WHITE PAPER

Advancing Human-Machine Collaboration in Cyberwork

Robert R. Hoffman
Institute for Human and Machine Cognition
rhoffman@ihmc.us
Esa M. Rantanen
Rochester Institute of Technology
David Schuster
San Jose State University

Abstract

A group of individuals whose backgrounds span cognitive systems engineering, human factors, social sciences, and computer sciences held a meeting in December 2018 at Embry-Riddle Aeronautical University. A consensus was that there was a significant role to be played by psychological sciences in the domain of cyberwork. This White Paper emerged from that meeting. *Our core proposal is to establish a cadre of trusted experts who can provide independent evaluations of proposed or implemented technologies and work systems*. From a human-centered perspective, the technologies must learnable, understandable, usable, useful, and helpful. These criteria form the theme of human-computer interdependence.

The immediate request is for seedling funds to support further planning for the Ψber project.

Introduction: Cyberwork is Deeply Cognitive

Cyberwork is not just technological. Our concern is that a focus on the perceived superiority of the technology can devalue the contribution of human skill and critical thinking. Four examples of the role of cognition are:

1. Effects and influences brought about in cyber and cyber-physical domains are planned, implemented, and matured over weeks, even months.
2. Cyber defense and offense are fundamentally about one person "getting inside the head" of another person to reveal their intent and deception strategy. Humans play a central role in even the most technological forms of deception, including automation, Artificial Intelligence, and algorithmic forms of deception.
3. Since the technology is continuously advancing and adversaries are always adapting, the mental workload for defenders keeps increasing. Learning must be continuous.
4. Cyberwork across the task spectrum requires intensive teamwork. While capitalizing on the specializations of individuals, teams must be adaptive and resilient with regard to roles, responsibilities, mission and context.

Human cognitive capabilities play a key role in all aspects of cyberwork, spanning network analysis and operations, compliance, vulnerability analysis, malware analysis, mitigation, threat emulation, and attribution.

"Psi" (ψ) is a Greek letter used as the symbol for psychology. And as cyber technology advances and threats morph their capabilities, the mental workload for defenders likewise increases. Therefore, the moniker Ψber aptly combines psychology ("Psi") with cyber (-ber) to emphasize the cognitive aspects of cybersecurity. The following question pairs call out the human-machine interdependence in cybersecurity:

The Role of the Human	
Are humans the weakest link in cyberwork? *They make errors, they succumb to hacks.*	Or are humans the strongest link? *They are adaptive, they devise deception ploys, they are able to mitigate attacks.*
The Role of the Technology	
Is technology the strongest link? *It can be validated; it can be controlled.*	Or is technology the weakest link? *It is always changing, it is usually brittle and of limited usability.*

The above four questions can all be answered "Yes."

We need to insure that we have a robust workforce of cyber experts and the best possible technologies, but these must be deeply integrated as "work systems." Human-computer interdependence and collaboration is the focus for a newly-formed group of individuals whose backgrounds span cognitive psychology, human factors, social sciences, and computer sciences. This group calls itself Ψber.

The Ψber Paradigm

The paradigm of Ψber is based on the following principles:

1. Ψber seeks a genuine integration of the human cognitive and social disciplines, achieved through the involvement of recognized leaders in their respective specializations.

2. Ψber adopts theoretical foundation based on the concept of human-machine interdependence and the concept of work system resilience.

3. Ψber adopts the core methodology of Participatory Design, in which cognitive systems engineers work closely together with cyber practitioners to insure that technologies are usable, useful, understandable, and learnable.

The Goals of Ψber

The initial goals of Ψber are:

1. Provide sponsors with trusted experts who can serve as "honest brokers" with regard to the psychology of cyberwork, human-centered technology design, and the creation of human-machine work systems.

2. Provide recommendations for how funding can be directed and how funding programs are conceptualized.

3. Apply results from research in cognitive engineering to benefit the practitioner community particularly with respect to decision making, mitigate human exploitability, and improve human information sharing to avoid biases.

4. Apply results from research in human factors and cognitive engineering to ensure the judicious and realistic integration of Artificial Intelligence and autonomous techniques into cyber defense and offense activities.

5. Support the integration of cognitive science concepts, models and methods into existing and developing instructional programs, competitions, and exercises, spanning government training and academic programs (Centers of Excellence). This will involve going beyond the manifest need to develop a workforce to apply advance training concepts to accelerate the achievement of a workforce of experts.

The Organization of Ψber

Ψber is modeled as both an organization and as a "community of practice." As an organization, its governance will be consensus-based. Ψber will be constituted as a not-for-profit public benefit corporation, enabling it to apply for both grants and contracts. The involvement of individuals is primarily determined by their interests and motivations.

Proposal

This proposal is a request for seedling funds to conduct a start-up activity. That activity will include the following elements in its Statement of Work:

1. Articulate to stakeholders not only how cognitive engineering perspective is crucial for the advancement of cyber capabilities, but also how it can provide tractable solutions in the design of human-machine technologies and work methods;

2. Enumerate the top problems in cybersecurity that can be best—or only—addressed by a deep collaboration of cognitive systems engineers and the cyber workers, including the US Cyber Mission Force;

3. Develop a corpus of cases of inadequate human factors design in cyberwork systems;

4. Develop a corpus of cases of cyber attack/defense in which social-psychological factors were crucial;

5. Conduct a review of literature relevant to Cognitive Systems Engineering in Cybersecurity. This will include cataloguing existing human performance models;

6. Take steps at designing courses in the area of Cyberpsychology;

7. Hold a follow-on meeting, in the Washington DC area, at which Ψber will meet with government stakeholders to discuss and further refine the Ψber concepts. Proximity to governmental cyber agencies

and activities will maximize the opportunities for stakeholders to be involved. The Applied Research Laboratory for Intelligence and Security of the University of Maryland, The Department of Industrial and Systems Engineering of the Rochester Institute of Technology, and the Florida Institute for Human and Machine Cognition have all expressed interest in providing a venue for Ψber meetings, and engaging in initiatives pursuant to the goals of Ψber.

Selected Pertinent References

Henderson, S. (2019, in press). *Deception by Design: Proven Methods for Comprehending, Creating, and Countering Deception*. Artifice, LLC, Epsom, UK.

Trent, S., Hoffman, R.R., Merritt, D., & Smith, S.J. (2019, Spring). Modelling the cognitive work of Cyber Protection Teams. *Cyber Defense Review*, 4 (1), 125-138.

Hoffman, R.R. (2019, Spring). The Concept of a "Campaign of Experimentation" for cyber operations. *Cyber Defense Review, 4* (1), 75-84.

Johnson, M., & Vera, A. (2019). No AI is an Island: the Case for Teaming Intelligence. *The AI Magazine, 40* (1), 17-28.

Trent, S., Hoffman, R.R., and Lathrop, S. (2016, May). Applied research in cyberdefense operations: Difficult but critical. *Cyber Defense Review* [http://www.cyberdefensereview.org].

Lathrop, S.D., Trent, S., & Hoffman, R.R. (2016). Applying human factors research towards cyberspace operations: a Practitioner's perspective. In *Proceedings of the Seventh International Conference on Applied Human Factors and Ergonomics* (pp. 281-293). New York: Springer.

Ψber Participants

POC Robert R. Hoffman, Ph.D., Institute for Human and Machine Cognition [rhoffman@ihmc.us]

Nathan Bos, Ph.D., Johns Hopkins University Applied Physics Laboratory
Susan G. Campbell, Ph.D., University of Maryland
Kelly Caine, Clemson University
Anita D'Amico, Ph.D., Secure Decisions, Inc.
Cynthia Dominguez, Ph.D. (Lt.Col. USAF, Ret.), MITRE
Cleotilde Gonzalez, Ph.D., Carnegie-Mellon University
Robert Gutzwiller, Arizona State University
Thomas Holt, Ph.D., Michigan State University
Gary Kessler, Ph.D., Embry-Riddle Aeronautical University
Vincent Mancuso, Ph.D., MIT Lincoln Laboratory
Kylie Molinaro, Ph.D., Johns Hopkins University Applied Physics Laboratory
Peter Pirolli, Institute for Human and Machine Cognition
Esa Rantanen, Ph.D., Rochester Institute of Technology
Char Sample, Ph.D., Army Research Laboratory
David Schuster, Ph.D., San Jose State University