# Research: Human Cognition

**A new direction in science of cyber security: computational cognition**

**Abstract**

Diffie and Hellman's "New directions in cryptography" provided a foundation for computer security based on computational complexity. Cyber security requires a new direction and new foundations. While we cannot hope to match the depth of the original cryptographic solutions, we cannot afford to ignore the depth of the current cyber security problems. The claim is that the foundations for work in a new direction are available but need to be consolidated in a genuinely unified framework.

**1 - Problem: Computational and cognitive aspects of cyber security**

Back in the 1970s, the advent of computer networks gave rise to a new family of security problems, that required taking "computation" into account. Diffie and Hellman's new direction in cryptography addressed those problems by leveraging the "computational" limitations and capabilities of attackers and defenders. Modern cryptography was subsequently built on the foundations of computational complexity.

That foundation was built on the mathematics of elementary number theory with well-defined principles for posing and solving problems of factorization. Constructive number theory is algorithmic where each step can be identified, analyzed, logically proved, and counted. Counting represents a level of effort; i.e., a computation. Classic elementary number theory largely overlooked such counting although the human ideal of elegance of a proof, itself a kind of counting, is the art of the number theorist. And, for a number theorist, a rigorous proof is the same as truth.

In computer science, the cost of counting steps is an essential property, affecting what can be known about algorithmically solving a problem on a computer. Algorithms were accordingly organized according to the number of steps to solve a given size problem.

Since the 2000s, the advent of cyber space, spanned by networks of humans and computers, gave rise to new families of security problems, addressed under the name of cyber security. This new family of security problems requires taking "human cognition" into account. Many of the overwhelming vulnerabilities that continue to emerge in the realm of cyber security arise from several sources including the "cognitive" capabilities and limitations of attackers and defenders, society's ability and willingness to act and react, and the semantics of the situations under consideration. It is open-world, dynamic, and non-Turing. Truth is now part of human belief and perception.

In this new cyber space, however, there are no clear notions of what to count or what is equal. The familiar ground truth of constructive mathematics and idealized computers is not evident. The accepted scientific truths honed by physical scientists, which has been so successful, is replaced by an Emersonian view of an authentic individual as the arbiter of truth; i.e., "truth" can be contextualized. The social sciences and history have much more to tell us about human nature, crowds and about online behaviors.

Historically for centuries, the task of building such bridges between the natural sciences, the humanities, and the formal sciences has been pursued by scientists and philosophers. The quest for common methodological foundations of social and natural sciences has taken a better part of the XIX and XX centuries.

When social networks recently migrated onto the Internet, with their logs providing steady streams of big data, that data opened opportunities for empirical studies at scale. That data regrettably also created new families of social problems with societal consequences, particularly involving privacy. It also created a tremendously profitable industry of influence, going well beyond the public relations campaigns of the last century. It also posed new problems for law enforcement. The urgency to study and understand has grown more urgent as fringe social cyber communities in this decade were able to challenge social stability and governments. This helped spawn new disciplines, including computational sociology and cyber forensics.

While the Internet as a computer network is globally connected, the dialogues conducted on the Internet (in cyberspace) are surprisingly fragmented, splintered, stove-piped, and islanded. Classic techniques for influence and propaganda are effective to recruit small but significant numbers of participants. The participants in these dialogues are under no obligation to confirm correctness or legitimacy. A group can claim to be an arbiter of truth until it collides with the real world and sometimes even then. Truth has become contextualized and reasoning replaced by manufactured consent and deceits.

Research Task

*Understand the epistemology of cyberspace, its dynamics, and the complexities (and hardness) of justification and deceit.*

**2 - Approach: Cyber security as social cyber-physical security on scientific foundations**

These groups with their mindset honed in their virtual world can threaten the functioning of a vibrant society in the real world. History can be made and altered by a few well-placed, well-timed, determined true believers. Society and democracies today seem ill-prepared for the shift in the power of these new influence campaigns waged over computer networks that can threaten destabilization rather a better informed and enlightened public.

Research Challenge

*Develop a theory and practice of social cyber operations as an emerging sub-domain national security with strategic consequences* on par *with network-centric warfare.*

The proposal is to begin to re-cast the theory of cyber security as a theory of social cyber-physical security, first by building on basic concepts of security protocols applied to dialogues of influence among discussants in social contexts and their framing of truth. The solutions arising from such a theory, in the long run, will be multi-spectrum and multi-paradigm.

Research Claim

*We contend that a unified theory including* ***layered models of channels and networks****, together with methods of* ***semantic analysis*** *and* ***concept mining*** *provides a framework for capturing cognitive and computational aspects of network processes in general, and of cyber security in particular.*

