SMALL WARS JOURNAL

October 21, 2017

# OODA Loops in Cyberspace

## A New Cyber-Defense Model

Robert Zager and John Zager

Colonel John Boyd's Observe/Orient/Decide/Act Loop ("OODA loop") is a widely adopted decision-making analytical framework.

We combine the OODA loop with the NSA Methodology for Adversary Obstruction to create a new cyber-defense model.

**OODA Loop – Overview**

---

*As an individual or group goes through the OODA cycle, they iteratively improve and are able to make decisions faster. Meanwhile, opponents reacting to those decisions find their OODA loops getting larger or slower.*

- David Shipley, CEO Beauceron Security[1]

---

Colonel John Boyd, USAF, Deceased, developed the Observe/Orient/Decide/Act Loop ("OODA loop") in an effort to explain adversarial engagements. With the exception of *Aerial Attack Study*, (1964) his earliest work, Boyd did not commit his works to formal papers or books; instead he communicated his ideas in essays and illustrated oral briefings.[2]

The OODA loop, which Boyd introduced in *Patterns of Conflict* (1986), resulted from his years of research and analysis in his effort to describe the nature of adversarial engagements. In *Patterns of Conflict*, Boyd did not provide an illustration of the OODA loop; instead he observed,[3]

> …in order to win, we should operate at a faster tempo or rhythm than our adversaries – or, better yet, get inside the adversary's Observation-Orientation-Decision-Action time cycle or loop. [emphasis in the original]

Although Boyd did not provide an illustration of the OODA Loop in *Patterns of Conflict*, the OODA loop is commonly drawn as illustrated in Figure 1. Osinga observes:[4]

In the popularized interpretation, the OODA loop suggests that success in war depends on the ability to out-pace and out-think the opponent, or put differently, on the ability to go through the OODA cycle more rapidly than the opponent. Boyd's name will probably always remain associated with the OODA loop and this popular interpretation.

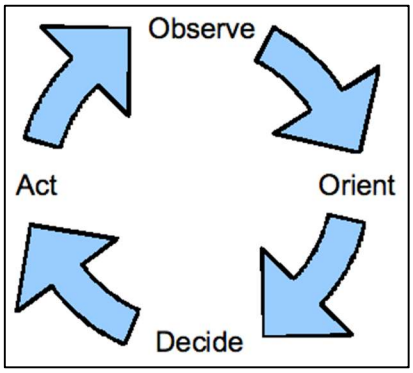

*Figure 1 Popularized OODA loop*

The OODA loop is a subject of significant discussion in the cybersecurity community. For example, Cisco summarizes the importance of the OODA loop to cybersecurity:[5]

> The OODA Loop assumes that continuous improvement is an integrated part of the process, allowing you to learn from your previous experiences, feeding lessons learned into the loop activities to achieve better performance every time you complete the four steps.

This version of OODA loop focuses on an introspective process in which faster completion of the cycle is the key to victory. Thus, commentators have developed enhanced decision making models to elaborate upon the OODA loop and suggest places for speeding the decision-making process while improving the quality of the information syntheses.[6] CERT summarizes this introspective view of the OODA loop:[7]

> The OODA Loop, in the military context, describes the ability to acquire, process and act upon information in comparison to one's adversary's ability to do so. The common phrase, "getting inside their decision cycle," is a reference to being able to cycle through this loop faster than your adversary.

During the development of the OODA loop, Boyd studied the continuous interplay of adversaries in aerial combat maneuvers and tactics. He observed how the actions of each combatant influenced the actions of the other. As we discuss below, Boyd's OODA loop is not about the advantage gained by making decisions faster. In Boyd's analysis, an optimal decision exists in the context of the opponent's decision.

**OODA Loop – A Tool of Cognitive Engagement**

---

*In EW we f*** with their minds.*

- Anonymous Naval Aviator, Electronic Warfare Squadron.[8]

---

In *Destruction and Creation* (1976) Boyd describes the continuing cycle of conceptualization and observation:[9]

> Back and forth, over and over again, we use observations to sharpen a concept and a concept to sharpen observations. Under these circumstances, a concept must be incomplete since we depend upon an ever-changing array of observations to shape or formulate it. Likewise, our observations of reality must be incomplete since we depend upon a changing concept to shape or formulate the nature of new inquiries and observations. Therefore, when we probe back and forth with more precision and subtlety, we must admit that we can have differences between observation and concept description; hence, we cannot determine the consistency of the system—in terms of its concept, and match-up with observed reality—within itself.
>
> Furthermore, the consistency cannot be determined even when the precision and subtlety of observed phenomena approaches the precision and subtlety of the observer—who is employing the ideas and interactions that play together in the conceptual pattern.

Boyd's analysis of the interplay of mental models and reality anticipates Smith and Hancock's groundbreaking psychological research *Situational Awareness is Adaptive, Externally Directed Consciousness* by almost twenty years.[10]

Boyd concludes *Conceptual Spiral* (1992),[11]

> Since survival and growth are directly connected with the uncertain, ever-changing, unpredictable world of winning and losing, we will exploit this whirling (conceptual) spiral of orientation, mismatches, analyses/ synthesis, reorientation, mismatches, analyses/synthesis … so that we can comprehend, cope with, and shape—as well as be shaped by—that world and the novelty that arises out or [sic] it.

Although Figure 1 represents the popular view of the OODA loop, Boyd's sketch of the OODA loop in *The Essence of Winning and Losing* (1995), Figure 2, provides a far more complex representation of the OODA loop which incorporates the unending iteration of observation and conceptualization. [12]

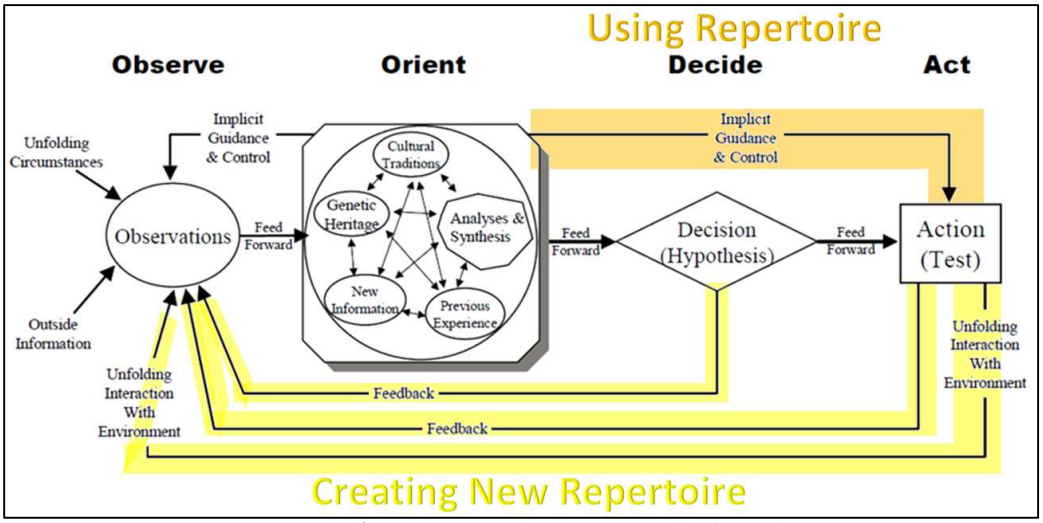


*Figure 2 Boyd's OODA loop, color annotations by the authors*

Referring to Figure 2, the upper path, labeled "Using Repertoire," is a rapid decision making system which uses implicit guidance and control (IG&C) to move from Orient to Act. The alternative decision path, which flows through hypothesis and uses feedback loops to test the hypothesis against reality, is the process of novelty which creates new repertoires. One must recognize, as Boyd did, that a repertoire is a double-edged sword.[13] While a repertoire provides a very efficient path from observation to action, it suffers from the problem of predictability.

Boyd's sketch of the OODA loop provides a far deeper insight into his view of the adversarial engagement than the simple OODA loop illustrated in Figure 1. Each party to the engagement must make observations and process those observations through the orientation process, then use orientation in the decision process, then turn the decisions into actions, which actions change the world which is being observed. Yet, it is even more complex than four sequential stages because each stage of the OODA Loop interacts with the other stages. Berndt Brehmer observed that because the OODA Loop contains numerous feedback loops, the OODA Loop is not truly a loop, instead it is a stage model with multiple loops.[14]

As Boyd hinted in *Aerial Attack Study* (1964),[15] the focus of the OODA loop is not about making faster decisions, rather, the OODA loop is about manipulating the environment to "inhibit an adversaries capacity to adapt to such an environment (suppress or distort observations)."[16] Instead of the

environment being a valuable information source for the adversary to analyze and use to improve its posture (the traditional analysis of Joint Doctrine's "Paradox of Warning"),[17] Boyd saw the environment as a means of disorientation to disrupt the adversary's decision-making. Disorientation is the intentional result of exploiting ambiguity, deception, superior mobility and surprise to subvert, disrupt or seize the connections, centers and activities that allow the adversary to function.[18] The goal of manipulating the environment is to:[19]

> Unstructure adversaries [sic] system into a "hodge podge" of confusion and disorder by causing him to over and under react because of activity that appears uncertain, ambiguous or chaotic.

In Boyd's analysis, the world is an uncertain place. Each adversary's OODA loop changes the world which is being observed. Thus, the adversarial engagement can be represented as two OODA loops which share a common environment into which the adversaries intentionally and unintentionally place artifacts, and from which observations are made.[20] Figure 3 from Naval Doctrine Publication 6 (NDP 6) illustrates interacting OODA loops.[21]

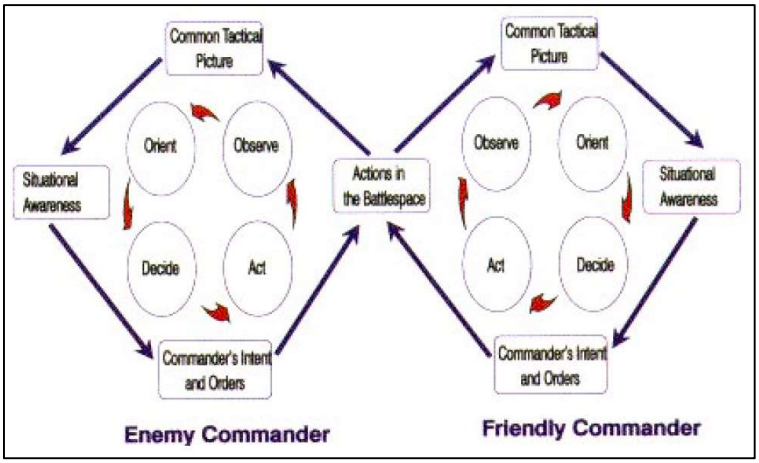


*Figure 3 Interaction of Friendly and Enemy Decision and Execution Cycles. Source: NDP 6*

Human adversaries observe unfolding events and change their behavior in response to adversary actions. NDP 6 notes the competitive nature of OODA loops:[22]

> Rather than operating in isolation, decision and execution cycles take place simultaneously, but not in synchronization, for both sides in combat...Since war is competitive, it is not the absolute speed of decision and execution that matters, but our speed relative to the enemy. Our goal is to be faster than the enemy, which means interfering with his command and control as well as streamlining our own. With this ability, we generate a dominant tempo that allows us to control the enemy's ability to transition between the different phases of the decision and execution cycle.

An example from the Vietnam War illustrates Boyd's analysis. The air combat superiority of North Vietnamese MiGs was a serious threat to U.S. bombers. In Operation BOLO, the U.S. manipulated the OODA loop of the North Vietnamese.[23] Derived from their observations, the North Vietnamese ground controllers had a concept of the radio traffic, routes and radar imagery of attacking U.S. F-105 bombers. When the ground controllers observed the radio and radar events that were consistent with an F-105 bombing raid, the ground controllers would send MiG fighters to intercept and destroy the U.S. bombers. Due to the air combat superiority of fighters over bombers, the North Vietnamese inflicted heavy losses on the U.S. bombers. Brigadier General Robin Olds, USAF, Deceased, turned the North Vietnamese air defense concept against the North Vietnamese. Olds equipped U.S. fighters with electronics to mimic bombers, flew bombing routes, and used bomber call signs and codewords. Olds also deployed fighters along North Vietnamese paths of retreat. When Olds attacked, the North Vietnamese ground controllers assembled their observations, applied their concepts to orient, decided

to engage with what they concluded were U.S. bombers and acted by sending MiGs to engage the presumptive bombers. Olds had interfered with the North Vietnamese OODA loop by using their concept of a U.S. bombing raid to disorient the ground controllers. No doubt North Vietnamese air defenses suffered substantial confusion and surprise when their pilots engaged U.S. fighters instead of U.S. bombers. The superior U.S. fighters inflicted heavy losses on the North Vietnamese air force. The secret of Olds' success was not that he made a faster decision, rather, it was his understanding of his adversary's conception of reality.

Boyd describes the adversarial relationship in terms of competing mental models which evolve with changing circumstances against a backdrop of time constraints. This is a conflict which unfolds in the minds of the adversaries. The minds of the adversaries compromise the cognitive dimension of the information environment.[24] It is for this reason that the authors have previously advocated the addition of the cognitive dimension as a fourth layer in the model of cyberspace.[25] Adding the cognitive dimension to cyberspace changes the analysis of cyberspace operations from a search for vulnerabilities in hardware and software into an engagement which includes information operations. The proposed revised layers of cyberspace are shown in Figure 4.

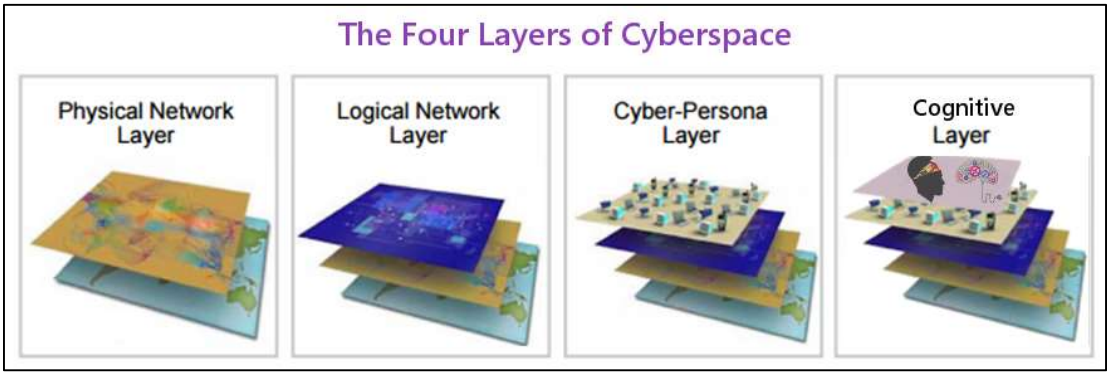


*Figure 4 The Four Layers of Cyberspace, Adapted from Joint Publication (JP) 3-12(R) Cyberspace Operations*

**OODA Loop – A Tool of Cognitive Engagement**

*On two occasions I have been asked, "Pray, Mr. Babbage, if you put into the machine wrong figures, will the right answers come out?" ... I am not able rightly to apprehend the kind of confusion of ideas that could provoke such a question.*

- Charles Babbage[26]

"Situational awareness" is a term from psychology which describes both a field of study and the coupling of actors to their operating environment.[27] Simply stated, situational awareness is knowing what's going on around you. Situational awareness researchers identify three mutually exclusive states of situational awareness.[28] These states are:

- **Retrospective** explanatory analysis; "what has happened?"
- **Concurrent** situational awareness; "what is happening?"
- **Prospective** predictive analysis; "what will happen?" [emphasis in original]

**The genius of OODA loop analysis was Boyd's recognition that an adversary's prospective predictive analysis could be weaponized, leading to a future loss of situational awareness.** We saw this in Operation BOLO when the attacking US forces devised their attack to invoke a prospective predictive analysis which resulted in a loss of situational awareness during the course of the engagement. Rather than using terms of psychology that did not exist in his time, Boyd used the ancient lexicon of Sun Tzu to describe states of situational awareness.[29] Boyd used Sun Tzu's term "cheng" to describe taking actions that are consistent with the adversary's expectations. Boyd used Sun Tsu's term "ch'i" to describe taking

actions inconsistent with the adversary's expectations, thereby depriving the adversary of situational awareness.

Because "present loops shape the character of future orientation"[30] Boyd set forth five techniques that place information into the environment with the intent to disrupt future orientation. These five OODA loop manipulation techniques are, quoting Boyd:[31]

- Ambiguity:
  Alternative or competing impressions of events as they may or may not be.
- Deception:
  An impression of events as they are not.
- Novelty:
  Impressions associated with events/ideas that are unfamiliar or have not been experienced before.
- Fast transient maneuvers:
  Irregular and rapid/abrupt shift from one maneuver event/state to another.
- Effort (cheng/ch'i or Nebenpunkte/Schwerpunkt):
  An expenditure of energy or an irruption [sic] of violence—focused into, or thru, features that permit an organic whole to exist.

These five techniques are used to create any or all of disorientation (a mismatch of events and observations), disruption (the adversary being engaged in uncoordinated actions) and overload (events unfold faster than the adversary can adapt).[32]

Cybersecurity practitioners use the OODA loop to promote the value of machine learning and artificial intelligence to improve cybersecurity.[33] The underlying concept is that data processing systems and machine learning can improve cybersecurity by speeding the execution of OODA loop.[34] The concepts of the OODA loop are used to make cybersecurity trustworthiness assessments.[35] IBM's Watson AI system uses the OODA loop as an information feedback loop to assimilate and comprehend over 100 analytics in its decision making process.[36] According to IBM, [37]

> Whereas the current generation of systems are reactive—detecting and responding to anomalies or attacks—cognitive security is proactive. Forward focused and continuously multi-tasking, cognitive systems scour for vulnerabilities, connect dots, detect variances and sift through billions of events to build upon a base of actionable knowledge.

This is a temporal jumble. What IBM calls "cognitive security" is conflating the three states of situational awareness. Collecting and analyzing historical events is retrospective explanatory analysis. Applying past knowledge to current events is concurrent situational awareness. Anticipating that future attacks will mimic prior attacks is prospective predictive analysis. While there is no doubt that more rapidly identifying, analyzing and understanding new attacks allows defenses to be more quickly adapted to changing events, this is not a predictive activity, this is a reactive activity. AI and machine learning systems seek to process historical information more quickly than humans can perform this task; the machines are not receiving signals from the future.[38] The machines cannot overcome data which lacks sufficient information from which to draw conclusions.[39] Moreover, as the number of variables and the size of the data sets increase, the number of statistically significant spurious correlations observed in historical data increases more quickly than the useful information.[40] This means that positive predictive power (PPV) of relationships uncovered in "big data" analysis are often overstated or simply wrong.[41]

Cybersecurity analysis focusing on the speed of an introspective process entirely misses the point of Boyd's OODA loop. When Boyd referred to "getting inside the adversary's OODA loop," he was not referring to speed, but to "friction." Boyd's organizing theme is friction. Friction impedes activity. The

effects of friction unfold through the execution of the competing OODA loops. **Friendly forces need to diminish their own friction while increasing the "adversary's friction and stretch out his time (for a favorable mismatch in friction and time)**, thereby denying the adversary the opportunity to cope with events/efforts as they unfold." [emphasis added][42]

Knowing the adversary is making a decision, the point of Boyd's OODA loop is to understand and exploit the adversary's decision making process long enough to achieve the desired objective. Consider the case of cold war submarine warfare.[43] Because propeller turbulence interfered with sonar observations behind a submarine, submarines tailed one another by hiding in the propeller turbulence. Submarines countered tailing operations by using evasive maneuvers. Submarine commanders, being human beings, tended to engage in anti-tailing maneuvers on a habitual schedule. U.S. submarine commanders exploited the habits of Soviet submarine commanders to track Soviet submarines for long periods of time.

> ***But what happens when suddenly our data is manipulated, and you no longer can believe what you're physically seeing?*** Admiral Michael Rogers, NSA Director[44]

The problem of trust assessment illustrates the manipulation of observations to influence decision making. Manipulation of trust is a hallmark of deception. Bernie Madoff is an example of this problem. Until his fraud was uncovered, he was a respected member of the financial community entrusted with billions of dollars. One of the greatest deceptions of all time was Operation FORTITUDE in which, over a period of several years, the British used a double agent who ultimately convinced the Germans that the Allied invasion would be at Calais. In reliance on false information from their trusted spy, the Germans concentrated defenses in Calais before, during and after D-Day. [45]

Thieves transferred almost $1 billion from the Central Bank of Bangladesh. They accomplished this feat by using stolen credentials to authorize the transfers and obscured the theft by changing two bytes of code in the targeted bank's funds tracking program.[46] The thieves' booty was ultimately trimmed to $101 million due to the thieves' spelling errors and the coincidence that one of the banks the thieves used to move the money shared a name with an entity on a Federal Reserve Bank watch list.[47]

Disruption of trusted sensors can lead to confusion and disarray among adversary forces.[48] Joint Publication (JP) 3-13.1 *Electronic Warfare* makes over forty references to deception as a tool of EW; on the other hand, Joint Publication (JP) 3-12(R) *Cyberspace Operations* makes none. False data can be used to subvert the decision making of Non-Person Entities (NPEs) that operate control systems, such as the power grid.[49] In a 2014 literature review, researchers discovered "the vulnerability of cyber situational awareness to deception is virtually absent from the literature, save the low-level race between exploits and intrusion detection systems."[50] Computational implementations of the OODA loop, being introspective, fail to take into account the manipulation of events to subvert the introspection process. Boyd warned that a system cannot validate itself.[51]

Recent advances in situational awareness research recognize that situational awareness is a systems level phenomenon in which "you" is the structure comprised of systems that include individuals, groups of individuals and non-human elements.[52] Researchers call this systems level approach "distributed situational awareness" or DSA. The crash of Air France Flight 447 demonstrates a failure of DSA in a complex system of men and machines.[53] In this tragedy the Pitot tubes froze, causing these crucial air speed sensors to fail. In response to Pitot tube failure and subsequent loss of air speed data, the autopilot disengaged. The human pilots, being unaware of the failure of the Pitot tubes or the disengagement of the autopilot, failed to take appropriate actions to control the plane. This is an example of how the false data from a sensor rippled through the OODA loops of men and machines in a failure of DSA.

OODA loop abuse is the lynchpin of every cyberattack. All cyberattacks can be seen as attacking DSA through the manipulation of OODA loops in which the attacker manipulates one or more of the OODA loops which contribute to DSA. The key to manipulating any OODA loop is understanding how the particular OODA loop works. Consider the example of a modern container terminal.[54] A modern container terminal is a marvel of automation. NPE operate automated mechanical handling equipment which moves containers from vessels and around the facility. The overall facility operates under the control of a Terminal Operating System which coordinates the movement of everything within the port, optimizing the flow of containers thereby optimizing port efficiency. The entire system is driven from container identifying information which is scanned using optical character recognition (OCR) and RFID. Thus, the OODA loop of the Terminal Operating System is dependent upon the OCR and RFID. Criminals engage in smuggling operations by corrupting that OCR and RFID information. Similarly, the OODA loops of GPS navigation and guidance systems can be disoriented by manipulating the input electromagnetic signals.[55] Ships' crews, seeking to evade detection of questionable activities, manipulate the OODA loops of tracking authorities by leveraging knowledge of shipping routes, shipping patterns and gaming electronic ship tracking systems.[56] The OODA loop of the powergrid management system depends upon satellite signals to coordinate grid management; false data can be presented to the sensors of the powergrid management network to disrupt that OODA loop and bring down the powergrid.[57]

The Business Email Compromise (BEC) illustrates an attack on layered defenses. As the BEC demonstrates, layered defenses are actually the interactions of OODA loops. Whether a particular layer is a defense or vulnerability can only be determined by the operation of its OODA loop in the context of DSA. In a BEC, adversaries seek to steal money by causing payments to be made to the adversary.

- Defensive Layer 1 - email spam filter. This OODA loop observes email characteristics and uses email characteristics to orient and determine if an email should be delivered. The adversary manipulates spam filter OODA loop using the tools of email marketing.
- Defensive Layer 2 - next generation firewall (NGF). The NGF's OODA loop observes the operation of files associated with the email by performing any executable files associated with the email and orients based on the results of the file execution. The adversary manipulates the NGF's OODA loop by sending an email that contains only text, there are no machine executables to observe.
- Defensive Layer 3 - human email recipient. The human's OODA loop observes the human-readable content of the email. The adversary manipulates the human's OODA loop by composing a deceptive message that contains false payment instructions for the human to enter into the accounting system. It is important to note that the OODA loop of a person does not require a conscious cognitive process. In fact, the adversary may intentionally target non-cognitive processes, such as habits, in which the OODA loop orientation, decision and act phases are a repertoire comprised of non-cognitive habitual responses or responses of low cognitive elaboration.[58] Cyber attackers frequently exploit activities that do not trigger significate user analysis (such as processing email, opening documents or entering credentials).
- Defensive Layer 4 - accounting system's access control process. The accounting system's access control system OODA loop observes user credential inputs and orients based on the credential data entered into the system. The adversary manipulates the accounting system's access control OODA loop by subverting the human OODA loop.
- Defensive Layer 5 - accounting system's data entry process. The accounting system's process's OODA loop observes user data entry inputs and orients based on the data entry requirements of the system. The adversary manipulates the accounting system's data entry OODA loop by, again, subverting the human OODA loop.
- Defensive Layer 6 - accounting system's payment processing system. This OODA loop observes payment instructions and orients based on the data residing in the system. The adversary, through the previous OODA loops, has introduced factually false payment data into the accounting system. The accounting system issues payments to the adversary using the factually invalid payment data.

In the BEC there are no data processing errors or malware or log files or other computing artifacts that could reveal the disorientation of the payment system. The loss of DSA in the BEC results from the interaction of these NPE and human OODA loops. Wells Fargo Bank recommends defending against the BEC by modifying the OODA loops through the addition of non-data processing steps in the vendor account maintenance process.[59]

Every decision making activity can be compromised by either or both of deceiving humans and manipulating data streams in a system of interacting OODA loops. Large portions of the Ukrainian power were brought down by a deceptive email which compromised the credentials of a human grid operator.[60] In the Stuxnet incident, users were unwittingly recruited to defeat the defensive OODA loops; in this case transporting innocent looking USB devices into the facility and plugging the USB devices into the network.[61] Much of the information about the attack is subject to obfuscation by the attacker.[62] Often the very machine data which feeds the defensive OODA loops is subject to anti-forensic manipulation by the attacker. Adversaries alter log files. Adversaries intentionally trigger deceptive alarms.[63] Adversaries hide the true nature of software, tricking defenders into whitelisting malicious code.[64] Adversaries lie and cheat. Understanding the "connect the dots" process used by defenders, the adversary applies the Maxims of Deception to distort the dots, thus undermining the work of cyberintelligence.[65] The OODA loops of people and NPE provide opportunities for adversary manipulation.

In August of 2015, the NSA released its Methodology for Adversary Obstruction.[66] The Methodology for Adversary Obstruction focuses on the actions undertaken by human adversaries during engagements in cyberspace. The Methodology for Adversary Obstruction introduces the terms, Access, Persistence and Control, to describe the evolution of a cyber engagement. Access (A) refers to how an intruder connects to the targeted network. The intruder then aims for persistence (P) by creating a "foothold" in the network to allow a sustained presence. All of these actions are focused on gaining control (C) to achieve the final objective, whether it is to interfere, monitor, steal or alter data, deceive, disable or destroy.[67] Each of these phases can be seen as sequences of OODA loops. Looking at the BEC example, access was gained by attacking the OODA loops of NPE and people. Persistence was gained from the human OODA loop. Control was the result of the adversary's false data becoming embedded in the payment OODA loop.

The Methodology for Adversary Obstruction is designed to decrease the tools, tactics and procedures that an adversary can employ against a target. The Adversary Obstruction Methodology addresses the system of interdependent OODA loops created by cyberspace's pervasive communication, command and control network. The Methodology for Adversary Obstruction sets forth the principles of cyber defense, which seek to limit access, persistence and control. These principles are:[68]

- Generate a plan to respond and ensure it is fully implemented without exceptions
- Reduce the attack surface to reduce external attack vectors into the network
- Harden devices to reduce internal and external attack vectors into the network
- Implement Credential Protections to degrade the adversaries' ability to maneuver on the network
- Align defensive resources to improve detection of and response to adversary activity
- Segregate networks and functions to contain damage when an intrusion occurs
- Develop a culture of cyber professionalism, to include leaders who set expectations

We propose combining OODA loop DSA analysis with the NSA's Access, Persistence, Control model to reveal dependences which are obscured by focusing on machines performing data processing tasks. The addition of one new principle is required to incorporate Boyd's OODA loop into the NDA's Methodology for Adversary Obstruction. That new principle is:

- Diminish friendly friction while increasing the adversary's friction.

Effective OODA loop analysis requires analysis of the completing OODA loops, not merely speeding defensive decision making processes. By knowing that the adversary is executing its own OODA loops, friendly forces can take measures to increase the adversary's friction. Referring back to cold war submarine warfare, in order to avoid becoming victims of their own habits, U.S. submarine commanders used playing dice to determine the timing of evasive maneuvers.[69] Randomization is a highly effective defensive strategy.[70] Randomization is an excellent means of befuddling the statistical inference engines used in machine learning and AI systems.[71]

Analyzing the friction of the competing OODA loops at each phase of the adversarial engagement reveals opportunities to tilt the engagement against the adversary. A few examples illustrate this concept. In cyberspace, access to systems is often gained by using common naming conventions to guess the email addresses of phishing targets. Attackers are aided in this process by email "bounce" messages. Understanding that the adversary's OODA loop is correlating email address guesses and system bounce messages opens OODA loop disruption opportunities. For example, simply inserting a few random characters in employee email addresses and suppressing bounce messages would increase the adversary's friction.[72] The increased difficulty of guessing email addresses will result in more rejected emails. The log files generated by the increased volume of rejected emails associated with repeated incorrect guesses can be a rich source of forensic data for security analysts. Friction generates heat and heat can be detected.

Adversaries often abuse credentials to compromise systems. Users inadvertently disclose credentials to adversaries in response to email attacks.[73] Users intentionally engage in poor credential practices which assist adversaries in compromising compromises.[74] Email systems can be enhanced with anti-deception technology to defend the email recipients' OODA loops against emails that facilitate the theft of credentials.[75] Adopting two factor authentication (2FA) introduces new requirements into the log-in process, thereby increasing the adversary's friction when using compromised credentials.[76] But that is not the end of the analysis. What adaptations will the adversary make to exploit the new OODA loop? 2FA that uses cellphones as the second factor can be undermined by compromising the user's cell phone or the cell phone 2FA process itself.[77] This OODA loop analysis reveals the adversary's next move, suggesting the need to adopt 2FA methods that are resistant to cell-phone compromise attacks such as fido[78] 2FA will also result in log-in failures when adversaries attempt to use defective stolen credentials. Again, increasing the adversary's friction generates heat for defenders to detect.

These ruses (modified email address/bounce suppression and 2FA) illustrate how deception can be used in defensive cyberoperations to assign tasks to the adversary which will consume the adversary's resources and disrupt decision-making, thereby increasing the friction of the adversary's OODA loop.

In addition to increasing the adversary's friction, the proposed principle looks to reducing friendly friction. This facet of the principle requires that when new measures are contemplated, the effect on friendly OODA loops must be considered. [79] Security measures which interfere with the performance of job tasks impose friction on system administrators (sysadmins) and users. This friction results in systems that sysadmins cannot maintain and users, being frustrated in the performance of their job tasks, circumvent. Recent press reports indicate that a leading international cyber security consulting firm has created a system in which sysadmins and users routinely engage in poor security practices.[80] "The goal is to build systems that are actually secure not theoretically secure: Security Mechanisms have to be usable in order to be effective."[81]

Applying OODA loop analysis can reveal crucial steps in DSA where modified friendly processes can defend against attempts to subvert friendly OODA loops, increase the adversary's friction and reduce friendly friction.

*The views expressed herein are the views of the authors and do not reflect the views of Iconix, Inc. or PepsiCo, Inc.*

## References and Notes


[1]. Shipley, David. "Why We're Losing the War for Cyber Security." *Pulse*. LinkedIn, 6 Jan. 2016. Web. 12 Sept. 2017. < https://www.linkedin.com/pulse/why-were-losing-war-cyber-security-david-shipley>.

[2] Hammond, Grant T. *The Mind of War: John Boyd and American Security*. Washington, D.C.: Smithsonian Books, 2004. Print. p.56.

A 6.5 hour briefing by Boyd is available in 14 parts on YouTube at https://www.youtube.com/user/Jasonmbro/videos

[3] Boyd, John. "Patterns of conflict." *Unpublished Paper, December* (1986). Slide 5.

[4] Osinga, Frans P. *Science, Strategy and War: The Strategic Theory of John Boyd*. New York: Routledge, 2007. Page 6.

[5] Muniz, Joseph, Gary McIntyre, and AlFardan Nadham. *Security Operations Center: Building, Operating, and Maintaining Your SOC*. Indianapolis: Cisco Press, 2015. Page 3.

[6] Biermann, Joachim, Pontus Horling, and Lauro Snidaro. "Automated support for intelligence in asymmetric operations: Requirements and experimental results." *Information Fusion, 2009. FUSION'09. 12th International Conference on*. IEEE, 2009.

Blasch, Erik P., et al. "User information fusion decision making analysis with the C-OODA model." *Information Fusion (FUSION), 2011 Proceedings of the 14th International Conference on*. IEEE, 2011.

Blasch, Erik, et al. "Issues and challenges in resource management and its interaction with levels 2/3 fusion with applications to real-world problems: an annotated perspective." *Proceedings of SPIE*. Vol. 6567. 2007.

Brehmer, Berndt. "The dynamic OODA loop: Amalgamating Boyd's OODA loop and the cybernetic approach to command and control." *Proceedings of the 10th international command and control research technology symposium*. 2005.

Dussault, H. M. B., and Maciag, C. J. Forensics, Fighter Pilots and the OODA Loop: The role of digital forensics in cyber command and control. *Digital Forensic Research Workshop*, 2004.

Gray, Douglas. *Improving Cybersecurity Governance Through Data-Driven Decision-Making and Execution (Briefing Charts)*. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2014.

[7] Wisniewski, Brian D., et al. "Improving Federal Cybersecurity Governance Through Data-Driven Decision Making and Execution." (2015). P. 5.

[8] Personal interview with a naval aviator who flew electronic warfare combat missions and who wishes to remain anonymous.

[9] Boyd, J. "Destruction and Creation, 1976." *Unpublished Essay, available at http://www.goalsys.com/books/documents/DESTRUCTION AND CREATION. pdf*. Slide 5.

[10] Smith, Kip, and Peter A. Hancock. "Situation awareness is adaptive, externally directed consciousness." *Human Factors* 37.1 (1995): 137-148.

[11] Boyd, John. "Conceptual spiral." *Lecture to Naval War College Faculty. Naval War* (1991). Slide. 38

[12] Boyd, John R. "The essence of winning and losing." *Unpublished lecture notes* (1996). Slide 3.

[13] Boyd, John. "Patterns of conflict." *Unpublished Paper, December* (1986). Slides 37-39.

[14] Brehmer, fn. 6.

For a comprehensive discussion of the OODA Loop and its embedded feedback loops, the reader is referred to:

Angerman, William S. *Coming full circle with Boyd's OODA loop ideas: An analysis of innovation diffusion and evolution*. No. AFIT/GIR/ENV/04M-01. AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH SCHOOL OF ENGINEERING AND MANAGEMENT, 2004.

Osinga, fn.4,

Schechtman, Gregory M. *Manipulating the OODA Loop: The Overlooked Role of Information Resource Management in Information Warfare*. No. AFIT/GIR/LAL/96D-10. AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH, 1996.

Tremblay Jr, Major Paul. *Shaping and Adapting Unlocking the power of Colonel John Boyd's OODA Loop*. Diss. masters thesis, United States Marine Corps Command and Staff College, 2015). Accessed on 1 January 2015. https://fasttransients.files.wordpress.com/2015/04/tremblayshapingadapting. pdf, 2015.

[15] Boyd, J. R. "Aerial Attack Study (Monograph)." (1964). Page 68.

[16] Boyd, John. "A New Conception of Air to Air Combat." *unpublished presentation* (1976). Slide 22

[17] Joint Publication (JP) 2-0, *Joint Intelligence*. Page I-27.

[18] See, for example, Boyd, fn. 13, Slide 98.

[19] Boyd, fn. 13, Slide 22.

[20] Naval Doctrine Publication 6, "Naval Command and Control." Department of the Navy (USA), 1995. Page 60.

[21] NDP 6, fn. 20, Page 60.

[22] NDP 6, fn. 20, Page 60.

[23] "National Museum of the US Air Force." *OPERATION BOLO > National Museum of the US Air Force > Display*. N.p., n.d. Web. 15 Sept. 2017. <http://www.nationalmuseum.af.mil/Visit/Museum-Exhibits/Fact-Sheets/Display/Article/196006/operation-bolo/>.

[24] Joint Publication (JP) 3-13, *Information Operations*. Page. I-3.

[25] Zager, Robert P., and John A. Zager. "George Washington's Teachings on Cyberwar." *Cyber-Physical Systems Virtual Organization*. National Science Foundation, 22 May 2017. Web. 15 Sept. 2017. <https://cps-vo.org/node/35651>.

[26] Charles Babbage, *Passages from the Life of a Philosopher*, London, Longman, Green, Longman, Roberts and Green, 1864, page 67.

[27] Stanton, N. A., et al. "State-of-science: situation awareness in individuals, teams and systems." *Ergonomics* 60.4 (2017): 449-466.

[28] DeYoung, Mark E., Randy Marchany, and Joseph Tront. *Network Security Data Analytics Architecture for Logged Events*. Virginia Tech, 4 Jan. 2017. Web. 11 Oct. 2017. <https://vtechworks.lib.vt.edu/handle/10919/77421>.

[29] Boyd, fn. 13. Slide 13.

[30] Boyd, John R. "Organic design for command and control." *A discourse on winning and losing* (1987). Slide 16

[31] Boyd, fn. 13. Slide 117.

[32] Boyd, fn. 13. Slide 117.

[33] Brooks, Teresa Nicole. "Survey of Automated Vulnerability Detection and Exploit Generation Techniques in Cyber Reasoning Systems." *arXiv preprint arXiv:1702.06162* (2017).

[34] Duffy, Nigel. "AI: Accelerating Decision-Making." *CIO Review*. CIO Review, n.d. Web. 11 Sept. 2017. <https://artificial-intelligence.cioreview.com/cxoinsight/ai-accelerating-decisionmaking-nid-23303-cid-175.html>.
Riley, Shawn. "Getting Inside the Threat Actor's OODA Loop to Stop Undetectable TTPs." *Pulse*. LinkedIn, 18 Sept. 2014. Web. 15 Sept. 2017. <https://www.linkedin.com/pulse/20140918175209-36149934-getting-inside-the-threat-actor-s-ooda-loop-to-stop-undetectable-ttps>.

[35] Arunkumar, Saritha, et al. "Assessing trust over uncertain rules and streaming data." *Information Fusion (FUSION), 2013 16th International Conference on*. IEEE, 2013.

[36] Muresan, Michael, and Lee Angelelli. "Next Generation Technology Applying Cognitive Solutions to Modeling and Simulation." *SISO*. Simulation Interoperability Standards Organization, 7 June 2016. Web. 11 Oct. 2017. <https://discussions.sisostds.org/index.htm?A3=ind1606&L=SIW-SG-ENGTAM&E=base64&P=8976&B=--_002_432F864F9D89B94F9D1A6AF48BF6E1E4A39D83B4UGUNHPAFIeasfcs_&T=application%2Fpdf;%20name=%22Applying%20Cognitive%20Systems%20To%22&N=Applying%20Cognitive%20Systems%20To&attachment=q>.

[37] "Evolve Your Defenses with Security That Understands, Reasons and Learns." *Cognitive Security White Paper*. IBM, n.d. Web. 15 Sept. 2017. <http://cognitivesecuritywhitepaper.mybluemix.net/>.

[38] Taleb, Nassim Nicholas. *Antifragile: Things that gain from disorder*. Random House, 2012. Page 68.

[39] Vijayan, Jai. "New Locky Ransomware Phishing Attacks Beat Machine Learning Tools." *DARKReading*. InformationWeek, 28 Sept. 2017. Web. 10 Oct. 2017. <https://www.darkreading.com/attacks-breaches/new-locky-ransomware-phishing-attacks-beat-machine-learning-tools/d/d-id/1330010?_mc=sm_dr>.

[40] Taleb, Nassim N. "Beware the Big Errors of 'Big Data'." Wired, 8 Feb. 2013. Web. 15 Sept. 2017. <https://www.wired.com/2013/02/big-data-means-big-errors-people/>.

[41] Ioannidis, John PA. "Contradicted and initially stronger effects in highly cited clinical research." *Jama* 294.2 (2005): 218-228.
Ioannidis, John PA. "Why most published research findings are false." *PLoS medicine* 2.8 (2005): e124.

[42] Boyd, fn. 30, Slide 23.

[43] Sontag, Sherry, and Christopher Drew. *Blind man's bluff: The untold story of American submarine espionage*. PublicAffairs, 2016. Chapter 6.

[44] Berman, Dennis K, *Adm. Michael Rogers on the Prospect of a Digital Pearl Harbor*, Wall Street Journal, 26 October 2015. Web. 26 October 2015, <http://www.wsj.com/article_email/adm-michael-rogers-on-the-prospect-of-a-digital-pearl-harbor-1445911336-lMyQjAxMTA1NzIxNzcyNzcwWj>.

[45] D-Day's Operation OVERLORD provides an example of the advantage to be gained by controlling the adversary's decision-making process. For years prior to the D-Day invasion, Allied Intelligence services carefully manipulated the German's OODA loop through a masterfully orchestrated misinformation campaign, Operation FORTITUDE. At the heart of this campaign stood a single man – Juan Pujol García, a failed Spanish chicken rancher codenamed "Garbo." Through a series of unbelievable events, Pujol became a German spy who turned his loyalties to the Allies. Starting in April of 1942, British intelligence used Pujol, the trusted German spy, to feed deceptive information to the Germans. For over three years leading up to D-Day and following the invasion, the Allies used Pujol to corrupt the German OODA loop. British intelligence deceived the Germans into believing that the Allies would invade at Calais. While the landings at Normandy were underway Pujol convinced the Germans that the invasion of Normandy was a diversionary measure, thereby forestalling the redeployment of German defenses from Calais. After it became clear that Normandy was not a diversion, Pujol maintained his trusted relationship with the Germans by convincing the Germans that the Allies had changed plans after the Normandy invasion. As the Nazi empire collapsed following the Allied invasion, the Nazi's awarded Pujol the Iron Cross for his services to the Reich. See, Seaman, Mark. *Garbo: The Spy Who Saved D-Day*. Dundurn, 2004.

[46] Shevchenko, Sergei. "Two Bytes to $951m." *BAE Systems Threat Research Blog*. BAE Systems, 15 Sept. 2017. Web. 15 Sept. 2017. <http://baesystemsai.blogspot.com/2016/04/two-bytes-to-951m.html>.

[47] Perlroth, Nicole, and Michael Corkery. "Details Emerge on Global Bank Heists by Hackers." *Details Emerge on Global Bank Heists by Hackers - The New York Times*. The New York Times Company, 13 May 2016. Web. 15 Sept. 2017. <https://www.nytimes.com/2016/05/14/business/dealbook/details-emerge-on-global-bank-heists-by-hackers.html>.

Das, Rishna N., and Jonathan Spicer. "How the New York Fed Fumbled over the Bangladesh Bank Cyber-heist." *Reuters Investigates*. Reuters, 21 July 2016. Web. 18 Sept. 2017. <http://www.reuters.com/investigates/special-report/cyber-heist-federal/>.

[48] John A. Volpe National Transportation Systems Center. *GPS Dependencies in Transportation: An Inventory of Global Positioning System Dependencies in the Transportation Sector, Best Practices for Improved Robustness of GPS Devices, and Potential Alternative Solutions for Positioning, Navigation and Timing*. Cambridge, Massachusetts: U.S. Department of Transportation, 2016.

[49] Akkaya, Ilge, Edward A. Lee, and Patricia Derler. "2013 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)."

[50] Franke, Ulrik, and Joel Brynielsson. "Cyber situational awareness–a systematic review of the literature." *Computers & Security* 46 (2014): 18-31.

[51] Boyd, fn. 30, Slide 20

[52] Salmon, Paul M., Guy H. Walker, and Neville A. Stanton. "Pilot error versus sociotechnical systems failure: a distributed situation awareness analysis of Air France 447." *Theoretical Issues in Ergonomics Science* 17.1 (2016): 64-79.

[53] Salmon, fn. 52.

[54] Beaumont, Peter, and Stephen Wolthusen *Cyber-risks in Maritime Container Terminals: Analysis of threats and simulation of impacts, Royal Holloway University of London, ISG MSC Information Security thesis series 2017,*

[55] Starr, Michelle. "Students hijack US$80m yacht with GPS spoofing - Roadshow." Roadshow. CNET, 29 July 2013. Web. 25 Jan. 2017. <https://www.cnet.com/roadshow/news/students-hijack-us80m-yacht-with-gps-spoofing/>.

[56] Ridwell, Henry. "Cargo Vessels Evade Detection, Raising Fears of Huge Trafficking Operations." *VOA*. Voice of America, 31 Mar. 2017. Web. 18 Sept. 2017. <https://www.voanews.com/a/cargo-vessels-evade-detection-trafficking/3789296.html>.

[57] Akkaya, fn. 49.

[58] Kahneman, Daniel. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux, 2011.

Vishwanath, Arun, Tejaswini Herath, Rui Chen, Jinggou Wang, and Raghav Rao. "Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability Within an Integrated, Information Processing Model." *Decision Support Systems* 51.3 (2011): 576-86.

[59] "Protect Your Accounts from Impostor Fraud." *Treasury Insights*. Wells Fargo Bank, n.d. Web. 15 Sept. 2017. <https://digital.wf.com/treasuryinsights/portfolio-items/tm3137/>.

[60] Lipovsky, Robert, and Anton Cherepanov. "BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry." *WeLiveSecurity*. ESET, 4 Jan. 2016. Web. 26 Jan. 2017. <http://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/>.

[61] "Stuxnet." Wikipedia. N.p.: Wikimedia Foundation, 22 Jan. 2017. Web. 23 Jan. 2017.

<https://en.wikipedia.org/wiki/Stuxnet>.
[62] Kessler, Gary C. "Anti-forensics and the digital investigator." *Australian Digital Forensics Conference*. 2007.
Threat Connect Research Team. "Guccifer 2.0: The Man, the Myth, the Legend?." *Threat Research*. ThreatConnect, 20 July 2016. Web. 18 Sept. 2017. <https://www.threatconnect.com/blog/reassesing-guccifer-2-0-recent-claims/>.
[63] Elgin, Benjamin, Dune Lawrence, and Michael Riley. "Neiman Marcus Hackers Set Off 60,000 Alerts While Bagging Credit Card Data." *Bloomberg*. Bloomberg L.P., 24 Feb. 2014. Web. 18 Sept. 2017. <https://www.bloomberg.com/news/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data>.
[64] Kovacs, Eduard. "Cybercriminals Trick Qihoo 360 into Whitelisting Malware." *Security Week*. Wired Business Media, 1 Apr. 2016. Web. 1 Sept. 2017. <http://www.securityweek.com/cybercriminals-trick-qihoo-360-whitelisting-malware>.
[65] Joint Publication (JP) 3-13.4, *Military Deception*. Pages A-1 – A-2.
[66] "NSA Methodology for Adversary Obstruction." *Information Assurance Directorate*. NSA/IAD, 15 Sept. 2015. Web. 26 Jan. 2017. <https://www.iad.gov/iad/customcf/openAttachment.cfm?FilePath=/iad/library/reports/assets/public/upload/NSA-Methodology-for-Adversary-Obstruction.pdf&WpKes=aF6woL7fQp3dJizXCkcbwTeLkU9HubDMyr393t>.
[67] NSA, fn. 66, Page 108.
[68] NSA, fn. 66, Page 108.
[69] Sontag, fn. 43. Page 135.
[70] Joint Publication 3-13.3, *Operations Security*. Page III-6.
[71] Li, Dongxu, and Jose B. Cruz. "Information, decision-making and deception in games." *Decision Support Systems* 47.4 (2009): 518-527.
[72] RFC 5321, Section 6.2.
[73] Schneier, Bruce. "Credential Stealing as an Attack Vector." *Xconomy*. Xconomy, Inc., 20 Apr. 2016. Web. 10 Oct. 2017. <http://www.xconomy.com/boston/2016/04/20/credential-stealing-as-attack-vector/#>.
[74] McMillan, Robert. "The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!." *The Wall Street Journal*. Dow Jones & Company, Inc., 7 Aug. 2017. Web. 18 Sept. 2017. <https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118>.
Sheridan, Kelly. "Credential-Stuffing Threat Intensifies Amid Password Reuse." *DARKReading*. InformationWeek, 23 May 2017. Web. 18 Sept. 2017. <https://www.darkreading.com/vulnerabilities---threats/credential-stuffing-threat-intensifies-amid-password-reuse/d/d-id/1328945>.
Nicholas, Malaika. "How Hackers Steal Your Reused Passwords–Credential Stuffing." *Dashlane Blog*. Dashlane Inc., 2 May 2017. Web. 18 Sept. 2017. <https://blog.dashlane.com/hackers-steal-your-reused-passwords-using-credential-stuffing/>.
Pauli, Darren. "Password Reuse Bot Steals Creds from Weak Sites, Logs in to Banks." *The Register*. Situation Publishing, 24 May 2016. Web. 18 Sept. 2017. http://www.theregister.co.uk/2016/05/24/password_reuse_bot_steals_creds_from_crap_sites_logs_in_to_banks/.
[75] Zager, John, and Robert Zager. "Improving Cybersecurity Through Human Systems Integration." *Small Wars Journal*. Small Wars Foundation, 22 Aug. 2016. Web. 18 Sept. 2017. <http://smallwarsjournal.com/jrnl/art/improving-cybersecurity-through-human-systems-integration>.
[76] Grassi, Paul A., James L. Fenton, Elaine M. Newton, and Andrew R. Regenscheid. *NIST Special Publication 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management*. Gaithersburg, MD: National Institute of Standards and Technology, 2017. *NIST*. NIST, n.d. Web. 18 Mar. 2017. <https://doi.org/10.6028/NIST.SP.800-63b>.
[77] Brandom, Russell. "This Is Why You Shouldn't Use Texts for Two-factor Authentication." *The Verge*. Vox Media, Inc., 18 Sept. 2017. Web. 18 Sept. 2017. <https://www.theverge.com/2017/9/18/16328172/sms-two-factor-authentication-hack-password-bitcoin>.
[78] fido alliance, <https://fidoalliance.org/>.
[79] Theofanos, Mary. *Poor Usability: The Inherent Insider Threat*. Gaithersburg, MD: National Institute of Standards and Technology, 2008. *Computer Security Resource Center*. NIST, 21 Mar. 2008. Web. 22 Sept. 2017. <https://csrc.nist.gov/CSRC/media/Presentations/Poor-Usability-The-Inherent-Insider-Threat/images-media/Usability_and_Insider_threat.pdf>.
[80] Thomson, Iain. "Deloitte Is a Sitting Duck: Key Systems with RDP Open, VPN and Proxy 'login Details Leaked'." *The Register*. Situation Publishing, 26 Sept. 2017. Web. 27 Sept. 2017. <https://www.theregister.co.uk/2017/09/26/deloitte_leak_github_and_google/>.
[81] Theofanos, fn. 79.Page 13.