Military Cyber Affairs
The Journal of the Military Cyber Professionals Association
ISSN: 2378-0789

Volume 2 | Issue 1 Article 4

2016

A Case for Deception in the Defense

Spencer R. Calder
Department of the Army, spencer.r.calder.mil@mail.mil

A Case for Deception in the Defense

Cover Page Footnote
I'd like to thank the Department of the Air Force, the Air University, and its body for helping this idea germinate. Specifically I'd like to thank Dr. Panayotis Yannakogeorgos, Special Agent Zachary Smith, and Majors Abe Rivas, and Sam Kidd for their help and friendship.

A Case for Deception in the Defense

SPENCER R. CALDER, Department of the Army

Cyber deception may be used fairly easily in a contested cyberspace to impose disproportionate operational cost to adversarial actors. Concepts of what comprise a legitimate defensive effort in cyberspace are changing. The concept of a rigid perimeter defense as a panacea are increasingly viewed as a fallacy. "Sovereign" cyberspaces are increasingly contested. Concurrently to these trends, the Department of Defense is moving toward standardization and homogenization of cyberspace that may facilitate enemy operation in our spaces. Military deception doctrine has been used successfully in conflict through the history of warfare in contested spaces and may provide a useful taxonomy to advance this discussion. Civil society has developed several tools that may afford an easy implementation of deception via existing infrastructure. Honeypots, tokens, and moving target defense may be more widely adopted today to sow ambiguity in adversary operations. Deliberate development of a deceptive capability could afford the ability to actually mislead our adversaries.

"It is now widely recognized that traditional approaches to cyber defense have been inadequate."[i] *- Kristen Heckman, et al.*

The Joint Information Environment (JIE) Operational Concept puts forth five imperatives in cyber-defense: to "*protect, detect, characterize, counter[act], and mitigate*"[ii] adversarial activity. The US government is severely challenged to meet this imperative. Protection, mitigation, counteraction and even detection, are problematic via current defensive means. US government cybersecurity efforts today can be categorized as fairly narrow. A recent MITRE study intones military departments have only one effective strategy – incident response.[iii] The community of practice commonly views security in binary terms; strategies are tested and bureaucratically palatable to the CIOs. Webroot – a cybersecurity consultancy – observed this year that 97 percent of exploitive software – malware – they detected was host specific. "Host specificity" counteracts current defensive strategies that "fingerprint" (i.e. create signatures for) malware. This makes exploitation significantly harder to detect, counter, and mitigate using our existing strategy.[iv] In order to provide for effective defense of institutional footholds in cyberspace, security must move past practices that are bureaucratically inexpensive. Cybersecurity must strive to be robust in the statistical sense, guarding against unforeseen threat vectors, and oriented towards the most acceptable outcomes. Instead of serving the CIO's "rate of detection" metrics, cybersecurity must be oriented towards success supporting national military objectives, in and through cyberspace. Despite the categorization of network defensive strategy as defense in depth, DoD Cybersecurity Providers increasingly pursue a limited set of tactics in support of bureaucratic aims.

The goal of this paper is to demonstrate the utility of including deception in cyber-defense doctrine, and to explore the benefits of its implementation. This study is designed for policymakers and cyber-professionals of all US Government entities to assist in formulation of new strategy. This paper will examine cyberspace and security broadly, highlight emerging concepts, and use military deception parlance to frame them. It is the belief of the author that defensive deception is a capability worth pursuing and that through the implementation of a defensive deception capability, we may impose disproportionate cost to adversarial decision-making.

1. Strategic Imperative

Currently US information and communication technology operates in a confederation of separate enclaves, pursuing security only at our perimeters. This is changing; however, what the changes mean has yet to be seen. As early as 2010, the communications community began to coalesce around the idea of a "Joint Information Environment"[v] (JIE). This environment was meant to simplify operation and defense of the systems supporting DoD operations. Through moving away from localized operation, maintenance, and defense into a single converged framework, the JIE ultimately converged control and cut cost. Several core services began to collapse into operation by the Defense Information Systems Agency (DISA). It began with authentication services, web-portals, and eventually interdepartmental email.

The most pertinent to this discussion are the proposed changes to the DoD's security architecture. The JIE Single Security Architecture (SSA), which includes Joint Regional Security Stacks(JRSS), is a grouping of sensors that use "fingerprinting" to detect and proactively block malware. While this does protect US government cyber-geography as pointed out previously, it's efficacy is increasingly challenged. Malware is adapting to bypass this methodology. Moreover, it relies on previous execution and detection of the malware to perform its job. This may not seem vital, but attackers favor undiscovered exploits when stakes are high. That is to say, in a war, the JRSS won't be of much use. Further still, under JIE's proposed SSA, the Departments (i.e. Army, Air Force, and Navy) will collapse into a jointly managed architecture. The outward appearance of improved security may be deceptive. In its effort to make an effective, clear, and unambiguous operating environment for joint management, it will have the same effect for adversarial actors. In pursuit of the best business case, the DoD set prime conditions for exploitation of US networks.

2. Human behavior is human behavior, even in cyberspace.

We bring with us the complexity of human behavior everywhere we go. It is only appropriate to recognize that we are bringing this baggage with us into cyberspace.[1] As humans begin to clarify our relation to cyberspace it seems reasonable to extend our normative behaviors into this new realm. In so doing, we may realize a more effective defense of our social apparatus in cyberspace. Using deception and manipulation in cyberspace as we do in the physical world can afford operational benefit to all domains.

"The renunciation of false opinions [may] be a renunciation of life, a negation of life. . . untruth [I]S a condition of life" – Friedrich Nietzsche[vi]

Although deception is generally a much-maligned facet of human communication, what Nietzsche asserted in "*Beyond Good and Evil"* as a "condition of life" is essential in the context of war. What serves a multitude of purpose in everyday social context, from saving face to influencing others' behavior, serves much the same in war. Ruses, feints, and other deception have been used since man started waging war to further our aims on the battlefield and now commercial cybersecurity providers are using it as well. Study of this behavior is fairly widespread in its broader social context; in cyberspace, it has been generally lacking.

[1] Like JP 3-14 or Psychological frameworks

DOI: http://doi.org/10.5038/2378-0789.2.1.1021

According to a survey of cyberdeception literature done by the MITRE corporation in 2012, there were only a few dozen studies on deception in cyberspace at the time, and of those, few used pertinent sociological descriptors.[2] Since 2012, however, there has been an uptick in notable network deception studies. After their initial assessment of the field of study, the MITRE team pursued its research, augmenting the body of research done by the US Naval Postgraduate School. In this course of study, MITRE conducted a cyber deception game, and pursued design of a framework for planning active deception.

3. Trends in Cyberdefense

Private sector efforts have been diverging from the fingerprinting of malware and defining heuristic characteristics for over three years.[vii] Corporations have shifted from a sole focus on building alarm systems and triggers (i.e. perimeter defense) to detect intrusions – which are being bypassed, as noted above – to more broad efforts to mitigate vulnerability across the whole "cyber-kill-chain". Some, like the ***Vulnerability Rewards Program (VRP)***, are aimed at finding and fixing vulnerabilities before they are exploited. VRPs have grown exponentially since 2009, including to the DoD in March 2016. Other efforts in the sector employ deception, intended to manipulate adversary behavior, diverting attention from critical systems to non-critical systems or intentionally feed adversaries disinformation. Others, like the "***Moving Target Defense"***[viii] seek to create a rapidly changing geography for the adversary to operate in. Conceptually, deception in cyberspace has been discussed since roughly the mid-1990s, originally in the form of the "honeypot," but has increasingly morphed into more complex forms, garnering increasing attention over the last few years. In 2013, MITRE attempted creation of an integrated defensive deception platform called "Blackjack," however, testing demonstrated some difficulties with real-world use. Since 2013 more attention has been focused on the concept. The topic was presented in three major computer conferences in 2015, as it is increasingly being viewed as a tenable defensive strategy. In the private sector, deception has made a convincing business case. Cymmetria, established in 2015, is comprised of numerous military and security professionals with backgrounds ranging from a Vice President of Kaspersky, to various prior service members of the Israeli Defense Force Unit 8200, a unit analogous to the US National Security Agency. The question posed to the DoD today isn't "does this have value," but rather, "can we leverage this concept?"

4. Military deception as a framework

This linkage with state security apparatuses isn't by chance alone – deception is frequently key to victory. Military forces are regular practitioners of deception in war, because its use can prove decisive. The Achaeans (Greeks) famously used subterfuge to decisively end the siege of Troy. World War Two included a massive deception campaign, planned by Allied Forces to assist the western offensive against German forces. This linkage with military success has ensured a robust relationship through time. The DoD has codified it in Joint Publication 3-13.4 "Military Deception." Each use, changed the tempo and focus of enemy forces, allowing the deceiver to gain the initiative.

[2] This study has been the foundation of a series of studies into cyberdeception by the MITRE corporation.

Military deception "is intended to deter hostile actions, [or] increase the success of friendly defensive actions."[ix] Deception imposes cost on the adversary, cost in detecting the lie, cost in incorrect action, or cost of exposed intent. Friendly operations are valuable as they impose additional impediment to adversary operations. Deception has been used in military operations since at least the time of Homer - roughly three thousand years ago. Militaries have used ruses and other measures to both deny information to the enemy and to feed them bad information so as to disrupt their decision cycle. The Naval Postgraduate School (NPS), in its seminal study of deception, identified two major branches of deception to achieve these aims: "Ambiguity increasing" deception, or "A-type," and "Misleading" deception, or "M-Type," deception.[x]

A historic example of A-Type cited by the NPS study was Operation Fortitude North.[3] [xi] In this case the US attempted to obfuscate the intended landing site for the invasion of mainland Europe (i.e. Operation Overlord) and impose dispersal of defensive forces. This was accomplished by signaling possible invasions of Norway, Romania, and France. The means used in the deception were diverse. Duplicitous diplomatic communications[xii], fake intelligence reports[xiii], and even entire fake units like Patton's First United States Army Group, were used to signal these intentions to the German Army in preparation for Overlord.

Misleading deceptions eliminate ambiguity and are eventually aimed at forcing incorrect action. Operation Fortitude South is cited by the NPS study as an example of an M-Type. Fortitude South was aimed at convincing the Germans that Allies were landing in Calais, significantly closer to Britain. Deception efforts here prevented the effective reinforcement by fixing German forces in northern France. Joint doctrine classifies these varieties as functions of MILDEC and adds three more. In addition to sowing ambiguity and misallocation, US doctrine says that MILDEC efforts may reveal enemy information, condition the enemy to friendly behavioral patterns, and cause the enemy to waste combat power.

5. Deception in Cyberspace

Deception is not limited to military operations or exclusively to any social context; it is a natural part of human interaction. Deception is deception wherever humans go, and its results are largely analogous. In the context of war, cyberdeception has largely the same intended outcomes as in the physical world – imposing cost to adversarial decision making and affording initiative to the defender.

Deception in cyberspace has been a growing trend since the concept of the "honeypot" was described by the SANS Institute in 2000.[xiv] Generally, this ***honeypot*** is a computer specially configured to attract exploits. These are split further into categories by purpose: defense and research. Defensive honeypots aim to distract hackers from systems with value into a controllable and disposable environment. Research oriented honeypots attempt to gather information on exploits in order to facilitate study by security researchers. Recently, researchers have been seeking to fuse the two in an attempt to rapidly fingerprint malware and deploy signatures to perimeter defense – seeking to improve it by improving speed of mitigation.

[3] Operations Fortitude North was part of Operation Bodyguard, the overarching deception plan supporting Operation Overlord in World War Two.

DOI: http://doi.org/10.5038/2378-0789.2.1.1021

Although the adversary gains a foot-hold in the defenders' space, the defender is able to mitigate vulnerabilities and change strategy more quickly.

During the last decade in cyberspace, deception and information manipulation have evolved continually. Tools that were originally fairly simple and limited have kept pace with cyberspace more broadly. The simple honeypot which began in the mid-1990s has branched into many variants, each with a different shape and foci. For example, "CONPOT" attempts to clone industrial control system (ICS) environments; "Artillery" seeks to function as an early warning system, enticing attackers with open ports;[xv] "Kippo" focuses logging adversarial actions and techniques.[xvi] Each variant can impede adversarial progress or feed friendly decision making.

From this basic concept, honeypots have continued to evolve into more sophisticated variants like the ***honeynet***, wherein multiple honeypots are assembled to create a more realistic exploitable environment, and to the ***honeytoken***, which are informational tokens used to demonstrate compromise. An example of a honeytoken would be a fictional persona, only existing in a particular dataset whose purpose is to reveal compromise of the data. If someone targeted the fictional persona with a spearphishing email it would feed friendly decision making and afford opportunity for what is later described as "misleading" deception.

A key concept to implementation of honeypots is the idea of "***interaction***" with adversaries. This concept being roughly parallel with a traditional ***deception story***. To have a credible honeypot it must *look* like a real victim machine. That is to say, fidelity is key to believability. Addressing this concern is increasingly becoming key to efficacy of deception in commercial defensive efforts. In Stuart and Leanne Hirshfield's recent study for the Air Force Research Laboratory exploring the physiological responses of subjects to deception in cyberspace, they identify the concept of ***suspicion*** underlying that of interaction. They go on to propose a three-stage model of this behavior (i.e. ***cues, filters, and outcomes***) that may help guide eventual implementation of these concepts operationally.

Interaction with these machines determines their credibility. Many computers are typically configured to respond to different questions (i.e. queries). Honeypots respond in the same way. "Interaction" defines what extent a hacker may interact with a given system before seeing that it is a honeypot. Shodan, an "internet-of-things" search engine, has a tool that audits the credibility of honeypot implementations in much the same way, using queries to establish extent of interaction that a particular computer will allow.[xvii] Unfortunately this same method can be used to assist in network reconnaissance. This highlights the importance of interaction and credibility in use of honeypots.

Creation of environments with little to no credibility may also work to support the deception story. Virtual environments and virtual computers have had an interesting relationship with malware. Given past usage of virtual environments for a limited scope of specific forensic uses, malware has historically preferred not to deploy in these environments, preferring to use their "zero-day" exploits in production environments. This trend is reversing, but it still demonstrates that malware is capable of detecting low-fidelity virtualized environments.

6. Deception in the attack

Part of the challenge in the use of deception defensively, is social. These techniques have been long associated with adversarial behaviors and subsequently shunned by network operators. Adversaries have employed deception to gain access to networks, sometimes using social manipulation (i.e. "social engineering,") to establish credibility and trust. Such was the case with the 2011 compromise of RSA, a security provider whose products protected over 40 million customers[xviii] The attack was launched by targeting an internal user with a semi-credible solicitation. Once the user opened the solicitation, its malicious contents executed, enabling eventual compromise of RSAs foundational security products.[4] This does not mean that the attack was instantaneous, much like war in general: adversarial actors in a network deal with the "fog and friction" of uncertainty. Exploits like RSA may typically take months to progress as adversaries constantly adjust targets and approaches – tailoring them to their environment.

Looking across this procedural chain, you can see that it is also *vulnerable* to defensive deception. Fake personas can impede effective targeting, high fidelity exploitable machines can deliver fake or harmful data to the adversary, ***low fidelity, high value machines*** can obfuscate location of important information, and data collection of this process can help identify adversarial aim. Neil Rowe of the Naval Postgraduate School demonstrated this conceptually in his 2007 study on manipulating network reconnaissance.

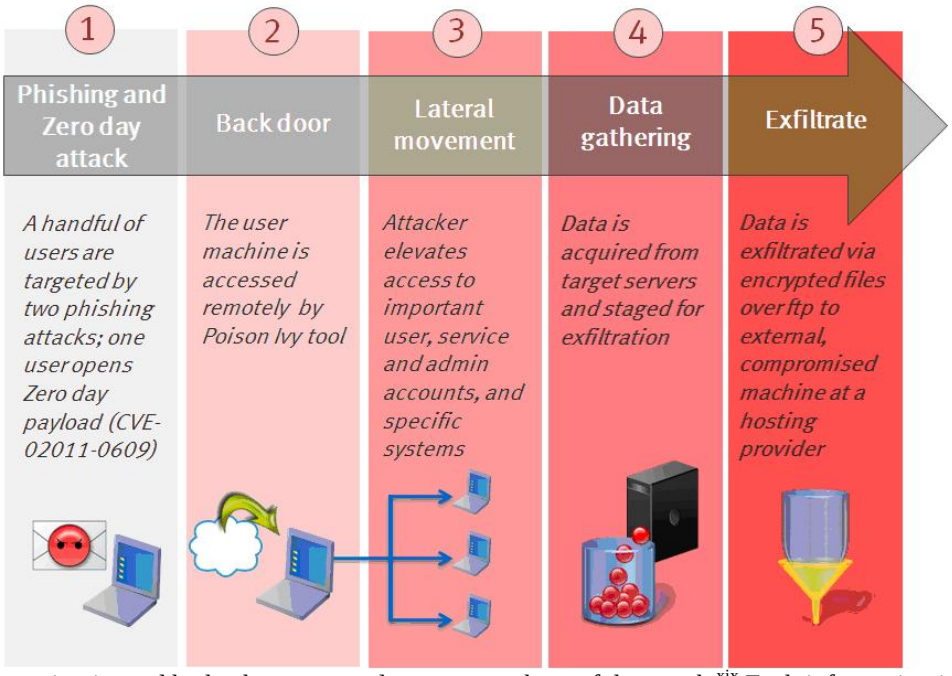

Figure 1. Deception is used by hackers across almost every phase of the attack.[xix] Each information input affords opportunity to deceive attackers.

[4] See Figure 1.

7. Deception in the defense

Malware's capacity to sense its place may be manipulated to confuse adversaries, as discussed above, with the cyber equivalent of camouflage (i.e. making valuable targets look less important and more generic). Using the framework of military deception, there are several tactics and techniques that may be employed in pursuit of defensive capability. Generally, they fall within the framework of military deception outlined above – working either toward ambiguity increasing (A-Type) or misleading (M-Type). However, use of A-type defensive deception may be the most viable in the short term.

MITRE recently examined the implications of using M-Type deception in a paper titled "Denial and Deception in Cyber Defense." Several salient points emerged. The first was that although misleading type deception can be more effective than ambiguity increasing deception, the institutional cost can be greater as well. In its paper, MITRE posits an eight-step deception process that seeks to create a functional M-Type deception.[5] This process is reliant on a "management model"[xx] not typically present in cyber operations. This is not to say that it cannot be created, or would be ineffective – on the contrary, it would be highly effective[6] – but creation of such a mechanism comes a price. In the interim, it may be easier to pursue ambiguity inducing deception. A-Type may still be used to sow ambiguity and imposer a steeper cost than is currently the case for advanced persistent threats (APTs). As explained above, effective conduct of action in cyberspace is difficult enough for an adversary at the moment. Attackers must spend considerable time conducting reconnaissance and figuring out what is *worth attacking* in the network and what their objective will be.

Tactics available in Cyberdeception

	Moving Target Defense	Low Fidelity, High Value Systems	Honeypots	Honeynets	Honeytokens
Type	Ambiguity	Ambiguity	Ambiguity, Misleading	Ambiguity, Misleading	Ambiguity, Misleading
Effect A - Type	A - Increases required reconnaissance period, disrupt previous access	A - Requires greater scrutiny to determine legitimacy (better performance if concurrent with M-Type Efforts)	A - Denial of attack vector (partial*)	A - Denial of attack vector (partial*)	Cueing
Effect M - Type	N/A	N/A	M - Active contributions to deception story	M - Active contributions to deception story	Cueing

* Depends on adversarial movement through network and detection

[5] 1. Define purpose, 2. Seek understanding of adversary, 3. Design cover story, 4. Plan friendly deception, 5. Prepare, 6. Execute, 7. Monitor, and 8. Reinforce deception as needed.

[6] By virtue of using the deception process above M-type deception adheres to doctrinal Principals of Military Deception – i.e. Focus, Objective, Centralized Planning and Control, Security, Timeliness, and Integration

A-type deceptions offer numerous benefits to defenders with a minimal institutional cost. They may be planned into acquisition efforts and deployed through normal operation channels. A-Type deception seems to be "low hanging fruit." It has a broad ***deception target*** because it aims to frustrate the adversarial operators, not planners. It doesn't require the same level of coordination for the ***deception story*** since the story only aims to complicate the environment. Moreover, the A-Type, once more developed, would offer the defender the greatest agility in response.

In the near term, cyberdeception will be limited principally to ***displays*** and ***demonstrations*** – that is to say, sowing ambiguity. ***Ruses*** and ***feints,*** however, will remain relatively unused at least for now.[7]With careful thought, resourcing, and ample planning, like that done by MITRE in their recent study, M-type deception may become feasible. It is important to realize these ***tactics*** may not remain relevant in the future. Incorporating deception into our strategy and doctrine, however, is merely embracing cyberspace as a human domain.

Deception imposes cost on the adversary: cost in detecting the lie, cost in incorrect action, or cost of exposed intent. These effects translate well into cyberspace. Cyberdeception tactics should not be viewed as static solutions to a problem but rather part of an exchange with attackers. As is true in conventional conflict, tactics, techniques, and procedures change rapidly. Doctrine and strategy change much more slowly and this is where deception must be built. Employment of deception in cyberdefense as a doctrinal change will, as with human behavior, remain pertinent well into the future.

8. Challenges

As discussed above, credibility remains a key challenge to establishing a viable defensive deception campaign. If honeypots look like honeypots, no one will engage with them. Likewise, no one will want to interact on a virtualized defense platform if they realize they are in it. That being said, what other challenges might an organization face? Defining a *valid* target may be one, and where should we conduct this effort? How do we delineate target audiences for military deception? The question is one of ***distinction***, and can be answered in observation of intent within the confines of organizational cyberspace. Cyber personas are by nature, ambiguous. Early internet culture valued anonymity above all else, and this proclivity has resulted in a social construct that blurs the link to the real world. Unauthorized access to US networks may afford the distinction required to delineate validity as a deception target, but this question will remain pertinent.

Conclusion

Within the departments and supporting agencies (i.e. the Services and the DoD) we have the resources to create a fairly robust deceptive effort. USSTRATCOM, the parent of both JFHQ-DoDIN and USCYBERCOM, already has authority to conduct transregional MILDEC. Core Data Centers capable of virtualizing servers and handling large volumes of traffic, national cyber ranges that simulate operational terrain of the DoDIN, and a nascent national cyber mission force

[7] Honeytokens *may* be categorized as a ruse, as it cues friendly forces to adversarial intent.

DOI: http://doi.org/10.5038/2378-0789.2.1.1021

– including "Cyber Protection Teams". All of these resources can be leveraged to provide a capable infrastructure that enables both active and passive deception. By leveraging our own networks in support of military deception, we may impose new costs and shape adversary action. Given the operationalization of M-Type deception in cyberdefense, stolen technologies could become liabilities and false situational templates could be laid, all of which complicate adversary decision calculus. Today, these options seem to be at our fingertips. In cyber operations, the only thing needed is doctrinal shift - a more mature understanding of the operational environment. We assume we can "dominate" our own networks. We cannot. We need a pragmatic doctrine that operates in today's context. We will need deception if we are to fight for key cyber terrain.

Why then, should we not adapt current war-fighting doctrine for cyber operations? We know that foreign actors access our networks and the information stored therein. We know that our perimeter defenses and sensors will be useless against state cyberforces in a war. The same pattern of exploitation has been happening in networks now for over 10 years – expecting perimeter security to improve will not make it so. Deception offers an additive defense.

The case for employment of "A-Type" Deception in the network has been mounting for several years. A confluence of factors is now creating an imperative for the development and employment of this capability in the joint environment. The diminished efficacy of current defensive capability combined with a relatively unambiguous operational environment has created the perfect domain for the adversary in US cyberspace. If the USG does not deploy this capability, it *will* be caught flat footed in our next major conflict.

---

[i] Kristen Heckman, Frank Stetch, Ben Schmoker, Roshan Thomas, "Denial and Deception in Cyberspace", *Computer* Vol 48, Issue 4, 2015, 36.

[ii] "Joint Information Environment (JIE) Operations Concept of Operations" JIE Operations Sponsor Group, Department of Defense, September 18, 2014.

[iii] MITRE, "Denial and Deception in Cyberspace", 36.

[iv] 2016 Threat Report, Webroot, https://www.webroot.com/shared/pdf/Webroot_2015_Threat_Brief.pdf, retrieved March 3, 2016.

[v] LTG Dennis Via, comments at AFCEA Technet 2010, http://c4i.gmu.edu/eventsInfo/reviews/2010/slides/VIA-AFCEA_GMU_Brief_FINAL.pdf

[vi] Friedrich Nietzsche, Beyond Good and Evil, (Project Gutenberg, 2003) https://www.gutenberg.org/files/4363/4363-h/4363-h.htm retrieved 17 Mar 2016

[vii] 2013 Chief Information Security Officer Report, FireEye Security, Retrieved Mar 2016.

[viii] Rui Zhang, Su Zhang, Alex Bardas, Scott DeLoach, Ximing Ou, Anoop Singal "Investigating the Application of Moving Target Defense to Network Security" IEEE 6th International Symposium on Resilient Control Systems, 2013 1.

[ix] Joint Publication 3-13.4 - Military Deception. Department of Defense, http://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf , 2. Retrieved 10 January 216

[x] Doanld Daniel, Katherine Herbig, William Reese, Richards Heuer, Theodore Sarbin, Paul Moose, Ronald Sherwin, "Multidisciplinary Perspectives on Military Deception." Naval Postgraduate School, Monterrey, CA 1980.

[xi] Michael Donovan, "Strategic Deception: Operation Fortitude" US Army War College, 2002 3. http://www.dtic.mil/get-tr-doc/pdf?AD=ADA404434 Retrieved 17 January 2016.

[xii] Michael Donovan, "Strategic Deception: Operation Fortitude" US Army War College, 2002 8.

[xiii] Federal Bureau of Investigation, Operation Bodyguard: FBI Recognizes WWII Counterintelligence Landmark in New York, https://www.fbi.gov/news/stories/2014/june/operation-bodyguard/operation-bodyguard, retrieved 2 Feb, 2016

[xiv] Loras Even, Honey Pot Systems Explained, https://www.sans.org/security-resources/idfaq/what-is-a-honeypot/1/9, retrieved 4 Feb 2016.
[xv] TrustedSec, Project Artillery, https://www.trustedsec.com/artillery/, retrieved 4 Feb 2016.
[xvi] Kippo - SSH Honeypot, https://github.com/desaster/kippo, retrieved 4 Feb 2016
[xvii] Shodan, "Honeypot Or Not?" https://honeyscore.shodan.io/ retrieved 10 February 2016.
[xviii] Riva Richmond, "The RSA Hack: How They Did It," http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/?_r=0, retrieved 8 Feb, 2016.
[xix] RSA FraudAction Research Labs, "Anatomy of an Attack", https://blogs.rsa.com/wp-content/uploads/2014/08/APT-chart1.jpg retrieved 8 Feb 2016
[xx] MITRE, "Denial and Deception in Cyberspace", 38.

DOI: http://doi.org/10.5038/2378-0789.2.1.1021