Integrating Ethical Sensemaking into Cybersecurity: A Problem-Based Learning Approach

Jordan Richard Schoenherr,[1,2] Robert Thomson,[1] & Aryn Pyke[1]

Jordan.Schoenherr@carleton.ca
Robert.Thomson@westpoint.edu
Aryn.Pyke@westpoint.edu
[1]Army Cyber Institute, US Military Academy
[2]Department of Psychology / Institute of Data Science, Carleton University

Abstract. Cyberoperations present unique ethical challenges that are often left unaddressed in contemporary approaches to education. Despite an understanding of the technical affordance of network architecture, security protocols, and software vulnerabilities, this in no way guarantees that software developers and cyberoperatives understand or use the ethical affordances of these systems. However, given that the ethical features of cyberspace are defined in terms of both a social and technical context, educational and training activities should be developed in comparable situations. Following a review of the ethical considerations associated with cyberoperations, we consider the use of problem-based learning (PBL) to develop ethical sensemaking competencies. We then consider the adaptations of a task based on PBL (capture-the-flag) for the development of these skills in social simulation studies.

Keywords: ethics sensemaking, problem-based learning, capture-the-flag, cybersecurity

1 Introduction

Networks are penetrated every day, affecting typical users and prominent public figures. Consequently, there is an increased need for the development of a cyber workforces that has a broad range of competencies (e.g., Thomson, 2019). Ethics of software development, cybersecurity, cyberoperations have become a topic of increasing concern (e.g., IEEE, 2016). With the emergence of many professional and legal standards, the rapid evolution of technology, and the erasure of geographic boundaries in cyberspace, ethics education and training programs must be developed to address these concerns. Following a review of these standards and the efficacy of problem-based learning (PBL) tasks such as cyber capture-the-flag (CTF), we outline a number of features of a CTF task that can help develop ethical sensemaking competencies in network security professionals that can be used to simulate social situations.

2 Ethical Issues in Cybersecurity

Software developers and network security professionals must be located at the core of ethics curriculum for cyberoperations. The roles and responsibilities of developers, their values and behavior, as well as the physical and virtual work environments that they operation in must be addressed in substantive ways. (Council, 2018) The requirement of continuing professional development (CPD) should also be a feature of an ethics curriculum (e.g., Kennedy, 2005).

In most cases, developers will need to consider how a user will typically interact with the networks, software, and how they will interpret and use the output of these systems. In additional to technical issues that can arise in terms of the creation and management of these networks, ethical issues have also been independently examined (Christen et al., 2020). These issues include how to treat log files containing user activities, the level of encryption required, whether and to what extent a program should be used, anticipating how software can be misused, and how much effort should be placed in defending users' data if it is requested by a governmental organization. The response to each of these questions is nuanced and embedded within specific events. Consequently, developers must consider organizations code of conduct, collective agreements, as well as local, national laws, and international laws. In the context of cyberoperations within warfare, it is less clear that developers have the necessary there will likely be significant conflict of values and competencies. Moreover, if unprepared, their actions are likely to have intended (e.g., to disable a network, physical infrastructure) and unintended consequences (e.g., infection of adjacent systems, compromising confidential files). Individuals that are removed from the specifics of the situation are unlikely to be well situated to address these concerns.

Ethical Issues. An exhaustive list is outside the scope of the present article. However, a number of general frameworks and guidelines have been established in the information and computer science more generally. For instance, Mason (1986) notes that four considerations values are critical to information ethics: privacy, accuracy, property, and accessibility. More recently, van de Poel (2020) identifies four core value clusters that are critical to cybersecurity: security, privacy, fairness, and accountability. Each of these values can come into conflict (e.g., privacy-security, security-fairness). For instance, van de Poel acknowledge that the ethics of cybersecurity studies typically focuses on the values and conflicts between security and privacy, i.e., the monitoring required by security necessarily result in losses of privacy. However, these values need no conflict. Rather the assumption of the inevitability of value conflicts can occur when considering values at too general a level. For instance, if privacy is conceived of in terms of confidentiality, then security can increase privacy due to the protection of sensitive information. Moreover, while accountability implies transparency, seemingly placing it into conflict with privacy, accountability does not require total disclosure of information. Consequently, a more nuance understanding of values and potential conflicts is required.

Similar ambiguity can be identified in the context of cyberoperations. One area where this is immediately clear are the educational practices referred to as 'ethical hacking' (Palmer, 2001). Ostensibly, instruction provides learners with the ability to engage

in “white hat” or “grey hat” operations – penetrating a network in order to identify its vulnerabilities (Engebretson, 2013; Harper et al., 2011). However, by providing these lessons, educators have given learners the tools to engage in malicious forms of this behavior without understanding the implications of their actions (Jamil & Khan, 2011; Georg et al., 2015). In the absence of monitoring and regulation mechanisms, educators are leaving network security professionals to make decisions concerning the ethical issues that are relevant to a specific context.

3 Ethical Sensemaking in Cybersecurity

At its core, ethical sensemaking requires an understanding of the affordances of an environment. Consequently, when adapting this approach to cybersecurity practices the knowledge and skills required of a network security professional must be defined.

Cyber Expertise. Cybersecurity expertise reflects a broad set of competencies including knowledge of attack strategies, kinds of malware, software vulnerabilities as well as principles for defense and cryptographic techniques (Thomson, 2019). At a cognitive level, this technical knowledge is likely organized into schemata that can be used in complex decision-making environments, resulting in the rapid allocation of attention to relevant features. In contrast, little attention has been paid to the ethical affordances of these systems. For instance, although the Department of Homeland Security’s National Initiative for Cybersecurity Careers and Studies (NICCS) Cybersecurity Workforce Framework (see also, Dawson & Thomson, 2018), the framework only makes a minimal mention of ethics (K0003; i.e., “laws, regulations, policies, and ethics”). Moreover, ethics is neither explicitly defined nor discussed. Consequently, ethical sensemaking requires understanding the relevant standards and principles, the underlying system architecture, as well as how individuals will trust and use a system.

More generally, sensemaking (e.g., Weick et al., 2005) is a continuous judgment and decision-making process that requires the construction of meaning for, and interpretation of, an otherwise ambiguous situation. In that most situations are underdefined in terms of their ethical affordances, sensemaking approaches have been adopted in ethics (e.g., Sonenshein, 2007). For instance, in the context of virtual environments and autonomous and intelligent systems, Schoenherr (2020) notes that sensemaking requires an understanding of the moral developmental stage of the learners, the effects of attention and memory on decision-making, the social identity and category of the object and subject of the ethical decision-making process, and the available and activated social schemata. In terms of interactional schemata, Schoenherr and Thomson (2020) have noted that sensemaking in cybersecurity has often been based on a limited set of analogies (e.g., Cyber Hiroshima, guerilla warfare, Cold War). However, analogies can emphasize and deemphasize crucial features of the environment, leading to biased decision-making. Instead, they argue that predicting agents’ behavior in a social network requires an understanding of the schemata that the use in a situation. For instance, cyberoperations can be considered in terms of a ‘chicken game’ wherein both sides are antagonistic to one another and fearful of cessation of adversarial actions (e.g., reciprocal aggression) or they can be understood in terms of an assurance dilemma wherein

mutual cooperation is emphasized (e.g., sharing malware knowledge). Consequently, providing learners with a task embedded within a relevant context should facilitate the acquisition of ethical sensemaking competencies.

4 Problem-Based Learning Approaches

Developing an instructional activity requires that we consider both the evidence supporting a tasks construct validity as well as the programmatic context in which it is implemented. In the case of an ethical sensemaking task, it must be adapted to the competencies and skills associated with cybersecurity as well as the curriculum of the institution. Thus, rather than adopting a curriculum-level approach that would be subject to change in dynamic learning environments such as cybersecurity, modularized tasks should be created that develop specific competencies using a combination of contemporary programming languages and systems along with robust engagement strategies (e.g., Thomson, 2019).

One general approach to develop these competencies is problem-based learning (PBL, Barrows, 1986; Jonassen, 2000; Servant-Miklos, et al., 2019). PBL reflects a learner-centered approach to education that uses realistic, group-based self-directed learning. In order to guide learners' performance in a task, educators or tutors are available for limited guidance (Servant-Miklos et al. 2019). Meta-analyses of PBL suggest its effectiveness, with PBL being most effective in specific educational contexts (Walker & Leary, 2009).

4.1 Gamification and Capture-the-Flag Competitions.

Gamification of educational task has received increased interest in recent years (Nah, et al., 2014; Kiesler, et al., 2011). Games have the potential to engage learners, developing important features of character such as creativity, persistence, and resilience (McGonigal, 2011). In Cyber CTF competitions, teams solve hands-on computer security challenges that include content relevant to the types of threats and problems faced by cyber-security professionals (e.g., digital forensics, cryptographic methods, software reverse-engineering, web security, and network traffic analysis) providing a simulation of the kind of tasks and environments that they will work within.

CTF competitions exist to support a wide variety of education and knowledge levels, from middle and high school levels to the levels that would challenge established security professionals (McDaniels et al., 2016). Solvers are not expected to rely only on their own pre-existing knowledge, but rather to collaborate and use the internet to discover possibly relevant information, methods and/or tools. Many CTF competitions are provide participants with sets of categories that vary in terms of their difficulty, much like the gameshow Jeopardy. Participants in these tasks can then freely select which problem from a set they wish to solve. Once a problem is solved, learners will find a 'flag', represented by a predefined set of characters, i.e. {this is a flag}. The team then enters the corresponding string into a competitor's website, and their team is awarded points. The competition is often mediated through a web site interface. This

approach enables learners to explore features of the problem space using a variety of strategies.

Cyber Capture the Flag Exercises contains many key characteristics of problem-based learning (Savery, 2015; Walker & Leary, 2009), including:

i) Collaboration (team-work);
ii) Student-centered & Self-directed Learning;
iii) Content relevant to real world problems;
iv) Inclusion of Complex & Ambiguous Problems.

One such competition that is geared to middle and high schools' students is PicoCTF ('pico', here, meaning 'little'; picoctf.com; Owens, Jones, & Carlisle, 2019). Traditional CTFs target students with significant competitive experience and therefore do not tend to include game-like interfaces, graphics, or story-lines. In contrast, PicoCTF was designed with graduated gameplay to bootstrap student learning from novice through relative expert. PicoCTF has a story-driven game option (for the interface, see Figure 1).

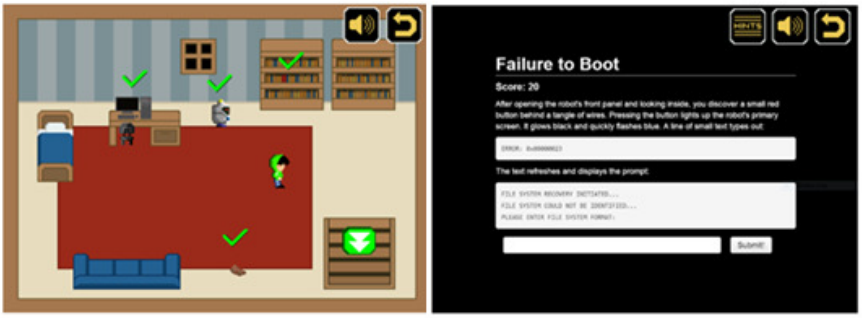

***Figure 1*. The Game-Based interface (left) and Text-Based Interface (right) for PicoCTF.**

The Text-Based Problem Viewer displays the description for each challenge, ideal for older browsers and serious competitors. The Game Viewer is an HTML5 game developed in part by a student-run CMU Entertainment Technology Center team consisting of artists, game play engineers, and producers. In the game, the player can explore and interact with the world by clicking on objects to view challenges. The game was divided into multiple levels of increasing difficulty, each advancing the story and increasing in difficulty. This improved the entertainment value of the competition for relative novice players. In post-competition surveys, 75% of students who scored under 500 points used the game interface while experts (scoring >500) only used the game viewer approximately 10% of the time.

4.2 Positive Learning Outcomes

Problem-based CTF challenges have been shown to be an effective instrument for attaining learning objectives (Carlisle et al., 2015). For instance, when included in coursework, CTF challenges are associated with an increase in student motivation in the classroom, increasing overall time spent studying by emphasizing self-directed learning (Zhang et al., 2013). In addition, the collective identity developed by organizing these competitions into virtual classrooms further improved outcomes relative to students who did not participate as part of a classroom. (Owens, et al., 2019; White et al., 2010) Specific to PicoCTF, by increasing problem difficulty gradually, it is possible to scaffold learning without intimidating students with complex terminology and novel problems.

Outside the classroom, major technology companies use problem-based cybersecurity challenges as a way to screen potential applicants. Several companies have developed their own underlying skill and problem-solving assessments to screen for key aptitudes in their cyber applicants such as outside-the-box thinking, fluid intelligence, and a lifelong love for learning. (Dawson & Thomson, 2018) In addition, applicants showing a history of competing at CTFs can demonstrate sustained and objective improvement in real-world applications, which goes beyond simple cyber-based certifications.

5 Ethical Sensemaking in a Capture-The-Flag Exercise

The positive learning outcomes associated with Cyber CTF along with the context that the task is presented in, make it an ideal platform for developing ethcial sensemaking abilities. The adaptation of a CTF task into one that can develop ethical sensemaking competencies can be relatively straightforward. Many contemporary games have ethical scoring systems embedded within them, making them useful platforms for ethics training (Schoenherr, 2020). This can take the context of flags of differential value or dual-currency approaches. We will now consider three main features of problem-based learning that can be adapted to create ethical sensemaking tasks using the CTF paradigm.

Identifying Ethical Affordances. At the core of sensemaking approaches is providing learners with the ability to ethical affordances of the situation, i.e., those features that are associated with unethical or ethically ambiguity behaviors. In the context of cybersecurity, this can be understood in terms of how network defense and malware are designed. For instance, developers of malware with cyber-physical implications (e.g., Stuxnet; Genge et al., 2011) should consider the nature and extent of the damage caused following malware deployment, what risks there are in widespread disruption to non-targeted systems, and the consequences of misattribution. For instance, CTF narratives can be created that demonstrate the unintentional impact of malware on non-target populations. Similarly, network surveillance must also consider the extent to which personal and organization information is placed at risk. For instance, cyberoperations are often confronted with ill-defined network boundaries and grey legal areas (e.g., defending forward; Flynn, 2020), For instance, should one hack-back at a bot-net client computer, which is most likely an unwitting user who downloaded the wrong software?

Of equal importance to understanding these general ethical affordances is determining whether learners can identify what features of a program relate to formal standards and policies. For instance, Senarath et al. (2019) examined the extent to which software developers used Privacy Engineering Methodologies (methods for ensuring user privacy during software development). They found that the perceived usefulness of the privacy methods as well as their compatibility with a developer's approach were the main determinants of whether the methods were used or not. Consequently, problem-based learning tasks can direct learners' attention to these features. In the context of cyber CTF education tasks, after action reviews (debriefings) can also be used to determine which ethical affordances learners understood, applied, and were affected by.

The Many Hats of Cyberoperatives. Over the course of their career, cyberoperatives might be required to engage in black, grey, and white operations. Each of these activities represents a role with an associated schema. In the case of white hat operations, cyberoperatives will be working in the constraints of domestic and international laws in order to fulfill organizational goals or national security objectives. Thus, instructors can assess the extent to which learners are aware of how general legal frameworks apply to a specific situation. Specific variants can also require learners to engage in the healthcare context, governmental, and non-governmental organizations. Moreover, depending on design of the task, learners can be placed under speeded stress in order to see how rapidly they can make these decisions and which affordances are most salient.

In contrast, black hat operations will violate some or all standards and legal frameworks. Black hat operations represent situations in which learners can use all possible technical affordances to software and hardware in order to penetrate a network. Even in the event that a cyberoperative will never engage in black hat operations, it is still a useful activity to understand how these individuals react/respond in order to predict their behavior in certain situations and understand fully the capability of the devices and networks that are currently in use to identify their vulnerabilities. However, by framing tasks as 'black hat operations', learners might have different exchange schemata activated (e.g., Schoenherr, 2020; Schoenherr & Thomson, 2020).

Social Influence and Contextual Factors. A basic feature of ethical sensemaking is the ability to identify ethically relevant features of a situation as well as the set of possible responses. Problem-based learning, and capture-the-flag tasks in particular, can teach learners about ethical affordance as well as the importance of social influence, conformity, and obedience. For instance, studies of obedience to authority demonstrated that the majority of individuals would engage in ethically questionable behavior given the specifics of the situation (Blass, 1999). Moreover, studies have also indicated that peers can influence ethical behavior, with cheating more likely to occur when individuals have peers that cheat (McCabe & Trevino, 1997).

Similar situations might occur in the context of cyberoperations. Cyberoperatives might start out engaging in white hat operations such as network defense. However, over time, more proactive defense measures might result in network intrusion or direct requests from superiors to engage in conflict-promoting behavior. CTF tasks can help develop ethical resiliency by demonstrating how learners can identify the circumstances leading to these situations. For instance, the collective identity that is developed during

these tasks can be exploited, resulting in groupthink concerning what actions are ethically appropriate.

6 Considerations for Modeling Ethical Behavior

A challenge in modeling ethical behavior is the lack of common-sense reasoning in extant models. Two main techniques in modeling ethical behavior include deontological models (rule-based) and utilitarian (value-based; Yilmaz & Sivaraj, 2019). Both systems rely on constraint-satisfaction as a mechanism to support ethical decisions in the decision-making process (Yilmaz, et al., 2017; McLaren, 2006). A challenge for any static rule-based system is that ethical affordances are generally context-sensitive, and rules are usually too-strict to capture real-world nuance. Utilitarian models can be more flexible, but are a more complex as the relative 'value' of ethical behavior is complex to define and may not accord with many values (e.g., *no man left behind* does not maximize effectiveness, but does have positive morale implications).

To promote the development of effective models, the data from ethical problem-based learning approaches can be used to model and predict effective collaborative cyber workforce strategies and individual differences associated with performance. Interactions between ethical affordances, social influence, and roles (e.g., white hat or black hat) can provide critical insight into vulnerabilities in network security personnel's responses to situations. By manipulating other factors such as time pressure, the limits of cybersecurity professionals can be identified and modelled to identify areas where autonomous and intelligent network security systems should be implemented.

7 Conclusions

The set of ethical norms and conventions applicable to software developers, network security professionals, and cyberoperatives is at once rich and ill-defined. Professional codes of conduct, international standards, and individual morality will all contribute to an ethical sensemaking process. Although professionals might understand the technical affordances of software and networks, this does not address their ethical sensemaking competencies. Available evidence also suggests that learners have difficulties identifying these issues (Senarath, et al., 2019). However, given the technical nature of cyberoperations, learners must be presented with ethical challenges in a relevant environment to sensitize them to these features. Didactic tasks that outline ethical principles and standards are likely to be insufficient in achieving these goals. In the tradition of PBL, cyber CTF competitions present one means to achieve this. These tasks can vary the ethical standards that are applicable to a situation, the nature of these operations (e.g., black, grey, or white hat), as well as the social context in which these operations occur.

8 References

ACM (2018). *ACM Code of Ethics and Professional Conduct*. ACM Council.

Barrows, H. S. (1986). A taxonomy of problem-based learning methods. *Medical education, 20*, 481-486.

Blass, T. (1999). The Milgram Paradigm after 35 years: some things we now know about obedience to authority. *Journal of Applied Social Psychology*, 29, 955-978.

Carlisle, M., Chiaramonte, M., & Caswell, D. (2015). Using ctfs for an undergraduate cyber education. In *Proceedings of the 2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*.

Christen, M., Gordijn, B., & Loi, M. (2020). *The Ethics of Cybersecurity*. Springer.

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology. doi: 10.3389/fpsyg.2018.00744*

Engebretson, P. (2013). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* Elsevier.

Flynn, M. J. (2020). Civilians 'Defending Forward'in Cyberspace. The Cyber Defense Review, 5(1), 29-40.

Genge, B., Fovino, I. N., Siaterlis, C., & Masera, M. (2011, March). Analyzing cyber-physical attacks on networked industrial control systems. In International Conference on Critical Infrastructure Protection (pp. 167-183). Springer, Berlin, Heidelberg.

Georg, T., Oliver, B., & Gregory, L. (2018). Issues of Implied Trust in Ethical Hacking. *The ORBIT Journal, 2(1), 1-19*.

Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G., & Williams, T. (2011). *Gray Hat Hacking: the Ethical Hackers Handbook.* McGraw-Hill Osborne Media.

IEEE Global Initiative (2016). *Ethically Aligned Design*. IEEE Standards.

Jamil, D., & Khan, M. N. (2011). Is ethical hacking ethical. . *International journal of Engineering Science and Technology, 3*, 3758-3763.

Jonassen, D. H. (2000). Toward a Design Theory of Problem Solving. *Educational Technology Research and Development, 48*, 63-85.

Kennedy, A. (2005). Models of continuing professional development: A framework for analysis. *Journal of In-Service Education*, 235-250.

Kiesler, S., Kraut, R. E., Koedinger, K. R., Aleven, V., & Mclaren, B. M. (2011). Gamification in education: What, how, why bother. *Academic Exchange Quarterly, 15*, 1-5.

McCabe, D. L., & Trevino, L. K. (1997). Individual and contextual influences on academic dishonesty: A multicampus investigation. *Research in higher education*, 38, 379-396.

McDaniel, L., Talvi, E., & Hay, B. (2016). Capture the flag as cyber security introduction. *In Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS) (pp. 5479-5486).* IEEE.

McGonigal, J. (2011). *Reality Is Broken: Why Games Make Us Better and How They Can Change the World.* New York: Penguin Press.

McLaren, B. M. (2006). Computational models of ethical reasoning: Challenges, initial steps, and future directions. IEEE intelligent systems, 21(4), 29-37.

Nah, F. F., Zeng, Q., Telaprolu, V. R., Ayyappa, A. P., & Eschenbrenner, B. (2014). Gamification of education: a review of literature. . In *International Conference on HCI in Business* (pp. 401-409). Springer.

Owens, K., A, F., Jones, L., & Carlisle, M. (2019). pico-Boo!: How to avoid scaring students away in a CTF competition. In *Colloquium for Information System Security Education.*

Palmer, C. C. (2001). Ethical hacking. *IBM Systems Journal, 40*, 769-780.

Savery, J. R. (2015). Overview of problem-based learning: Definitions and distinctions. In *Essential readings in problem-based learning: Exploring and extending the legacy of Howard S. Barrows* (pp. 5-15).

Schoenherr, J. R. (2021). Ethics Sensemaking and Autonomous and Intelligent Systems: Ethical Features of A/IS Affordances. In Frontiers of AI Ethics (DeFalco, J. & Hampton, A.). Routledge Publishing.

Schoenherr, J. R. & Thomson, R. (2021). Beyond the Prisoner's Dilemma: Alternative Models of Cybersecurity. In Frontiers of AI Ethics (DeFalco, J. & Hampton, A, Ed). Routledge Publishing.

Senarath, A., & Arachchilage, N. A. (2018). Why developers cannot embed privacy into software systems? An empirical investigation. In *Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering* (pp. 211-216).

Senarath, A., Grobler, M., & Arachchilage, N. A. (2019). Will they use it or not? Investigating software developers' intention to follow privacy engineering methodologies. *ACM Transactions on Privacy and Security (TOPS)*, 22, 1-30.

Servant-Miklos, V. F., Norman, G. R., & Schmidt, H. G. (2019). Learning, A Short Intellectual History of Problem-Based. In *The Wiley Handbook of Problem-Based Learning* (pp. 3-24).

Thomson, R. (2019). The Cyber Domains: Understanding Expertise for Network Security. In P. Ward, J. Schraagen, J. Gore and E. Roth (Eds). *Oxford Handbook of Expertise*. Oxford Publishing. DOI: 10.1093/oxfordhb/9780198795872.013.31

Walker, A., & Leary, H. (2009). A problem based learning meta analysis: Differences across problem types, implementation types, disciplines, and assessment levels. *Interdisciplinary journal of problem-based learning, 3*, 6.

Wayner, P. (2014, April 12). 12 Ethical Dilemmas Gnawing at Developers Today. *InfoWorld*, pp. Retrived from: https://www.infoworld.com/article/2607452/12-ethical-dilemmas-gnawing-at-developers-today.html.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the process of sensemaking. *Organization Science*, 16, 409-421.

White, G. B., Williams, D., & Harrison, K. (2010). The CyberPatriot national high school cyber defense competition. *IEEE Security and Privacy, 8*, 59-61.

Yilmaz, L., & Sivaraj, S. (2019). A Cognitive Architecture for Verifiable System Ethics via Explainable Autonomy. *In Proceedings of the 2019 IEEE International Systems Conference (SysCon) (pp. 1-8).* IEEE.

Yilmaz, L., Franco-Watkins, A., & Kroecker, T. S. (2017). Computational models of ethical decision-making: A coherence-driven reflective equilibrium model. *Cognitive Systems Research, 46, 61-74*.

Zhang, K., Dong, S., Zhu, G., Corporon, D., McMullan, T., & Barrera, S. (2013). picoCTF 2013 - Toaster Wars: When interactive storytelling game meets the largest computer security competition. In *IEEE International Games Innovation Conference (IGIC 2013)* (pp. 293-299). Vancouver.