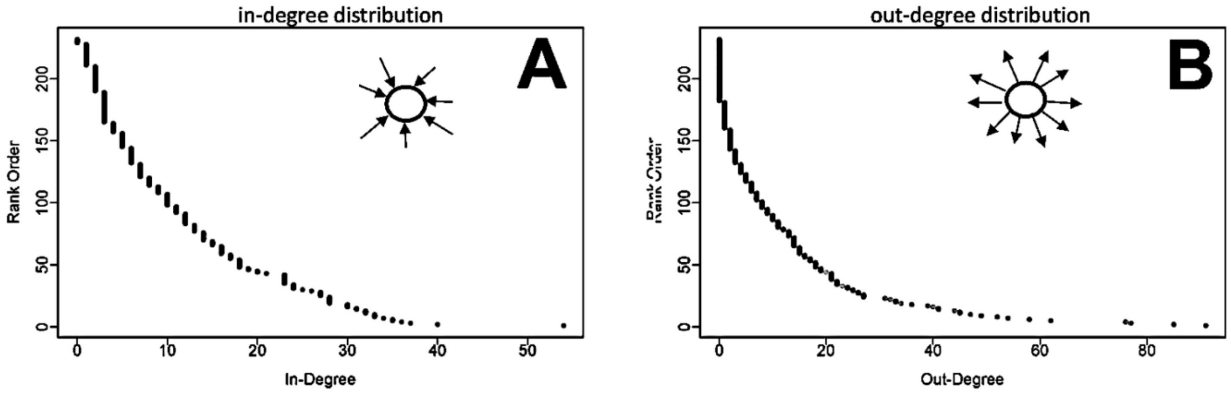


**Figure 6-7: Cumulative Communication Distribution Functions of Email Inputs (A) and Outputs (B) for the Entire Communications Network. The predominance of some command personnel is evident when expressed as a percentage of all ties.**

The three basic units trained in enhanced and equipped communication consisted of Mission Command personnel from one U.S. division and two participating subordinate brigades, one U.S. heavy brigade combat team, and one French coalition brigade combat team.

Individual Situation Awareness data were collected using the SAGAT methodology from participating staff at these three base units, and data processing used "Graph Theory" Analysis on all email communications and Situation Awareness data (collected by quiz).

Email communications are aggregated at the cell level to reveal cell-to-cell functional matches (A) and recombined at the individual node level based on the amount of information exchanged (B).

We observed Pareto imbalances in information sharing within Mission Command's communication networks. Of the 250 people in the network, we find that key individuals at the tail end of the Pareto distribution dominate collaborations. Most individuals, who constitute what we call the "trivial many," have only a few interactions, while a few individuals, who we will call the "vital few," have a very large number of interactions and occupy a dominant place in the interaction network. From a systems perspective, these individuals are most likely to experience cognitive overload and should be the primary beneficiaries of assistive automation.

The study of Situation Awareness was conducted using an electronic "Pop Quiz" based on Endsley's (2000) model of important mission events and developed using a goal-oriented task analysis methodology. It allows for the objective measurement of each individual's SA. These results are analyzed in relation to the previous communication study.

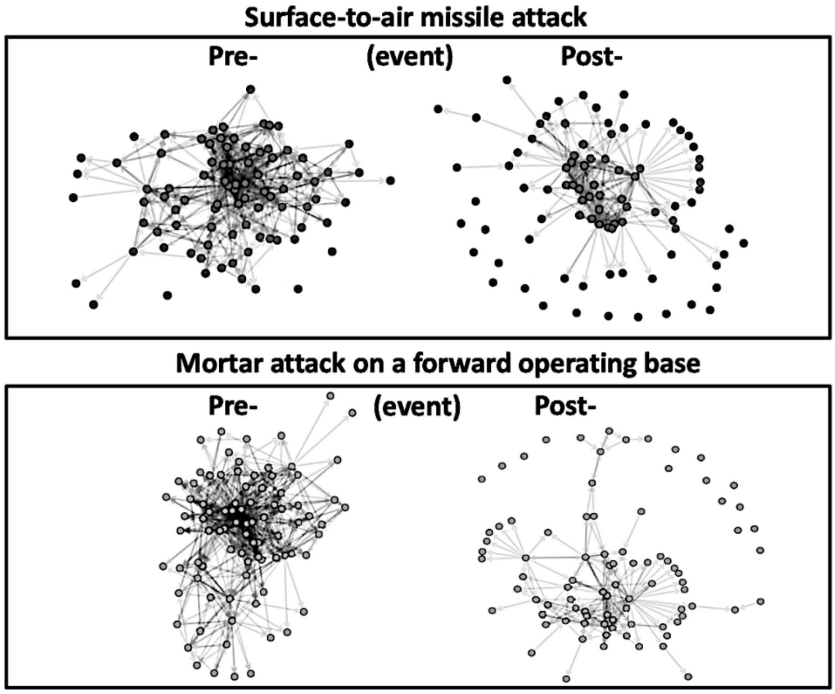


**Figure 6-8: Examples of Reorganization of Unit Command Communication Networks According to Shocks (Pre- and Post-Critical Event: Missile or Mortar Attack).**

The results are detailed in Buchler et al. (2016) and highlight challenges faced by networked military organizations: robust but uneven information sharing, sources and "information sinks," clearly stratified situation awareness, and that information sharing does not always increase situation awareness.

There are still questions that need to be answered. How does the network react to shocks or adverse events? What kinds of organizational adaptations occur (e.g., self-synchronization)? (Fitzhugh et al., 2020). For example, what is the evolution of situation awareness as a function of network reorganization following a shock?

One observational feature concerns the existence of "emergent coordinators" and their role in network reorganization. These roles are unformalized, and each event produced the release of 2 – 5 emergent coordinators (Buchler et al., 2018).

## 6.6 CYBERSIMULATIONS DEVCOM

We were able to study the behaviors of teams of actors during three episodes of a cyber competition, the "U.S. Collegiate Cyber Defense Competition" (CCDC 2016, 2017, and 2018 – www.nationalccdc.org). Our goal was to understand what combination of skills or tools, team dynamics, and leadership style makes a team more or less effective, through the objective measurement of mission effectiveness.

The strategic question was how to study what makes one team better than others. The scenario pitted teams of attackers (the reds) against teams of defenders (the blues) and was designed to foster team-based cyberwork. The simulation environment provided a sufficient degree of realism, with experimental control through performance outcome measures.

The task was broadly consistent with the performance of information security professionals. It consisted of keeping the services that must remain efficiently managed, available, and operational. Teams were required

to complete assigned tasks within a given time frame, such as creating policy documents, making technical changes, attending meetings, responding to incidents, i.e., analyzing cybersecurity incidents and submitting reports, and thwarting adversarial cyber-attacks.

Measures of team quality and performance were sociometric data, with wearable sensors measuring interactions between team members, a survey given to team observers (in 2016 and 2017) to assess the degree of collaboration and leadership style of the team, and skill measures from survey given to the team of defenders to assess experience, communication style, tasks/roles, and team structure.

Factorial analyses on the survey data were conducted based on the three group categories: failure by storming (ranked low), normal (ranked medium), successful (ranked high).

It can be seen that group dynamics evolve over time in a manner consistent with a form of "team maturation" according to Tuckman's (1965) "Forming, Storming, Norming, and Performing" model. This model describes the stages that a team goes through, from the moment a group meets for the first time until the end of a project. In addition, team members evolve in parallel as they progressively reach the status of colleague. The performance of the team depends on the success of this maturation.

The results (Buchler et al., 2018) are summarized and presented, for two competitions, in Figure 6-9. They confirm the need for team structuring with a probable maturation of shared situational awareness as a function of the progress of the experiment with a sequential stage model (Tuckman model). They indicate that the leadership dimension and face-to-face interactions are important factors that determine the degree of success of a team. On expert teams, everyone knows what to do. These high-performing teams exhibit less face-to-face interaction. In addition, it is observed that the factors of good performance vary according to the type of task asked of the team, reflecting the agility and adaptability acquired by a mature team. Thus, it appears that functional specialization within a team and well-guided leadership are significant predictors of detection and speed of effective response to shocks, in this case cyber-attacks.

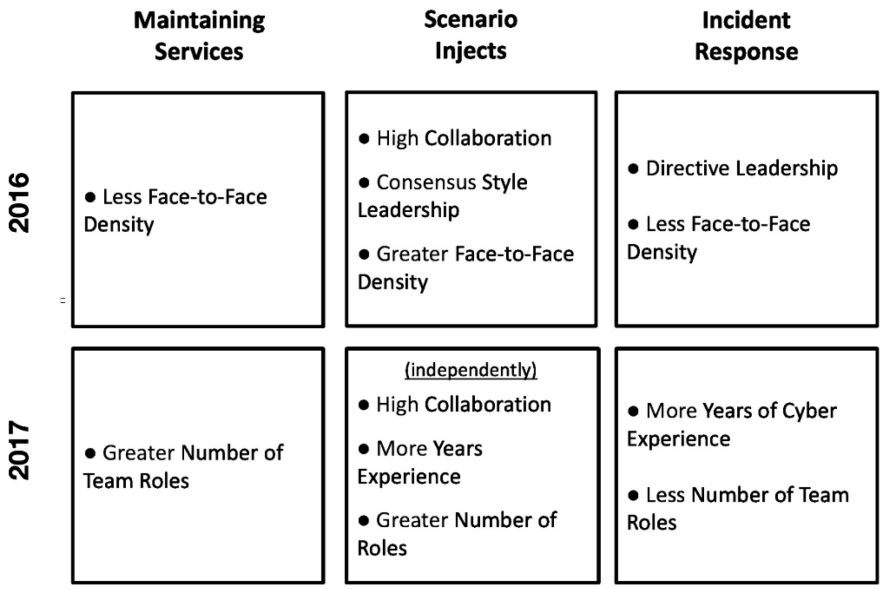


**Figure 6-9: Results of the DEVCOM Experience.**

Given the quantity and depth of skills needed to perform well in the cyber domain, these predictive measures give us some insights to support the development of good cyber teams.

## 6.7 CONCLUSION

These two studies converge in our belief that resilience to attacks, and especially to cognitive warfare, requires training teams and establishing normative work routines for performance by coaching teams to a high level of maturity.

Human collaboration and team leadership structure are critical to managing complex technical systems and coordinating effective responses to threats.

This research has also shown the utility of wearable technology metrics collected during the workday: automatic capture of face-to-face human interactions via infrared sensors, conversation times and voice characteristics of exchanges, physical proximity of employees, and spontaneous physical activity levels captured by accelerometers. Rapid advances in wearable technology and physiological recording are a boost to research, but also to the management of teams working in environments whose characteristics can also be detected online, such as communications. The efficient analysis of "big data" is also a favorable factor.

At the same time, we can bring these studies closer to the theory of decision making with the OODA loop to promote resistance and cognitive performance (see Figure 6-1), with the proposal, in addition to the TRL and HRL scales (see Figure 6-2), of a "Cognitive Technological Maturity" scale built from data on "Human-System Integration" (HSI) and the structuring capacity of the teams in which the operators using the systems are involved.

Figure 6-10 represents, in this scale, the state of the situation of the teams of the current forces and the point of agile adaptation and intelligent organization towards which the forces of the USA and its NATO allies must tend. This goal must be achieved through a coordinated effort of increased collaboration within teams, but also across teams, domains, and nations, and through the development of relevant human metrics to ensure effective human-system integration.

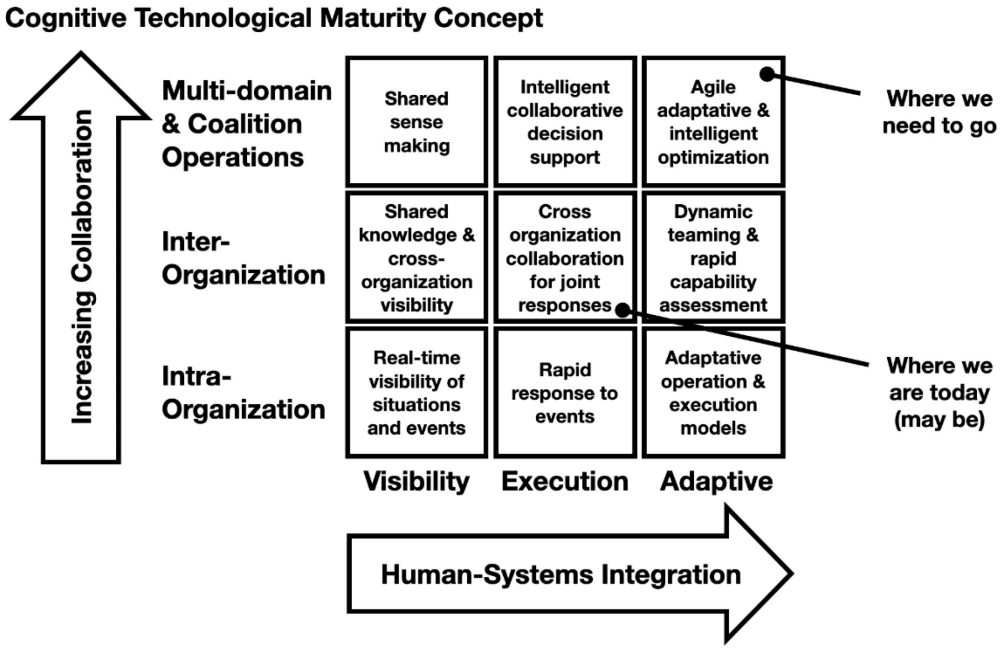


**Figure 6-10: Concept of Cognitive/Technological Maturity Concept (inspired by Lin et al, 2004).**

## 6.8 REFERENCES

Alberts, S.D., Garstka J. (2004). Network Centric Operations Conceptual Framework Version 2.0. Technical Report, US Office of Force Transformation and Office of the Assistant Secretary of Defense for Networks and Information Integration, US Department of Defense: Washington DC, USA. https://www.hsdl.org/?view&did=446190.

Alberts, S.D., Garstka J., Stein, F.P. (2004). Network Centric Warfare: Developing and Leveraging Information Superiority. Department of Defense CCRP Publication Series, Washington DC, USA. http://www.dodccrp.org/files/Alberts_NCW.pdf.

Boyd, J.R. (1976). Destruction and Creation. Command and General Staff College: Fort Leavenworth KS, USA. http://www.goalsys.com/books/documents/DESTRUCTION_AND_CREATION.pdf.

Buchler, N., Fitzhugh, S.M., Marusich, L.R., Ungvarsky, D.M., Lebiere, C., Gonzalez, C. (2016). Mission Command in the Age of Network-Enabled Operations: Social Network Analysis of Information Sharing and Situation Awareness. Frontiers in Psychology, 7, 937, 1-15. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4916213/pdf/fpsyg-07-00937.pdf.

Buchler, N., Rajivan, P., Marusich, L. R., Lightner, L., Gonzalez, C. (2018). Sociometrics and Observational Assessment of Teaming and Leadership in a Cyber Security Defense Competition. Computers & Security, 73, 114-136. https://www.researchgate.net/publication/321057288_Sociometrics_and_observational_assessment_of_teaming_and_leadership_in_a_cyber_security_defense_competition.

Cole, A., Le Guyader, H. (2020). Cognitive: 6th Domain of Operation. NATO-ACT Innovation Hub: Norfolk VA, USA. https://www.innovationhub-act.org/sites/default/files/2021-01/NATO%27s%206th%20domain%20of%20operations.pdf.

Endsley, M. R. (2000). Theoretical Underpinnings of Situation Awareness: A Critical Review. In M.R. Endsley, D.J. Garland (Eds.) Situation Awareness Analysis and Measurement. Lawrence Erlbaum Associates: Mahwah NJ, USA, 3-32. https://www.researchgate.net/publication/230745477_Theoretical_underpinnings_of_situation_awareness_A_critical_review.

Fitzhugh, S.M., Decostanza, A.H., Buchler, N., Ungvarsky, D.M. (2020). Cognition and Communication: Situational Awareness and Tie Preservation in Disrupted Task Environments. Network Science, 8, 4, 508-542. https://www.cambridge.org/core/journals/network-science/article/abs/cognition-and-communication-situational-awareness-and-tie-preservation-in-disrupted-task-environments/47D44CB0AF1F48B39F029E53F25C6655.

Garneau, C.J., Hoffman, B.E., Buchler, N.E. (2020). Behavioral Observations Logging Toolkit (BOLT): Initial Deployed Prototypes and Usability Evaluations. CCDC Data & Analysis Center – DEVCOM Reports. Aberdeen Proving Ground MD, USA. https://apps.dtic.mil/sti/pdfs/AD1099977.pdf.

Handley, H.A.H., Savage-Knepshield, P. (2021). Evaluating the Utility of Human Readiness Levels (HRLs) with Human System Integration Assessments (HSIAs). Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 64, 1, 1537-1540. https://journals.sagepub.com/doi/abs/10.1177/1071181320641368?cookieSet=1.

International Organization for Standardization (2013). Space Systems: Definition of the Technology Readiness Levels (TRLs) and their Criteria of Assessment. ISO 16290:2013. American Society for Testing and Materials – ASTM International Editions: West Conshohocken PN, USA. http://www.iso.org/iso/catalogue_detail.htm?csnumber=56064.

Kott, A. (2007). Information Warfare and Organizational Decision-Making. Artech House Publishers. Norwood MA, USA. https://us.artechhouse.com/Information-Warfare-and-Organizational-Decision-Making-P1031.aspx.

Kott, A. (2008). Battle of Cognition: The Future Information-Rich Warfare and the Mind of the Commander. Greenwood Publishing Group: Westport CT, USA. https://products.abc-clio.com/abc-cliocorporate/product.aspx?pc=C2605C.

Kott, A., Alberts, D.S. (2017). How Do You Command an Army of Intelligent Things? IEEE Computer, 50, 96-100. https://arxiv.org/pdf/1712.08976;How.

Kott, A., Linkov, I. (2021). To Improve Cyber Resilience, Measure It. IEEE Computer, 54, 2, 80-85. https://arxiv.org/pdf/2102.09455.pdf.

La Fleur, C., Hoffman, B., Gibson, C. B., Buchler, N. (2021). Team Performance in a Series of Regional and National US Cybersecurity Defense Competitions: Generalizable Effects of Training and Functional Role Specialization. Computers & Security, 104.

Lin, G., Wang, K.-Y., Luby, R. (2004). A New Model for Military Operations. OR/MS Today, 6 December 2004. https://doi.org/10.1287/orms.2004.06.15.

Savage-Knepshield, P., Martin, J., Lockett III, J., Allender, L. (2015). Designing Soldier Systems: Current Issues in Human Factors (Human Factors in Defence). Ashgate: Burlington VT, USA. https://1lib.fr/book/2836338/3d230e.

Savage-Knepshield, P.A., Hernandez, C.L., Sines, S.O. (2021). Exploring the Synergy Between Human Systems Integration and Human Readiness Levels: A Retrospective Analysis. Ergonomics in Design: The Quarterly of Human Factors Applications, 22 April 2021 (in press). https://journals.sagepub.com/doi/full/10.1177/10648046211009718.

Théron, P., Kott, A., Drašar, M., Rzadca, K., Le Blanc, B., Pihelgas, M., Mancini, L., De Gaspari, F. (2019). Reference Architecture of an Autonomous Agent for Cyber Defense of Complex Military Systems. In Jajodia, S., Cybenko, G., Subrahmanian, V., Swarup, V., Wang, C., Wellman M. (Eds) Adaptive Autonomous Secure Cyber Systems. Springer, Cham. New-York, NY, USA. https://link.springer.com/chapter/10.1007/978-3-030-33432-1_1.

Tuckman, B.W. (1965). Developmental Sequence in Small Groups. Psychological Bulletin, 63, 384-399. http://dennislearningcenter.osu.edu/references/GROUP%20DEV%20ARTICLE.doc.

U.S. Army Headquarters (2016). U.S. Army Field Manual FM 3-13, Information Operations. Army Publishing Directorate: Washington DC, USA. https://www.globalsecurity.org/military/library/policy/army/fm/3-13/fm3-13_2016.pdf.

# REPORT DOCUMENTATION PAGE

| 1. Recipient's Reference | 2. Originator's References | 3. Further Reference | 4. Security Classification of Document |
|---|---|---|---|
| | | ISBN<br>978-92-837-2392-9 | PUBLIC RELEASE |

**5. Originator**

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

**6. Title**

Cognitive Warfare: The Future of Cognitive Dominance

**7. Presented at/Sponsored by**

First NATO scientific meeting on Cognitive Warfare (France) – 21 June 2021. Symposium organized by the Innovation Hub of NATO-ACT and ENSC, with the support of the French Armed Forces Deputy Chief of Defence, the NATO Science and Technology Organization / Collaboration Support Office, and the Region Nouvelle Aquitaine.

| 8. Author(s)/Editor(s) | 9. Date |
|---|---|
| B. Claverie, B. Prébot, N. Buchler and F. Du Cluzel | March 2022 |
| **10. Author's/Editor's Address** | **11. Pages** |
| Multiple | 118 |

**12. Distribution Statement**

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

**13. Keywords/Descriptors**

Cognition; Cognitive bias; Cognitive domain; Cognitive war; Cognitive warfare; Cyber-psychology; Human

**14. Abstract**

This document, published by the NATO-CSO, brings together articles related to the presentations given during the first Symposium on Cognitive Warfare, held in Bordeaux, France, in June 2021, on the initiative of the NATO-ACT Innovation Hub and the Bordeaux-based ENSC, with the support of the French Armed Forces Joint Staff, the NATO-STO-CSO, and the Region Nouvelle Aquitaine. This first Symposium reflected on human cognition, its strengths and weaknesses, its collaborative organization for military decision-making, its relation with and dependence on digital technology, and its social and political dimensions within the context of fierce international competition. The Supreme Allied Commander for Transformation (SACT) and the French Armed Forces Vice-Chief of Defence expressed their views on the topic. This first Symposium was the starting point of a series of meetings and workshops further exploring the subject, on the initiative of NATO CSO and ACT.