Cyber Issues Related to
Social and Behavioral Sciences for National Security

Josiah Dykstra, Ph.D.
National Security Agency
February 12, 2017

Introduction

Cyberspace plays an increasingly dominant role in the missions of the intelligence community (IC), and yet the intersection between cyber and social and behavioral sciences (SBS) remains largely undervalued, underappreciated, and underdeveloped. There is a great need for focused SBS research and application across the breadth of IC cyber missions. This white paper outlines some areas of need at the intersection of cyber issues and SBS for national security.

Key challenges, questions, and needs

There are at least three broad areas of need concerning SBS in cyber:

1. **Analysis of Foreign Use of Cyberspace**. The IC's analysis and assessment of online activity is not always informed by considerations of the intelligence targets' individual human traits, attributes, and characteristics, nor by societal and cultural factors. SBS may improve analytical tools and techniques applied to cyberspace, and analysis informed by target-specific social and behavioral traits in cyberspace. This area focuses on the question *what is the intelligence target doing online and why*?
2. **Data Gathering for Cyberspace**. SBS may be applied to cyberspace and used to improve data gathering tools and techniques. SBS is likely to improve analytic tool development through improved interfaces, automated and recommended actions, and assessment of analytic value. Knowledge and application of SBS is also likely to improve the security and effectiveness of cyber-specific data gathering such as computer network exploitation. This area focuses on the question *how can we most successfully find, collect, evaluate, and disseminate the highest-value intelligence from cyberspace?*
3. **Defense of the IC Workforce.** The IC workforce interacts in cyberspace for communication, analytic, mission, and other purposes but defensive security and human

resilience of the IC may be increased with deliberate attention to human and behavioral factors. This area focuses on the question *how can we keep the workforce safe, healthy, and productive, while supporting the mission and protecting civil liberties*?

Examples of key questions in these areas include:

- What social and behavioral attributes can be passively inferred from online activity?
- What social and behavioral factors dominate an individual's online activity and risk decisions, such as whether or not an individual opens a suspicious email?
- What models or human-centric approaches best support cyber system monitoring, including representation and visualization of socio-technical interactions such as human behavior and influence, to aid understanding of the cyber system, infer risk, and identify compromise (including insider threat)?
- How do social and behavioral factors influence individual reaction and response to online threats (e.g. phishing emails) and alerts (e.g. antivirus notifications)? Could such reactions and responses be overridden, influenced, or manipulated?
- For the IC workforce, how do behavioral factors affect the utility and adoption of technology-enabled human-augmentation (e.g. recommender systems) for cyber data gathering?
- How can social and behavioral factors improve analytics for risk analysis, including operational security and insider threat detection? What observable behaviors are good indicators or predictors of security risks or threat risk?

The IC could benefit from a dedicated, centralized, and focused effort to explore questions like these related to SBS in cyber. To my knowledge, such as construct does not yet exist in the United States, but the idea is not unprecedented. For example, the Defence Science and Technology Laboratory (Dstl) in the UK Ministry of Defense, has a focused effort on behavioral science in cyber. Other pursuits – including the NSF Cyber-Human Systems, NSF Secure and Trustworthy Cyberspace, and DHS Cyber Analytics, Behavior and Resilience programs – support scientific advancement in SBS for cyber, but are not tailored or specific to national security needs.

Importance for today and foreseeable future

There is widespread consensus that online activity continues to grow, and expanded worldwide interconnectivity will continue. The Internet of Things will create even more data about individual human users, as we've already seen with devices such as fitness trackers. In fact, the IC should have had a focus on SBS in cyberspace long ago. Unfortunately, the work in cyber-related SBS is disjoint and unfocused particularly for national security objectives.

Thankfully, governments are now starting to recognize the conceptual need for SBS in cyber. The US Federal Cybersecurity Research and Development Strategic Plan (2016) emphasized the need for study of human aspects of cybersecurity, and explicitly called for the "Development of validated models of varied adversary motives, responses, and susceptibility to deterrence actions such as denial, attribution, and retaliation. Understanding and anticipating adversary reaction to defensive actions and discovering their vulnerability to misinformation and confusion would further serve to reverse their asymmetric advantage." Similarly, the UK's National Cyber Security Strategy 2016-2021 says that "[the] Government will ensure that the human and behavioural aspects of cyber are given sufficient attention, and that systems beyond the technical, such as business processes and organisational structures, are included within cyber science and technology."

Anticipated national security benefits

National security derived from cyber analysis today is undeniably productive and valuable. Nevertheless, if the IC continues in a similar trajectory as today without a focus on SBS, our analysis of cyber activity could become overwhelmed by large volumes of disparate data. There is both promise and potential for SBS to enhance both cyber defense and offense for national security if we can learn to harness it appropriately. This promise is easily seen in insider threat defense, where human motivation and action – even as they manifest in online activity – are paramount to protection of our sensitive and classified national security systems. We can also anticipate that SBS will improve intelligence targeting and better understand adversaries' intent.

References

Bandi, S., M. Gratian, M. Cukier, J. Dykstra, and A. Ginther. 2017 “Correlating Human Traits and Cyber Security Behavior.” In Review.

Bashir, M., C. Wee, N. Memon, B. Guo. 2017. “Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool,” *Computers & Security*, Volume 65, March 2017, pp. 153-165.

Bhatt, Sh., and T. Santhanam. 2013. “Keystroke dynamics for biometric authentication—A survey.” *Pattern Recognition, Informatics and Medical Engineering (PRIME), International Conference on*, pp. 17-23.

Briggs, P., D. Jeske, and L. Coventry. 2016. "Behavior Change Interventions for Cybersecurity." *Behavior Change Research and Theory: Psychological and Technological Perspectives*, pp. 115-135.

Dykstra, J. and C. L. Paul. 2015. “Stress and the cyber warrior: cognitive workload in a computer operations center,” *Journal of Sensitive Cyber Research and Engineering*, vol. 3, no. 1, pp. 1-23.

National Science Foundation, “Cyber-Human Systems (CHS),” https://www.nsf.gov/cise/iis/chs_pgm13.jsp.

Pfleeger, S.L., and D. D. Caputo. 2012. “Leveraging behavioral science to mitigate cyber security risk,” *Computers & Security*, Volume 31, Issue 4, June 2012, pp. 597-611.

Shi, Weidong, et al. 2011. "Senguard: Passive user identification on smartphones using multiple sensors." *Wireless and Mobile Computing, Networking and Communications (WiMob), 2011 IEEE 7th International Conference on*.

U.K. Government. “National Cyber Security Strategy 2016 to 2021,” November 1, 2016, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

U.S. Government. “Federal Cybersecurity Research and Development Strategic Plan,” February 2016, https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf.

Vieane, A. 2016. “Addressing Human Factors Gaps in Cyber Defense,” *Proceedings of the Human Factors and Ergonomics Society 2016 Annual Meeting*.