BECO: Behavioral Economics of Cyberspace Operations

By Victoria Fineberg

This paper proposes a risk-management framework Behavioral Economics of Cyberspace Operations (BECO) for hardening Cyberspace Operations (CO) with the Behavioral Economics (BE) models of cognitive biases in judgment and decision-making. In applying BE to CO, BECO augments a common assumption of a rational cyber warrior with more realistic expressions of human behavior in cyberspace. While the current development of the cyber workforce emphasizes education and training, BECO addresses typical conditions under which rational decision-making fails and knowledge is neglected. The BECO framework encompasses a full set of cyber actors, including attackers, defenders, and users on the friendly and adversary sides, across the full CO spectrum in space and time, and offers a structured approach to the cognitive bias mitigation.

Bringing BE into CO

This paper proposes enhancements of Cyberspace Operations (CO) by adapting Behavioral Economics (BE) models in a novel framework Behavioral Economics of Cyberspace Operations (BECO). The essence of BECO is the identification of cognitive biases of CO actors, mitigation of biases on the friendly side, and exploitation of biases on the adversary side. BECO is a CO-focused extension of the Behavioral Economics of Cybersecurity (BEC) framework (Fineberg, 2014) that augments the National Institute of Standards and Technology's Risk Management Framework (RMF) of information security (NIST SP 800-39, 2011) by introducing a new class of vulnerabilities corresponding to persistent human biases. BECO takes it further by applying the BEC risk management approach to cyber operations and CO-specific cyberactors. Figure 1 depicts the progression from BE to BEC and BECO and the concepts that link them.

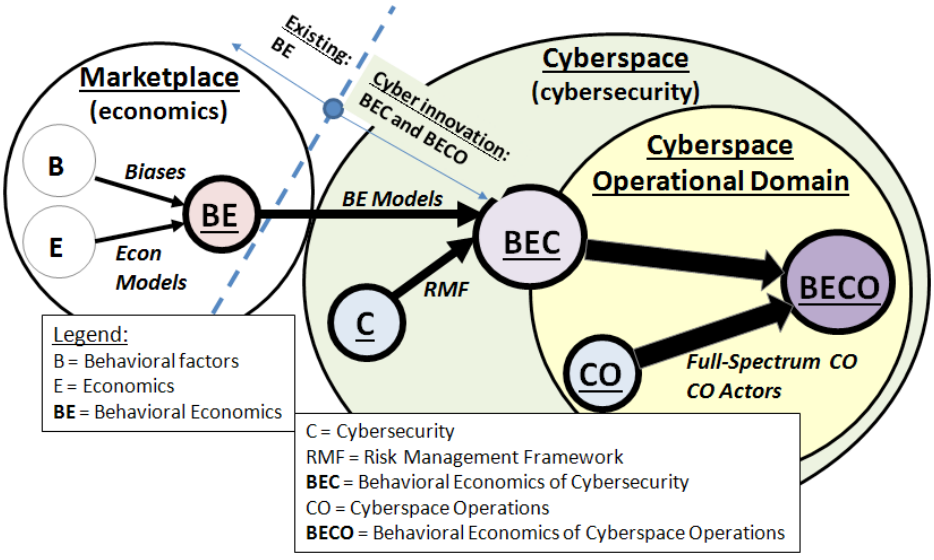

Figure 1. Progression from BE to BEC and BECO.

While the current cognitive analysis of warfighting is rooted in psychology (Grossman and Christensen, 2007), the awareness of the BE discoveries is rising in the military community (Mackay & Tatham, 2011; Holton, 2011). However, in the existing work, the BE relevance is limited to providing general analogies between the BE findings and military scenarios, without offering a practical approach for using BE in the operations. In contrast, BECO provides an overarching framework of behavioral models encompassing the full spectrum of

operational scenarios and cyberactors. The goals of this work are to raise the awareness of persistent human biases of CO actors that cannot be eliminated by traditional training, provide a framework for identifying and mitigating critical biases, and influence policies guiding cyberspace security and operations.

Cyberspace Operations and BECO

The CO concept is evolving, and this paper uses the current tenets of the United States Cyber Command (USCYBERCOM) as the basis for analyzing the CO characteristics addressed in BECO. CO are conducted in cyberspace, which Department of Defense (DoD) has designated as a warfighting domain (Stavridis & Parker, 2012, p. 62) and a part of the Information Environment (IE) that exists in three dimensions: Physical, Informational, and Cognitive. CO is a component of the Information Operations (IO) conducted in IE, as shown in Figure 2.

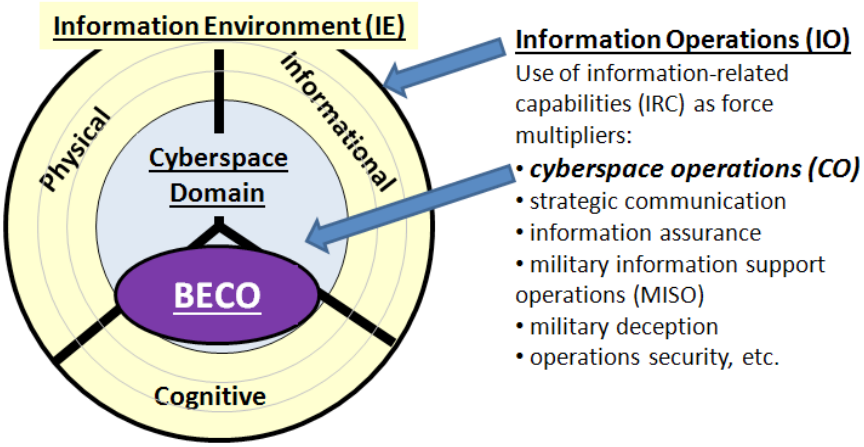

Figure 2. Key concepts related to Cyberspace Operations.

The joint doctrine defines the *Information Environment (IE)* as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information" (JP 3-13, 2012, p. vii); the *Information Operations (IO)* as "the integrated employment, during military operations, of [Information Related Capabilities] IRCs in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own" (p. vii); *Cyberspace* as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (p. II-9); and the *Cyberspace Operations (CO)* as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace" (p. II-9). The IE migration towards the Joint Information Environment (JIE) will facilitate the cyberspace defense, and BECO will enhance JIE's cognitive dimension.

The USCYBERCOM's mission is to conduct the full-spectrum CO in the three focus areas including the defense of the DoD Information Networks (DoDIN), support of combatant commanders, and response to cyber attacks (U.S. Cyber Command, 2013). Correspondingly, USCYBERCOM operates across three Lines Of Operation (LOO) including DoD Network Operations (DNO), Defensive Cyber Operations (DCO), and Offensive Cyber Operations (OCO) (Pellerin, 2013a). DNO provides a static defense of the DoDIN perimeter. DCO includes maneuvers within the perimeter to stop attacks that have passed the static DNO defenses, actions outside the perimeter to stop impending attacks, and employment of Red Teams. OCO is "the ability to deliver a variety of effects outside our own network to satisfy national security requirements" (Pellerin, 2013a). Figure 3 below provides a graphical representation[1] of these COs.

BECO uses the full-spectrum nature of USCYBERCOM to define a comprehensive set of cognitive CO scenarios, as discussed below.

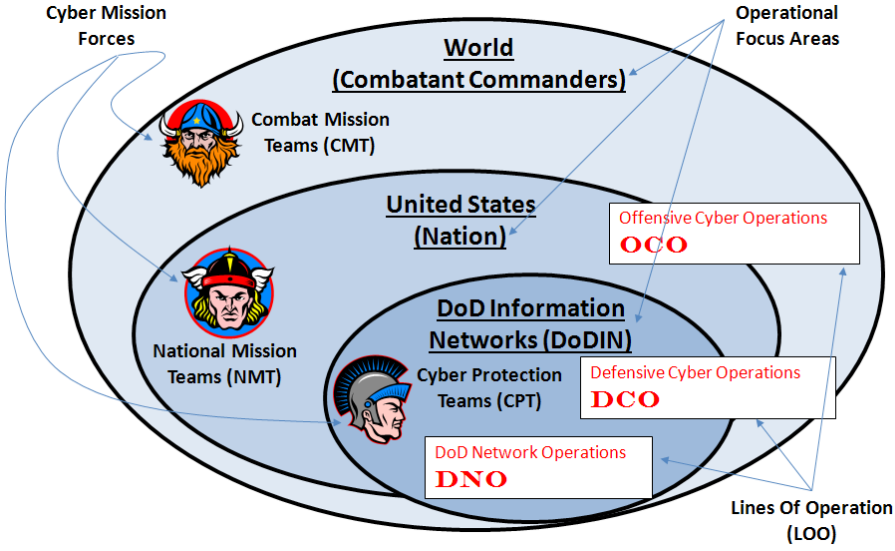

Figure 3. Graphical representation of the CYBERCOM COs.

1 This figure is developed for this paper as a graphical representation of the CYBERCOM COs using publically available information. The figure is not developed or endorsed by the CYBERCOM and is used for illustration only.

Behavioral Economics

This section provides some BE background with the emphasis on the BECO relevance.

BE Background

Behavioral Economics (BE) is a recent science that emerged at the confluence of psychology and economics to correct Standard Economics (SE) models for cognitive biases demonstrated in psychological experiments. SE relies on the *rational-agent* model of the preference-maximizing human behavior. In contrast, BE is based on the statistically significant evidence of systematic deviations of the economic actors' behavior from the rationality assumed in SE. Economists use the terms 'rationality' and 'biases' in a specific context. Kahneman, a 2002 winner of the Nobel Memorial Prize in Economic Sciences, explains that *rationality* is logical coherence, which could be reasonable or not (2011). The rational-agent model assumes that people use information optimally and that the cost of thinking is constant. However, empirical evidence shows that even high-stake strategic decisions are biased (Kahneman, 2013). A *bias* is a systematic error, an average system error that is different from zero (Kahneman, 2006). BE studies biases that represent psychological mechanisms skewing people's decisions in specific directions, beyond the considerations of rationality and prudence.

Psychology: Fast and Slow Thinking

The differences between biased and rational decision making can be traced to the distinction between two types of thinking that Kahneman (2011) calls System 1 (S1) and System 2 (S2), respectively. S1 refers to the fast, automatic, intuitive thinking; and S2 refers to the slow, deliberate, effortful thinking. The S1 thinking includes *automatic* activities of memory and perception; and *intuitive* thoughts of two types, the expert and the heuristic. The *expert* thought is fast due to prolonged practice, and the *heuristic* thought is exemplified by one's ability to complete the phrase 'bread and …' and answer 2 + 2 = ? In contrast with S1, S2 performs effortful mental activities that require concentration. Examples of S2 activities include parking a car in a narrow space, filling out tax forms, and complex computations. Figure 4 summarizes the key features of S1 and S2 with the emphasis on the S1-based heuristics that are the main cause of cognitive biases in judgment and decision making.

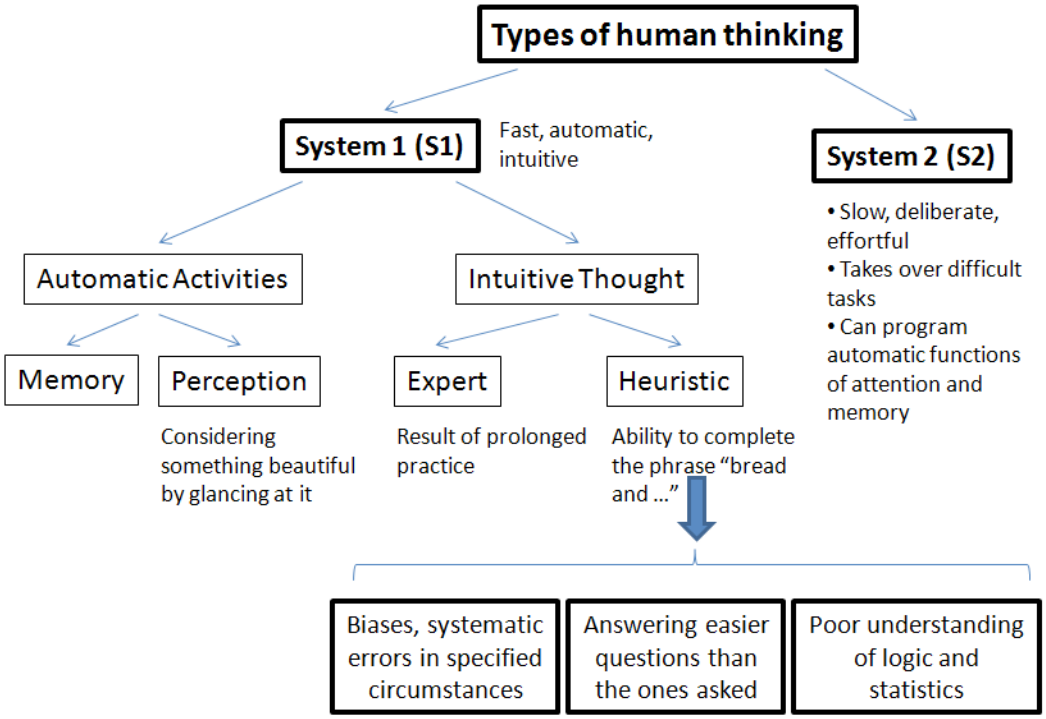

Figure 4. Types of human thinking.

Interactions between S1 and S2 are complex and generally favor decisions made by S1, even though S2 has some limited capacity to program normally-automatic functions of attention and memory. S1 produces biases, which are systematic errors it makes in specific circumstances, such as answering easier questions than those asked and misunderstanding logic and statistics.

S2 is used to focus on a task, but the intense focus blinds people to other stimuli and cannot be sustained for prolonged periods of time. Most thinking originates in S1, but S2 takes over when decisions are difficult and has the last word. While it may be desirable to switch from S1 to S2 in order to avoid making biased choices, Kahneman notes that "because System 1 operates automatically and cannot be turned off at will, errors of intuitive thought are often difficult to prevent. Biases cannot always be avoided, because System 2 may have no clue to the error. Even when cues to likely errors are available, errors can be prevented only by the enhanced monitoring and effortful activity of System 2. As a way to live your life, however, continuous vigilance is not necessarily good, and it is certainly impractical" (2011, p. 28). Furthermore, "effort is required to maintain simultaneously in memory several ideas that require separate action" (p. 36) and "switching from one task to another is effortful, especially under time pressure" (p. 37).

The fast and slow thinking patterns of S1 and S2 apply to all areas of decision making including economics (BE), cybersecurity (BEC), and cyber operations (**BECO**). When cyberactors focus on absorbing tasks, they are oblivious to other important signals and commit biases that override their experience and training.

Incorporation of Biases in Economics, Cybersecurity, and CO

The integration of psychological findings of behavior and judgment into economics, i.e., the progression from SE to BE, required revisions of mainstream economic methods. According to Rabin, the difference between psychology and economics is that "while psychology investigates humans in all their richness, economics requires models that are not so rich as to retard the process of drawing out their economic implications" (1996, p. 2). Psychologists provide the breadth of information about the human psyche, and economists then use the filters of simplicity and tractability to select the psychological findings that enable them to build meaningful economic models.

Economic methods include methodological individualism, mathematical formalization of assumptions, logical analysis of the relationship between conclusions and assumptions, and empirical field testing. In SE, *methodological individualism* consists of two basic components: actors have well-defined preferences and they rationally maximize these preferences. BE revises these components by applying empirical evidence from psychology to the economic assumption-making to modify the nature of the preferences (Rabin, 1996, Section 2), demonstrate systematic errors that individuals commit when maximizing their utility functions (Rabin, 1996, Section 3), and describe scenarios where the very concept of people maximizing their preferences does not hold (Rabin, 1996, Section 4). Some cognition-based modifications are relatively easy to incorporate into economic models; other psychological findings raise awareness of the model shortcomings and improve economics on an *ad hoc* basis. Psychologists and experimental economists conduct controlled laboratory experiments to generate hypotheses, and economists test these hypotheses in uncontrolled field studies. Likewise, BECO is a hypothesis for integrating BE models into the CO Concepts of Operations (CONOPS) to be tested in field studies, as illustrated in Figure 5.

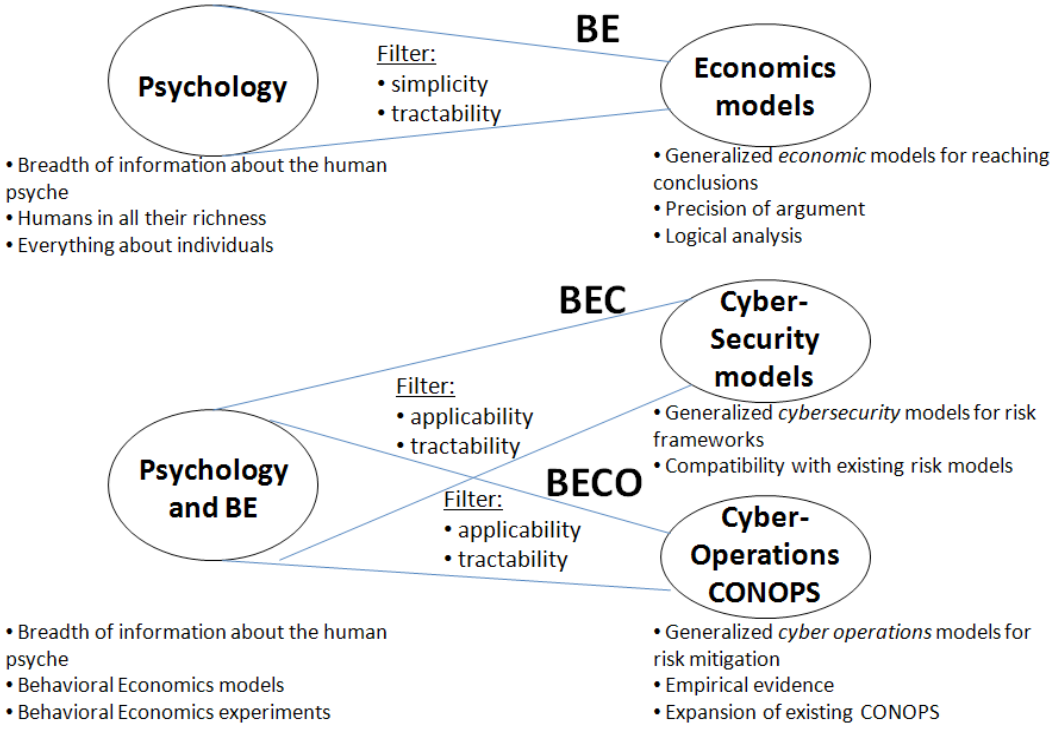

Figure 5. Relationships Between Psychology, BE, BEC, and BECO.

BECO will identify psychology and BE findings that could provide meaningful CONOPS enhancements. As with BE, some of these findings will be incorporated into CONOPS directly, while others will be used to raise awareness and improve the operations on an *ad hoc* basis.

BECO Solution and Innovation

BECO is a proposed framework for increasing the effectiveness of Cyberspace Operations, such as those of USCYBERCOM, by defining a risk management framework of the CO cognitive dimension. BECO identifies biases in the operational judgment and decision-making and seeks their mitigation on the friendly side and their exploitation on the adversary side. In this context, "the friendly side" refers to the United States and its allies, and "the adversary side" refers to states and non-state entities opposing the U.S. in cyberspace.

BECO Description

BEC model. BECO is an application of BEC to CO, where BEC is a framework for conducting BE-based cybersecurity risk management (Fineberg, 2014). BEC is defined in three *dimensions* of Cyberactors, Security Services, and Controls as depicted in Figure 6.

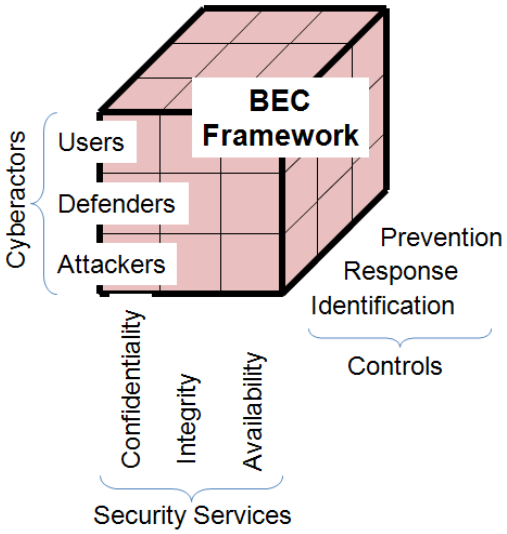

Figure 6. BEC framework.

Cyberactors are classes of individuals defined by their distinct cyber roles of Users, Defenders, and Attackers. Users are seeking functional capabilities of cyberspace, *Defenders* are protecting cyberspace, and *Attackers* are exploiting cyberspace. *Security Services* are classes of features that ensure proper cyberspace operation and include Confidentiality, Integrity, and Availability. *Confidentiality* is protection of the user information, *Integrity* is protection of cyber systems and data from unauthorized access and malicious manipulation, and *Availability* is the user's ability to use cyberspace systems and data. *Controls* are risk-management responses for upholding cybersecurity including Identification, Response, and Prevention. *Identification* uncovers significant cognitive biases that apply to various scenarios, *Response* mitigates biases on the friendly side and exploits biases on the adversary side, and *Prevention* encompasses research, training and other preparation.

The BEC cube can be used for comprehensive Risk Management and for selecting and controlling the greatest risks. In the Risk Assessment phase, cognitive vulnerabilities are represented by one or more squares on the Cyberactor-Security Services surface; and in the Risk Response phase, mitigation is selected along the Controls axis.

BECO model. BECO applies BEC to CO exemplified by the USCYBERCOM's mission. The principal distinctions between the two frameworks are their respective scopes and sets of actors. The scope of BEC is the general cybersecurity risk management, whereas the scope of BECO is risk management of the full-spectrum CO, as depicted in Figure 7. The BEC RMF is applied to each BECO actor, thus creating a five-dimensional analysis space of Cyberactors, Security Services, Controls, Planning Levels, and Lines of Operation.

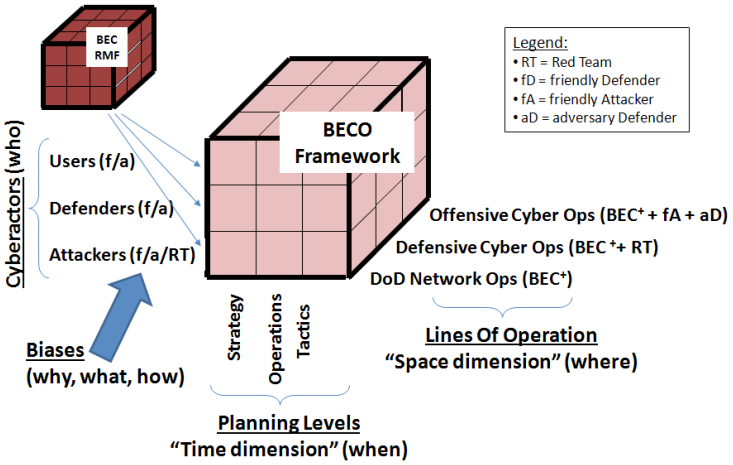

Figure 7. BECO framework.

A comprehensive scope of BECO is assured by its incorporation of a comprehensive set of questions "who, why, what, how, when, and where." "Who" are CO cyberactors, and "why, what, and how" represent actors' biases and actions. "When" is the time dimension, the timeframe of the strategic, operational, and tactical levels of the CO planning. "Where" is the space dimension, such as the USCYBECOM's Lines Of Operation (LOO) including DoD Network Operations (DNO), Defensive Cyber Operations (DCO), and Offensive Cyber Operations (OCO). DNO provides typical enterprise security within the

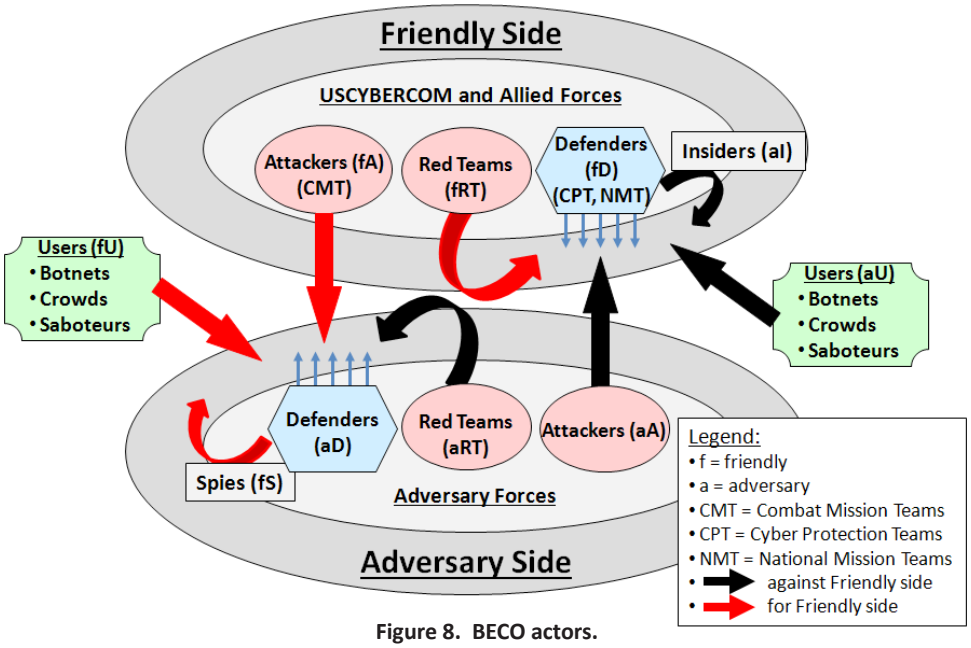

Figure 8. BECO actors.

defense perimeter, and its risk management corresponds to the original BEC. DCO extends DNO with the maneuver capability outside the perimeter and employs Red Teams. OCO engages in global military actions, in which USCYBERCOM's attackers are on the friendly side. In CO, the scope of actors expands beyond BEC's Users, Defenders, and Attackers by the considerations of the friendly and adversary sides as depicted in Figure 8, where the friendly-side USCYBECOM forces are described by Pellerin (2013b).

The *friendly* side includes Defenders (fD) such as USCYBERCOM's Cyber Protection Teams (CPT) and National Mission Teams (NMT), Attackers (fA) such as Combat Mission Teams (CMT), and Red Teams (fRT) testing the friendly defenses. On the *adversary* side, Attackers (aA) are regular BEC attackers and Defenders (aD) are BECO entities whose cognitive biases are exploited by fAs. Insiders (aI) are adversarial actors sabotaging the friendly side from inside the friendly defense perimeter; similarly, Spies (fS) are supporting the friendly side from inside the adversary defense perimeter. BECO Users include both adversary Users (aU) and friendly Users (fU) that may undermine the friendly and the adversary sides, respectively.

Examples of BECO Biases

Insider Biases and Mitigation

The BECO Black Swans are insiders (aI) that disclose information of vital importance or enable adversaries to penetrate the friendly defenses. Insiders may operate in various building blocks of the BECO framework and are particularly dangerous in *Strategy* and *Operations*. Like with all Black Swans (Taleb, 2010), their actions and motivations are analyzed *a posteriori*, and CO proceeds to fight the last war. The most dangerous insiders are turn-coat defenders. Their downfall is gradual, from minor infractions to full-blown national security violations. This pattern resembles *coherent arbitrariness* (Ariely, Loewenstein, & Prelec, 2000), a human propensity for mentally anchoring on arbitrarily selected initial conditions ("arbitrariness") and then making judgments systematically related to the initial selection ("coherence").

In Ariely's experiments, students were either paid or received payment for listening to his poetry recital, depending on whether a session was offered as an entertainment or a chore (2009). The students' initial decision to pay for Ariely's poetry was as arbitrary as that of Tom Sawyer's friends agreeing to pay for whitewashing his aunt's fence, but after that decision had been made, the amounts paid were coherently proportional to the duration of the experience. To fight the formation of undesirable patterns, Ariely urges decision makers to question their repeated behaviors and pay particular attention to the initial decisions in what is going to become a long stream of decisions. Likewise, in **BECO** it is important to identify and prevent decisions that may turn defenders into insiders and break harmful patterns as soon as they form.

Insider actions may also be forestalled by using a powerful psychological mechanism of *cognitive dissonance* described by Leon Festinger (1962) as "that if a person knows various things that are not psychologically consistent with one another, he will, in a variety of ways, try to make them more consistent" (p. 93). Ariely provides an example of how "doctors reason that if they are telling others about a drug, it must be good—and so their own beliefs change to correspond to their speech, and they start prescribing accordingly" (2012, p. 81). Furthermore, actions create preferences, because "decisions can be highly sensitive to situational factors, even when such factors are unrelated to the actual utility of that course of action" and individuals "rely not only on stable hedonic utilities but also on their memories of utility for their own past behaviors" (Ariely & Norton, 2008, p. 13). In **BECO**, cognitive dissonance can be used to enhance the loyalty of the cyber workforce by asking defenders to perform patriotic duties beyond their normal responsibilities and thereby develop a positive mindset. Negative attitudes of defenders must be curtailed before they deepen and lead to adversarial insider actions.

Hawkish Biases

Hawkish biases influence military strategy towards aggressive "hawkish" attitudes and downplay conciliatory, or "dovish," attitudes beyond common considerations of prudence. They affect attackers on the friendly and adversary sides in the BECO *strategy* block. Mitigation of these biases requires actions by attackers, defenders and Red Teams as discussed in this section. The name "hawkish biases" was introduced by Kahneman and Renshon (2009) who reviewed an extensive list of cognitive biases in the context of military and diplomatic actions and found that all of them were strongly directional towards aggression. The set of *positive illusions* includes "unrealistically positive views of one's abilities and character, the illusion of control, and unrealistic optimism" (p. 4). *Unrealistically positive views* lead people to consider themselves better decision makers and negotiators than they are. People experience the *illusion of control* when they exaggerate the impact of their actions on the outcomes, and under stress, they prefer strategies that they think would give them more control. *Unrealistic optimism* causes people to overestimate the odds of positive for them events, have more confidence in their predictions than the circumstances warrant, and discount the abilities and skills of their peer group. Political science studies and simulated conflicts have demonstrated that the positive-illusion biases cause leaders to have unrealistically positive views of the balance of military power, and many wars start because leaders on each side believe that they will win. Furthermore, during a conflict, negotiations stall because each

side thinks that it has a stronger hand and, therefore, it is less likely to make concessions. Positive illusions take place in **BECO** when each side overstates its attack capabilities against the other side's defenses. The attackers' illusion of control may be exploited by the opponent setting up deception systems.

The *Fundamental Attribution Error (FAE)* is a bias of explaining behaviors of others by exaggerating their intentions and discounting their circumstances. This bias persists even when people are aware of it. In conflicts, "beliefs in the hostile intentions of adversaries tend to be self-perpetuating—and … self-fulfilling" (p. 8), whereas the true reasons for hostile actions could be in response to the opponent's domestic politics or to one's own aggression. With the FAE, the hawkish behavior is prompted by attributing the opponent's moderate behavior to their situation and their hostile behavior to their disposition. The FAE affects **BECO** when each side assumes that the other side is preparing cyber attacks. Moreover, in cyberspace, the FAE may be exaggerated even further, because many exploits are invisible until they are launched. The players must be aware of the FAE and try to distinguish genuine attacks from random events before responding in kind. Considering the difficulty of attribution in cyberspace and the need for an almost instantaneous response, defenders must have effective diagnostic capabilities. When there is a possibility that an adversary may misperceive an attack, direct communications between decision makers are particularly important.

Loss aversion is a manifestation of people's greater sensitivity to losses than gains. Related biases are the *endowment effect* of overvaluing the items people already own in comparison to identical items that do not belong to them, and the *status-quo bias* of the preference for the existing situation even if a change would be more beneficial. Loss aversion negatively affects negotiations, because each side considers its concessions as greater losses than they are gains for the other side. In **BECO**, the endowment effect causes cyberactors to overestimate the merit of their strategies, processes, and technologies. Recommendations for significant changes must not only be justified logically but also address commanders' biases, and analyses of alternatives must be conducted by independent parties. *Confirmation bias* causes commanders to overvalue evidence supporting their beliefs that some types of cyber attacks are more likely, some adversaries are more dangerous, and some defenses are more effective. The BECO countermeasures should include independent reviews and stress tests by Red Teams.

Risk seeking in losses causes people facing a sure loss to take greater risks. In conflicts, the side anticipating a significant loss is prone to engage in a disastrous campaign that has a small chance of winning; instead of ignoring *sunk costs*, leaders escalate commitment . An *agency problem* compounds these effects, because leaders ("agents") are punished for losses and rewarded for gains even in situations where their constituency ("principals") would have preferred a loss to a foolish risk. In **BECO**, the players that consider themselves more vulnerable, e.g., non-state entities, may be attacking more aggressively to avoid a certain loss. Considering that in cyberspace the actual capabilities are concealed and perceptions are more potent than in physical realms, irrationally-motivated attacks are more likely. The agency problem is also evident in the botnet phenomena where the owners of infected computers ("adversary users," or aU) are "agents" who don't really suffer from the Distributed Denial of Service (DDoS) attacks that they precipitate.

Pseudo-certainty is a bias in multi-stage decision-making of choosing the certain outcome of the last stage while disregarding the probability of reaching that last stage. This situation frequently arises in international politics where decision makers focus on the certainties of the final stage and disregard the contingency of the final stage on preceding stages, which may strongly depend on the decision makers' choices. Thus, "actors under-emphasize the effect of their own actions" (p. 19). In **BECO**, this means that an actor may focus on its strength in a full-blown cyber conflict and disregard the statistical uncertainties of the preliminary actions leading to it. Field experiments may indicate that in BECO individual hawkish biases might benefit from a consolidated approach if any of them reinforce or diminish the influence of others.

BECO Mitigation

Biased decisions are frequently made when individuals are in a "hot" state, i.e., their reflexive thinking dominates their logical thinking (Ariely, 2009, pp. 120-121). This paper proposes a structured mitigation approach for preparing friendly-side cyberactors for potential hot states as depicted in Figure 9.

The mitigation framework covers a range of approaches starting with the hot state avoidance (1), proceeding to switching to a cold state in different parts of the process (2 and 3), and then moving to various approaches to the preparation to and management of the hot state itself (4 through 8). This framework formalizes recommendations found in discrete sources as follows:

1. Avoid some hot states all together (Ariely, 2009, pp. 130-131), because upon entering these states resistance to temptation becomes extremely difficult. A **BECO** example of such hot-state avoidance is blocking access to the Internet pornography sites.

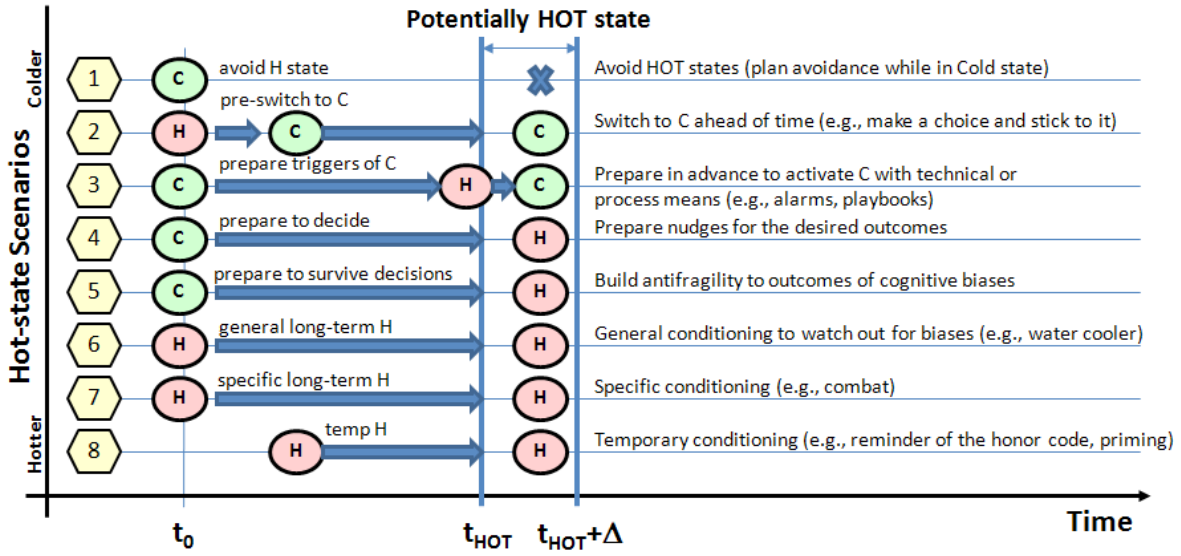

Figure 9. A structured approach to mitigating cognitive biases.

2. When a choice is difficult to make, because all options have approximately the same utility even as the details vary, choose one option and stick to it instead of prolonging the analysis and getting paralyzed by choice (Ariely, 2009, pp. 194-196). In **BECO**, this corresponds to choosing certain critical operational responses in advance.

3. Powerful technical and process controls must be defined to activate cyberactors' cold state at the point where they are likely to make critical mistakes, thus satisfying Kahneman's wish to have "a warning bell that rings loudly whenever we are about to make a serious error" (2011, p. 417). An existing example of such a control is an operating system that asks users to confirm that they want to delete a file. In **BECO**, Tactics, Techniques, and Procedures (TTPs) must be defined for anticipated critical decision points, forcing cyber warriors to invoke their System 2 thinking.

4. Nudges (Thaler & Sunstein, 2009) and defaults are used to suggest a preferred option without forcing it. In **BECO**, this approach is more applicable to cyber users who are free to choose than to warfighters who can be compelled to act in certain ways by their organizations.

5. Taleb (2010) urges to consider Black-Swan events not as exceptions that are explained *a posteriori*, but as a class of low-probability high-impact events that cannot be *individually* predicted. The best preparation for potential Black Swans is to cultivate antifragility (Taleb, 2012) that would protect an entity from a broad range of calamities. A current example of such preparation is Continuity Of Operations Planning (COOP), which Fineberg recommends enhancing with random stress testing (2012). Stress testing for developing antifragility should also be incorporated into a variety of **BECO** scenarios, e.g., cyber flag exercises (Alexander, 2012, p. 14).

6. Behavioral economists warn that the knowledge of cognitive biases does not prevent people from committing these biases. Kahneman admits that his intuitive thinking is just as prone to overconfidence and other System 1 manifestations as it was before he started studying these issues. However, he has improved his ability to *recognize situations* in which errors are likely, and once he recognizes them, to slow down and invoke System 2 (2011, p. 417). It is also easier to recognize errors of others than one's own, because "observers are less cognitively busy and more open to information than actions." Kahneman recommends having water-cooler discussions to take advantage of the group influences. **BECO** training should include developing the recognition of error-prone situations, and BECO CONOPS should include activities that activate group influences.

7. Conditioning for specific situations prepares people for taking the correct action when the situation arises, as for example, practiced by psychiatrists in the behavioral therapy of Exposure Response Prevention (ERP) for treating conditions such as panic. ERP practitioners select appropriate frequency, duration, rate of build-up, and escape prevention to achieve high levels of effectiveness. Likewise, certain combat situations require a single instantaneous decisive action. For physical combat, Grossman and Christensen recommend operand conditioning, i.e., realistic training until a warrior performs required actions automatically without thinking, because "whatever you rehearse is what you do under stress" (2007, p. 47). For example, practice shooting at moving targets shaped as human silhouettes has increased the front-line firing rate from 15 to 20 percent

in World War II to 90 percent during the Vietnam War. The **BECO** counterpart of such a conditioning is General Alexander's request for a single standard for taking action (2012, p. 14).

8. People can be prepared for decision making in a process called "priming," which is widely used in cognitive psychology experiments to affect the choices people make in a hot state. For example, Ariely (2009, p. 283) shows how reciting of the Ten Commandments prior to exams has resulted in significantly reduced student cheating. Likewise, in **BECO** cyber warfighters can be primed with the reminders of their honor code.

While cognitive biases have been extensively identified and thoroughly studied, their mitigation is challenging. A critical issue is that mitigation may work in laboratory experiments but not in real-life scenarios. Another problem is that any given mitigation may work in a short term but wear off with repetition. Nevertheless, the principal reason for identifying cognitive biases in BECO is the potential ability to develop effective responses. To facilitate research of mitigation, a full-scope cyber force such as USCYBERCOM can use its defense forces to test its attackers and use its attack forces to test its defenders as depicted in Figure 10.

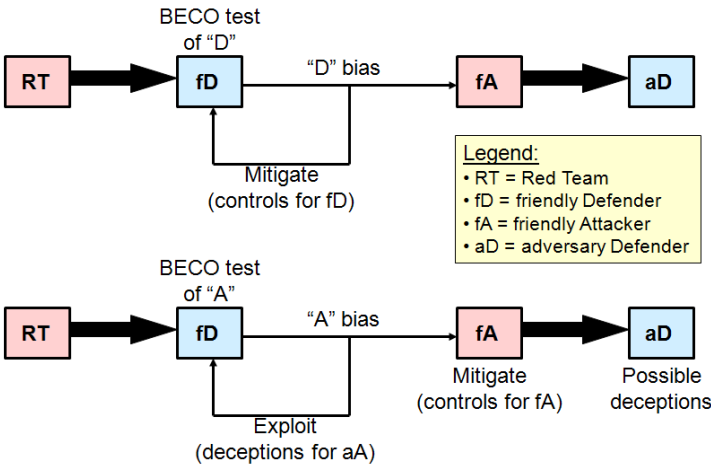

Figure 10. Bias testing architectures.

The top part of Figure 10 illustrates how Red Team (RT) probing of vulnerabilities of the friendly-side defenders can be used to strengthen friendly defenders (fD) and weaken adversary defenders (aD). For example, RTs may discover that defenders get accustomed to false alarms and start neglecting them. To mitigate this tendency with fDs, new TTPs will be implemented to vary the strength and appearance of the alarms using psychological techniques of irregular reinforcement. To exploit this tendency with aDs, friendly attackers (fA) will stage multiple false attacks before launching the actual attack.

The bottom part of Figure 10 illustrates how cognitive biases revealed by RTs can be used to strengthen friendly attackers (fA) and weaken adversary attackers (aA). For example, an attacker may be affected the paradox of choice, i.e., getting paralyzed with indecision when confronted with too many choices (Iyengar & Lepper, 2000). To exploit it, fDs can present to aAs many enticing choices. To mitigate it, fAs can be requested to follow strict decision making processes for selecting their targets and abandoning exploits upon reaching certain thresholds, thus eliminating the perils of choice.

These mitigating approaches and their details must be thoroughly researched and carefully implemented to provide the friendly side with tangible advantages in the cyber warfare. An important part of this research is the role of leaders and groups, who serve as psychological weapons (Grossman & Christensen, 2007, pp. 205-208) and, as most other organizations, "naturally think more slowly … and impose orderly procedures" (Kahneman, 2011, p. 418), thus mitigating the quirks of the individual human cognition.

Conclusions

This paper proposes a novel framework BECO of using the behavioral economics (BE) models of cognitive biases in judgment and decision making for hardening cyberspace operations (CO). BE adapts psychology research to economic models, thus creating more accurate representations of human interactions. BEC (Fineberg, 2014) uses BE discoveries to modify the risk management framework of cybersecurity by introducing a new class of vulnerabilities corresponding to persistent human biases. And now BECO applies the BEC framework to cyberspace operations by providing an overarching approach to the cognitive characteristics of the full spectrum of the CO actors and scenarios. Cyberspace operations are exemplified by the USCYBERCOM's mission, and cyberactors include attackers, defenders, and users on both the friendly and adversary sides. The paper reviews selected BE biases applicable to CO and offers a structured approach to the cognitive bias mitigation.

BECO provides an asymmetric advantage to cyber superpowers that have resources to research cognitive biases in their operations and implement effective controls. While non-state actors may obtain technologies developed by major states, they cannot replicate a unique operational environment of a cyber power. Furthermore, full scope forces, such as USCYBERCOM, can use their attack and defense capabilities to cross-test and strengthen the cognitive aspects of both. BECO goals are to define interdisciplinary research of cognition in cyberoperations, develop cyberoperations policies and strategies, and train cyber workforce.

About the Author

Victoria Fineberg is a Principal Information Assurance Engineer at the Defense Information Systems Agency (DISA). Victoria holds a Master of Science Degree in Mechanical Engineering (MSME) from the University of Illinois at Urbana-Champaign and a Master of Science Degree in Government Information Leadership with specialization in Cybersecurity (MS GIL-Cybersecurity) from the National Defense University's (NDU) iCollege. She is a licensed Professional Engineer and a Certified Information Systems Security Professional (CISSP). Prior to DISA Victoria worked at Bell Labs, Lucent Technologies. Her professional interests include cybersecurity, risk analysis, and the impact of cognitive biases on cyber operations.

References

Alexander, K. B. (2012). Statement before the Senate Committee on Armed Services. Retrieved from http://www.airforcemag.com/SiteCollectionDocuments/Reports/2012/March2012/Day28/032812alexander.pdf.

Ariely, D. (2009). *Predictably irrational: The hidden forces that shape our decisions*. Revised and expanded edition. New York, NY: Harper Perennial.

Ariely, D. (2012). *The (honest) truth about dishonesty: How we lie to everyone—Especially ourselves*. New York, NY: HarperCollins Publishers.

Ariely, D., Loewenstein, G., & Prelec, D. (2000). Coherent arbitrariness: Duration-sensitive pricing of hedonic stimuli around an arbitrary anchor. SSRN. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=243109.

Ariely, D. & Norton, M. I. (2008). How actions create – not just reveal – preferences. *Trends in Cognitive Sciences*, 12 (1), 13-16.

Festinger, L. (1962). Cognitive dissonance. *Scientific American*, 207(4), 93-107.

Fineberg, V. (2012). COOP hardening against Black Swans. *The Business Continuity and Resiliency Journal*, 1(3), 14-24.

Fineberg, V. (2014). BEC: Applying behavioral economics to harden cyberspace. *Journal of Cybersecurity and Information Systems*, 2(1), 27-33. Retrieved from https://www.csiac.org/journal_article/bec-applying-behavioral-economics-harden-cyberspace#.U6nby7H5eZk.

Grossman, D. & Christensen, L. W. (2007). *On combat: The psychology and physiology of deadly conflict in war and in peace*. 2nd Edition. PPCT Research Publications.

Holton, J. W. (2011). *The Pashtun behavior economy: An analysis of decision making in tribal society*. Master's Thesis. Naval Postgraduate School. Monterey, CA. Retrieved from http://edocs.nps.edu/npspubs/scholarly/theses/2011/June/11Jun_Holton.pdf.

Iyengar, S. S. & Lepper, M. R. (2000). When choice is demotivating: Can one desire too much of a good thing? *Journal of Personality and Social Psychology*, 79(6), 995-1006. Retrieved from http://www.columbia.edu/~ss957/articles/Choice_is_Demotivating.pdf.

JP 3-13. (2012). *Information operations*. Joint Publication 3-13. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

Kahneman, D. (2006). [Video File]. History and rationality lecture series. Hebrew University. Retrieved from http://www.youtube.com/watch?v=3CWm3i74mHI.

Kahneman, D. (2011). *Thinking, fast and slow*. New York, NY: Farrar, Straus and Giroux.

Kahneman, D. (2013). [Video File]. Annual Hans Maeder lecture with Nobel Prize-winning psychologist Daniel Kahneman. The New School. Retrieved from http://www.youtube.com/watch?v=l91ahHR5-i0&list=PLUWrLGgGJAm9pm4ANtiGk4VVflf45Hz0P&index=7.

Kahneman, D. & Renshon, J. (2009). Hawkish biases. Expanded version of an essay that appeared in *American Foreign Policy and the Politics of Fear: Threat Inflation Since 9/11*. New York, NY: Routledge Press, 79-96. Retrieved from http://www.princeton.edu/~kahneman/docs/Publications/Hawkish%20Biases.pdf

Mackay, A. & Tatham S. (2011). *Behavioural conflict: Why understanding people and their motives will prove decisive in future conflict*. Saffron Walden, Essex, UK: Military Studies Press.

NIST 800-39. (2011). Managing information security risk: Organization, mission, and information system view. *NIST Special Publication* 800-39. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

Pellerin, C. (2013a). Cyber Command adapts to understand cyber battlespace. U.S. Department of Defense. Retrieved from http://www.defense.gov/news/newsarticle.aspx?id=119470.

Pellerin, C. (2013b). DOD readies elements crucial to Cyber Operations. U.S. Department of Defense. Retrieved from http://www.defense.gov/news/newsarticle.aspx?id=120381.

Rabin, M. (1996). Psychology and Economics. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.42.9558&rep=rep1&type=pdf.

Stavridis, J. G. & Parker, E. C. III. (2012). Sailing the cyber sea. JFQ, 65(2), 61-67.

Taleb, N. N. (2010). *The Black Swan: The impact of the highly improbable*. New York, NY: Random House.

Taleb, N. N. (2012). *Antifragile: Things that gain from disorder*. New York, NY: Random House.

Thaler, R. H. & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth, and happiness*. London, England: Penguin Books.

U.S. Cyber Command. (2013). United States Strategic Command factsheet: U.S. Cyber Command. Retrieved from http://www.stratcom.mil/factsheets/Cyber_Command/.