Improving Cybersecurity Through Human Systems Integration

John Zager and Robert Zager

Abstract

Advanced Persistent Threat (APT) attackers accomplish their attack objectives by co-opting users' credentials. Traditional cyber defenses leave users vulnerable to APT attacks which employ spearphishing. The success of spearphishing attacks is not a data processing failure, but is the result of defenders failing to apply the principles of Human System Integration to the problem of spearphishing. We discuss an alternative defensive strategy which addresses human performance capabilities and limitations to disrupt spearphishing attacks.

Keywords: Human Systems Integration, HSI, negligent users, cyberspace operations, information operations, military deception, habit, cognitive dimension, phishing, spearphishing, APT, computer network defense, usability, Compliance Budget

Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation.

-2010 National Security Strategy

On 26 October 2015, Admiral Michael Rogers, Director of the National Security Agency, in an interview with the Wall Street Journal observed: [1]

> It is only a matter of when before someone uses cyber as a tool to do damage to critical infrastructure within our nation. I'm watching nation states, groups within some of that infrastructure. At the moment they seem to be focused on reconnaissance, but it's only a matter of time until someone actually does something destructive.
>
> The second trend that concerns me, historically to date we've largely been focused on the extraction of data and insights, whether it be for intellectual property for commercial or criminal advantage. But what happens when suddenly our data is manipulated, and you no longer can believe what you're physically seeing?
>
> And the third phenomenon when I think about threats that concern me is what happens when the nonstate actor, take ISIL for example, whose vision of the world is diametrically opposed to ours, starts viewing the Web not just as a vehicle to generate revenue, to recruit, to spread the ideology, but as a weapons system.

The most common means of compromising systems is the Advanced Persistent Threat employing highly targeted deceptive emails ("spearphishing") to trick the email recipient into compromising credentials. Commenting on the spearphishing problem, Jeh Johnson, Secretary of Homeland Security, observed: [2]

> What amazes me when I look into a lot of intrusions, including some really big ones by multiple different types of actors, it often starts with the most basic active spearphishing where somebody is allowed in the gate and penetrates a network simply because an employee clicked on something he or she shouldn't have. And the most sophisticated actors count on penetrating a system in that way, which means that a lot of our cybersecurity efforts have to be rooted simply in education of whatever workforce we have.

The problem of authorized users being tricked into unintentionally granting system access to attackers is termed the "Unintentional Insider Threat."[3] After the malicious actor has become an unintended system insider, defenders are left with the challenge of discovering the threat, stopping the undesired activities and remediating the damage. Because the defenders and the attackers use the same tools, systems and defenses, the unintentional insider has significant understanding of defensive strategies.[4] This knowledge can be used to compromise systems for long periods of time – even years. The damage that can be done by an attacker may not be repairable. How does one repair the theft of the C-17, F-22 and F-35?[5] Obviously a credit monitoring service will not restore the status quo ante for millions of U.S. government employees whose personnel records – including their fingerprints – were stolen in the Office of Personnel Management breach.[6]

In Section 1 of this paper we discuss traditional defenses. In Section 2 we focus on the user's role in the APT attack. In section 3 we discuss spearphishing as an information operation. Section 4 focuses on the cognitive dimension of the information operation. Section 5 discusses spearphishing as military deception. Section 6 concludes with a discussion of how human factors can be used to make users less susceptible to APT attacks.

Section 1. Traditional Defenses

… cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines.

-Dr. Frederick Chang, Former NSA Director of Research[7]

Traditional defenses use a layered security approach, combining numerous defenses including firewalls, intrusion detection, intrusion prevention, filters, anti-virus, encryption, and event logging/analysis. Because system defense is well-understood by attackers, the attackers and defenders are forced into a continuing process of modifying their behavior in response to the actions of the adversary. Attackers and defenders are locked in a continuing cycle of measure-countermeasure.[8] In this on-going cycle, attackers have perfected a highly effective attack methodology - spearphishing. Spearphishing attacks consistently reach their objectives by exploiting users. The user exploitation is created by email technology which enables attackers to communicate directly with authorized users. Email is a standards based system which uses well-known rules to enable honest email senders to deliver email.[9] Gaming the email system provides a reliable attack vector for sophisticated attackers who cleverly manipulate attacks employing the tools of email marketing to deliver email to targeted users. When a spearphishing attack reaches its objectives, defenders are left to engage in retrospective analysis, mitigation and remediation.[10]

The need to deliver legitimate email provides the opening that APT attackers use to defeat traditional defenses.

Section 2. Foundation for the APT Attack Methodology

If the enemy leaves a door open, you must rush in.

- Sun Tsu, *The Art of War*

Users control the data and data processing systems are merely the place where users create, use and store data. For example Joint Publication 6-0, *Joint Communications Systems,* states:[11]

> The first element of a C2 [command and control] system is **people**—people who acquire information, make decisions, take action, communicate, and collaborate with one another to accomplish a common goal. Human beings—from the senior commander framing a strategic concept to the most junior Service member at the tactical level calling in a situation report—are integral components of the joint communications system and not merely users. The second element of the C2 system is comprised of the **facilities, equipment, communications, staff functions, and procedures** essential to a commander

> to plan, direct, monitor, and control operations of assigned forces pursuant to the missions assigned. Although families of hardware are often referred to as systems, the C2 system is more than simply equipment. High-quality equipment and advanced technology do not guarantee adequate communications or effective C2. Both start with well-trained and qualified people supported by an effective guiding philosophy and procedures. [Emphasis in the original]

The preeminent role of people is explained in Joint Publication 3-13, *Information Operations*. JP 3-13 observes that the information environment is made up of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment is comprised of three interrelated dimensions which continuously interact with individuals, organizations, and systems. These three dimensions, the physical[12], informational[13], and cognitive, are illustrated in this figure from JP 3-13:[14]

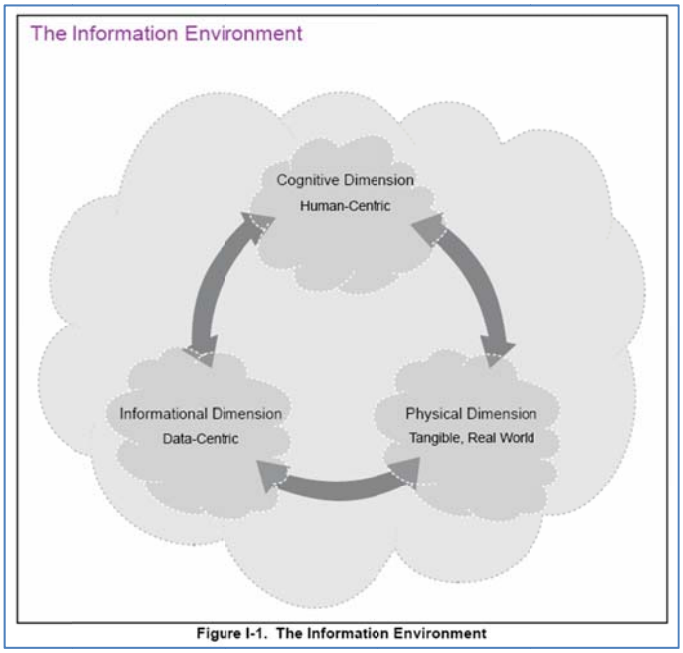


Figure I-1. The Information Environment

Illustration 1

"The cognitive dimension encompasses the minds of the people who transmit, receive, and respond to or act on information. It refers to individuals' or groups' information processing, perception, judgment, and decision making."[15] Human decision-making is not a computer process; it is an incredibly complex process of human psychology.[16] Factors influencing decisions include the environment in which the decisions are being made and incorporate individual and cultural beliefs, norms, vulnerabilities, habits, motivations, emotions, experiences, morals, education, mental health, identities and ideologies. Decisions can be rational or irrational, conscious or unconscious. Understanding these factors creates opportunities to influence the decision-making to create the desired effects. "As such, **[the cognitive] dimension constitutes the most important component of the information environment**. [emphasis added]"[17]

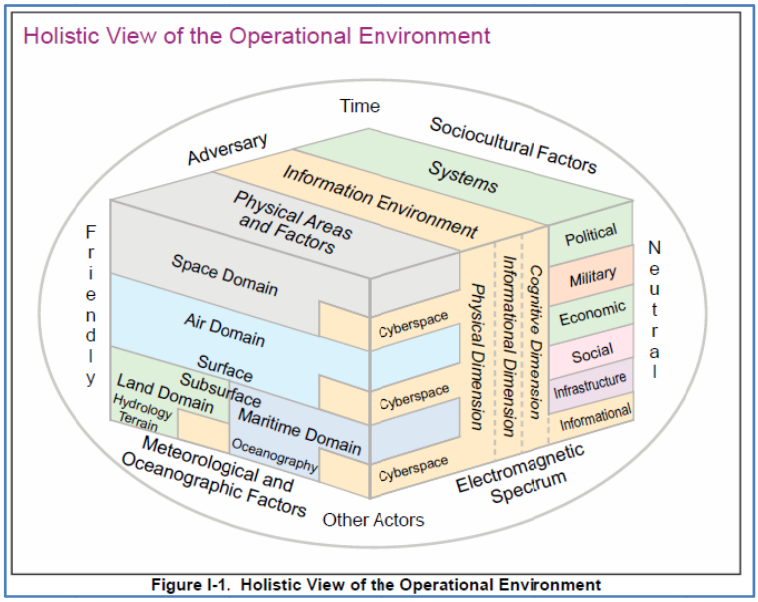


Figure I-1. Holistic View of the Operational Environment

Illustration 2

Joint Publication 2-01.3, *Joint Intelligence Preparation of the Operational Environment,* consolidates all aspects of the operational environment into a single holistic view of the operational environment.[18] Illustration 2 highlights the pivotal role of the information environment, particularly the Cognitive Dimension, in the global adversarial engagement. Controlling the cognitive dimension cascades throughout the operational environment. Illustration 2 also shows how cyberspace is an element of Information Operations. Cyberspace is both independent from and dependent upon the other four global

domains (air, land, maritime and space).[19] Cyberspace operations communicate information to and from the other global domains. At the same time, cyberspace is dependent upon the other four global domains to support cyberspace's physical systems.

Joint Publication 3-12, *Cyberspace Operations,* explains the relationship between cyberspace operations (CO) and information operations (IO) and, in doing so, sets forth the foundation for the APT attack methodology:[20]

> CO are concerned with using cyberspace capabilities to create effects which support operations across the physical domains and cyberspace. IO is more specifically concerned with the integrated employment of information-related capabilities during military operations, in concert with other lines of operation (LOOs), to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own. Thus, cyberspace is a medium through which some information-related capabilities, such as military information support operations (MISO) or military deception (MILDEC), may be employed. However, IO also uses capabilities from the physical domains to accomplish its objectives.

An APT is an information operation which uses cyberspace to influence decision making to create the effects desired by the APT attackers across the physical domains and cyberspace.

Section 3. The APT Information Operation

[Y]ou can have the greatest technology and greatest defensive structure in the world, but in the end, never underestimate the impact of user behavior on defensive strategy.

-Adm. Michael Rogers, NSA Director[21]

The purpose of an information operation is to influence the behavior of the target audience. JP 3-13 states: [22]

> IO integrates IRCs (ways) with other lines of operation and lines of effort (means) to create a desired effect on an adversary or potential adversary to achieve an objective (ends).

Spearphishing is classic information operation; spearphishing is an information operation that integrates the information related capability (IRC) Military Deception (way) with email (means) to influence authorized users to act for the benefit of the adversary (ends).

The recent theft of tens of millions of dollars from Ubiquiti Networks is a simple, yet highly effective, example of a spearphishing information operation. [23] Ubiquiti is one of the many victims of the Man-in-the-Email method which has netted attackers almost $215M between 01 October 2013 and 01 December 2014.[24] In this type of cyberattack, the attacker sends an email impersonating an employee or vendor which email contains fraudulent payment instructions. The recipient of the email sends money according to the fraudulent instructions. This spearphishing

attack is an example of the general structure of the spearphishing information operation because it:

- integrated Military Deception {impersonation deception story} (way)
- with email (means)
- to influence authorized users to act for the benefit of the attacker {making payments} (ends).

The Man-in-the-Email attacker effectively influences the victim's payment processing systems without ever directly accessing these systems, instead controlling a user who then misuses authorized system access to accomplish the attacker's objectives. The information operation is successful because the attacker controls the user who controls the data. By controlling the cognitive dimension, the attacker obtained its desired effects.

Another example of how a spearphishing attack is an information operation is the commodity Dridex attack. In the Dridex attack, the user is presented with an email from an apparently known sender with an attachment such that shown in Illustration 3.[25]

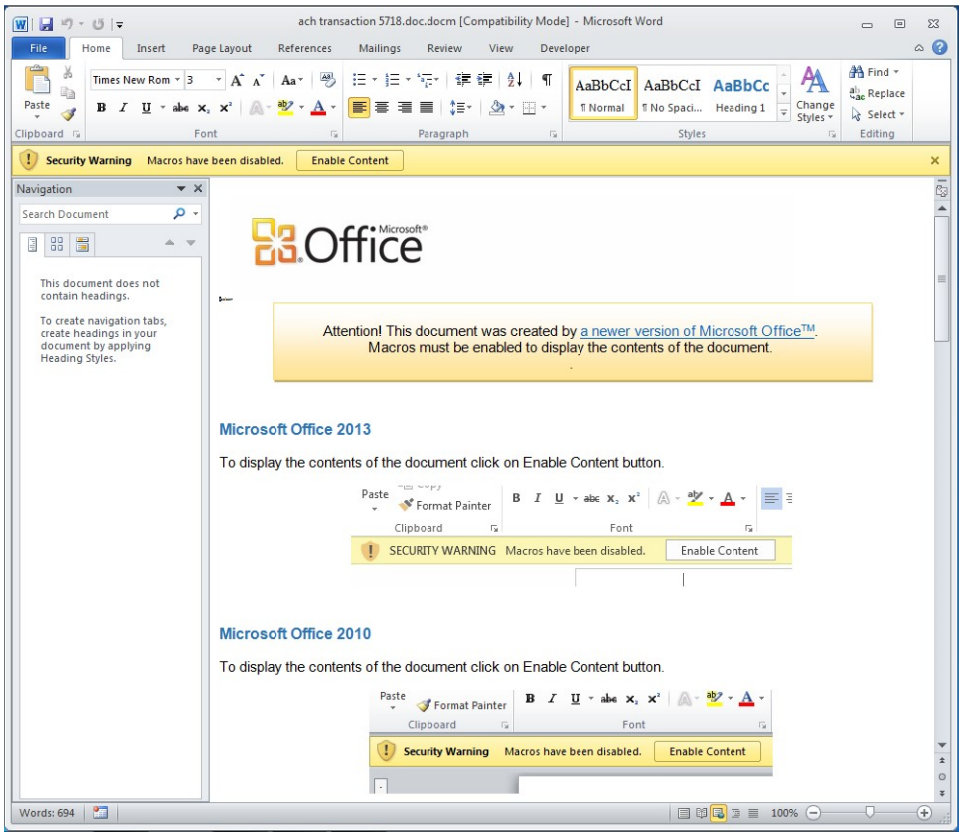


Illustration 3

Three distinct user interactions are required to activate the attack code which provides command and control to the attacker:

1. Open the email
2. Open the attachment
3. Enable the Content

The required user interactions are obtained by deception. Note how the adversary applied military deception to convert a system warning into a call to action. Because the Dridex attack leverages user interactions to infiltrate and evade detection, the commodity Dridex attack defeats technical defenses 99.97% of the time. The Dyre variant defeats technical defenses 99.98% of the time. The detection rate for targeted attacks is unknown.[26] The Dridex spearphishing attack is another example of the general structure of the spearphishing information operation because it:

- integrated Military Deception {impersonation deception story and content deception story} (way)
- with email (means)
- to influence authorized users to act for the benefit of the attacker {opening the email, opening the attachment, enabling the content} (ends).

In spearphishing the attacker uses military deception to influence the user thereby exploiting the authorized user's own system privileges to evade detection and accomplish the attacker's objectives.

Section 4. The Spearphishing Cognitive Environment

Defining [the] influencing factors in a given environment is critical for understanding how to best influence the mind of the decision maker and create the desired effects.

-Joint Publication 3-13, *Information Operations*

FISMA mandates that federal employees receive security awareness training.[27] In 2010 the Defense Science Board recommended that employees who fall for spearphishing should be reprimanded and be subject to dismissal.[28] On 17 September 2015, Paul Beckman, Department of Homeland Security CISO, said, "Someone who fails every single phishing campaign in the world should not be holding a [Top Secret Security Clearance] with the federal government. You have clearly demonstrated that you are not responsible enough to responsibly handle that information."[29] In a Wall Street Journal interview on 26 October 2015, Adm. Michael Rogers, NSA Director, took it one step further and said that court-martial was appropriate for people who fall for spearphishing.[30]

Paul Beckman's 17 September 2015 comments summarize the spearphishing problem:[31]

> [Mr. Beckman] sends his own emails designed to mimic phishing attempts to staff members to see who falls for the scam. "These are emails that look blatantly to be coming from outside of DHS -- to any security practitioner, they're blatant," he said during a panel discussion on CISO priorities … "But to these general users" -- including senior managers and other VIPs -- "you'd be surprised at how often I catch these guys."
>
> Employees who fail the test -- by clicking on potentially unsafe links and inputting usernames and passwords -- are forced to undergo mandatory online security training.

Mr. Beckman's comments make three assumptions about the information operation target audience:

1. Spearphishing emails are blatant, thus easy to distinguish from real email.
2. Security practitioners, having subject matter expertise, are able to identify spearphishing emails in operational settings.
3. Training will provide users with sufficient subject matter expertise to operate at the proficiency of security practitioners.

Regrettably, all three of these assumptions are invalid. In fact:

1. Spearphishing emails are not blatant. Col. Greg Conti, Director of the Information Technology Operations Center at the U.S. Military Academy observed, "What's 'wrong' with these e-mails is very, very subtle. They'll come in error-free, often using the appropriate jargon or acronyms for a given office or organization."[32]
2. Spearphishing subject matter expertise has a limited effect on spearphishing defensive behaviors in operational environments.[33]
3. Spearphishing training of the general user population is ineffective in improving defensive behaviors.[34]

Awareness training, although satisfying FISMA compliance, does not achieve improved security.

Why do people fall for spearphishing attacks? In order to answer this question, an information operation analysis is required. JP 3-13 instructs,[35]

> **Defining [the] influencing factors in a given environment is critical for understanding how to best influence the mind of the decision maker and create the desired effects.**

The decision maker in a spearphishing attack is the email user. The environment of this decision maker is his email display in the context of performing job duties. In spearphishing attacks, the choices made by users, not defects in technology, cause security compromises. Users are choosing to interact with the malicious emails. Users make these security choices in the context of their jobs, a context in which they seek to optimize employment performance, not security. This creates a conflict of interest in which the users focus on completing their primary (production) tasks and the requirements of security (enabling) tasks can present impediments to achieving the primary tasks. There is a limit to how much effort users will put into non-productive security tasks, which Beautement, Sasse, and Wonham named the Compliance Budget. [36] They summarize the Compliance Budget:

> The decision to comply or not comply can be addressed by the following simple formula:
> Task cost = individual benefits – individual costs.
> Compliance if task cost < compliance threshold.

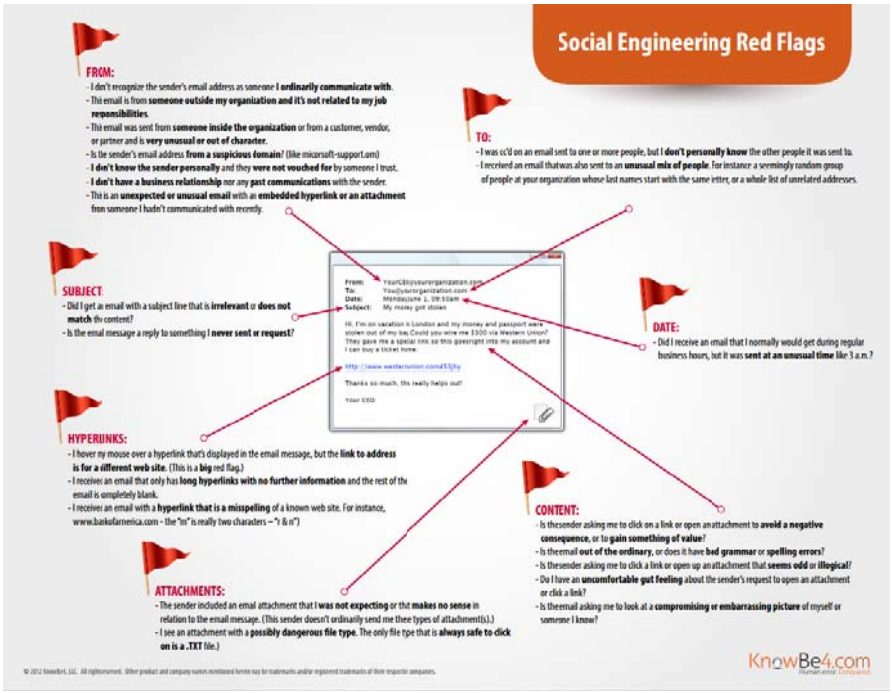
Four elements drive the user's costs of email processing. These are:

1. The Hassle Factor
2. The Availability of Information
3. The Ability to Process Information
4. Perceived Risk

The Hassle Factor. Beautement, Sasse, and Wonham observe that this user cost calculation is not based on a single interaction, but is made using the cumulative perceived costs of the compliance tasks, termed the "hassle factor." The hassle factor recognizes that the perceived cost of a task increases with repetition. Thus,[37]

> If the task in question is the tenth that day, the individual has been expected to undertake it will be seen as a far greater burden than the exact same task earlier in the day. This means that a steady erosion of the Compliance Budget will take place as tasks stack up, and the individual's tolerance for further tasks (or repetitions of the same task) will be reduced.

In every spearphishing email there is a divergence between the actual sender and the perceived sender, a divergence which we term the Spearphishing Incongruity. Illustration 4 outlines an excellent set of rules, in this case published by KnowBe4, a leading spearphishing training company:[38] By deconstructing every email using these twenty-two things to remember and applying these rules against a list of trusted URLs and file extensions, a user has a methodology to discover the Spearphishing Incongruity, thereby substantially reducing the likelihood of being deceived by a socially engineered email. These rules are effective in detecting a single stage spearphishing attack, thereby preventing a multistage attack.[39] The point of Illustration 4 is not to detail the 22 "Red Flags", but to suggest that the hassle factor of applying these 22 factors every time a user interacts with an email imposes a high compliance cost in the Compliance Budget calculation.



Source: KnowBe4
Illustration 4

The Availability of Information. In order to determine if an email is valid, the user must have the technical skills and information required to perform the analysis.

How do users determine what domain names are trustworthy? There is no directory of trusted domains. Users do not know all of the legitimate domains with which they interact, making users susceptible to deception by clever ruses.[40] Determining if a domain is trustworthy is a non-obvious task. Would anyone correctly guess that the real email address of a Silicon Valley Member of Congress uses the "address-verify.com" domain or that irs.gov is NOT the domain the IRS uses for email?[41] The general problem of knowing who stands behind a domain can be seen in the current presidential campaign season. The National Republican Congressional Committee set up domains that trick Democrats into opposing Democratic

candidates.[42] Supporters and opponents of Hillary Clinton have set up numerous Clinton look-alike domains.[43]

The difficulty of distinguishing good senders from bad senders was recently illustrated in the fallout from the Office of Personnel Management (OPM) compromise. After the breach, the OPM hired a contractor to provide identity theft benefits to impacted federal employees. The Information Assurance experts at Fort Meade, home of the NSA, incorrectly identified emails from OPM's contractors as a spearphishing attack and issued warnings to base personnel.[44] Rather than enhancing cybersecurity, this warning interfered with employees enrolling in the protection of their identities.

The Ability to Process Information. Assuming users are aware of which domains are trustworthy, many additional factors come into play. First, most people cannot decode URLs.[45]

Second, constant exposure to information does not imbue people with accurate memories of the information. In a study of people's ability to recall the Apple logo, an image that is reinforced almost constantly, people expressed great confidence in their ability to recall the logo, despite the fact that most people incorrectly recalled the logo.[46] The researchers concluded:

> Increased exposure increases familiarity and confidence, but does not reliably affect memory. Despite frequent exposure to a simple and visually pleasing logo, attention and memory are not always tuned to remembering what we may think is memorable.

Additionally, behavioral research has demonstrated that the number of mental steps required to reach a solution reduces the likelihood of success.[47] It is reasonable to assume that with the volume of email people receive, less time is spent on each individual email assessing individual risk. The current research supports the idea that the less time that is allocated to a response, the less likely a correct answer is chosen.[48] So any "solution" which creates more decision making steps is more likely to increase opportunity for error both by creating more opportunity for mistake and by shortening the timeframe for each individual decision.

Significant mental resources are required to process domain information.

Perceived Risk. Layered defenses do a very good job of protecting users from bad emails. For example, Proofpoint claims that it blocks 99.9% of bad messages.[49] In their on-going interactions with their inbox, users experience little risk. Instead, users experience a safe email experience. When an automated system has proven to be reliable, users tend to trust the automated system over their own judgment. Because of trust reposed in reliable automation systems, users fail to detect failures of reliable systems.[50] In the context of email, users presume that email in the inbox is trustworthy because delivered emails passed the safety tests of the email processing system.

Persistence of exposure to risk information also has an impact on individual perception of how "real" the risk really is. Researchers examining how frequent repetition and reminders of risk affect the perception of the risk found that there is an inverted U-shaped pattern of risk perception. This means that there is a certain threshold of risk exposure, and once that

threshold is reached more exposure to the risk information actually reduces the perception of that threat as an actual threat.[51]

When the hassle factor, the availability of information, the ability to process information and perceived risk are factored into the Compliance Budget, it becomes obvious that users are unlikely to proficiently and consistently engage in complex tasks when processing email. In fact, Vishwanath, et al. have established that users manage their Compliance Budget by applying a simple triad of perceived relevance, urgency clues and habit to process email.[52] These three factors are easily manipulated by spearphishers applying the principles of military deception.

Although the finding that email processing is habitual seems almost obvious upon reflection of one's own email processing practices, the significance of this finding cannot be overstated. Habit is a powerful force in the cognitive dimension that is hard-wired in the brain. Habit reduces cognitive load, driving rapid decision-making at the expense of deep reflection.[53]

Section 5. Spearphishing as Military Deception

deception story. *A scenario that outlines the friendly actions that will be portrayed to cause the deception target to adopt the desired perception.*

-Joint Publication 3-13.4, *Military Deception*

The purpose of military deception in an information operation is to influence the target to act according to the desires of the entity conducting the information operation. This diagram from Joint Publication 3-13.4, *Military Deception,* summarizes the three-tiered cognitive process of deception which culminates in the target audience taking the desired action:[54]

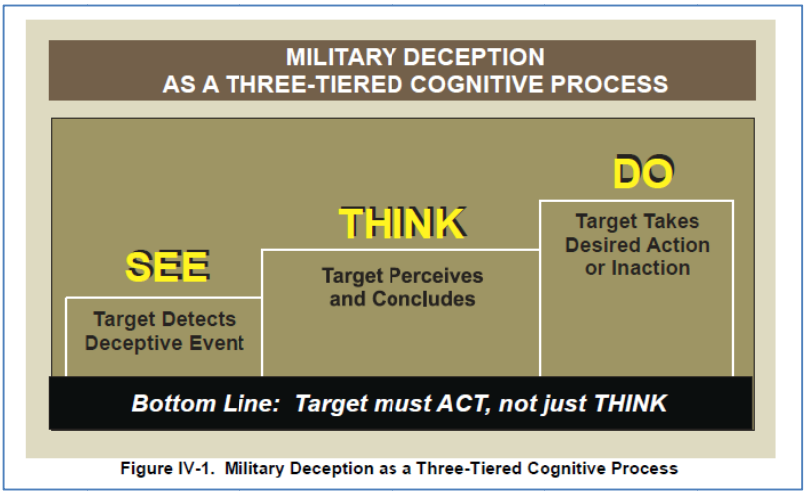


Figure IV-1. Military Deception as a Three-Tiered Cognitive Process

Illustration 5

The three-tiered cognitive process is demonstrated by this spearphishing email, Illustration 6,

that compromised the Israeli security forces:[55]



Illustration 6

The target audience (an Israeli police officer) saw an email from Lt. Gen. Benny Gantz, trusted head of Israeli defense forces, delivering a report about enemy rocket attacks ***(See)***. The police officer drew the conclusion that he should open the attachment ***(Think)*** and took the action of opening the attachment ***(Do)***. The consistent constellation of content comprising the perceived trusted sender, the text and the call to action caused the target audience to conclude this email was real, despite the fact that the purported sender, an Israeli general, probably does not send critical security email to police from a Gmail account.[56]

Because the email interaction is a habitual behavior, the spearphishing military deception process is a variation of the classic See-Think-Do process. Habits are invoked through a See-Respond-Reward process.[57] Thus, when the adversary seeks to elicit a habitual response, the adversary needs to use the cues that will trigger the desired habitual response. These cues are perceived relevance and urgency.[58]

The crucial element in the spearphishing attack is military deception based on tricking the target audience, the email recipient, into believing that the attacker is a trusted email sender. In every case, the attackers are trying to appear to be someone they are not. The attacker can masquerade as anyone that the attacker concludes is trusted by the target audience – be that a co-worker, the IRS, FedEx, a bank, or any other sender. That trust is stolen by manipulating the triad of perceived relevance, urgency clues and habit. The trust relationship is perceived by the human target audience in the cognitive dimension, not by computers.[59]

In a spearphishing attack, the adversary leverages the habitual nature of email processing to drive the MILDEC process. In response, the defenders anticipate a well-trained and vigilant end-user who will apply a Red Flag analysis to every incoming email. This engagement can be summarized by extending the model of layered defenses model set forth the Lockheed Martin's

Intelligence-Driven Computer Network Defense[60] with the addition of a column "Info Op", Illustration 7.

Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy	Info Op
Reconnaissance	Web analytics	Firewall ACL					Intelligence
Weaponization	NIDS	NIPS					ZDE, Web, Custom
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing			Email Victim
Exploitation	HIDS	Patch	DEP				Deceive User Into Action
Installation	HIDS	"chroot" jail	AV				Unintentional Malicious User
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect		Abuse Credentials
Actions on Objectives	Audit log			Quality of Service	Honeypot		Anti-Forensics

Source: Lockheed Martin [61]
Illustration 7

By using an authorized user as an unwitting agent, the spearphishing attacker is able to bypass defenses and exploit privileges that reside with the user. The Dridex attack (Illustration 3, above) demonstrates how a clever attacker can trick the user into taking a series of carefully orchestrated actions, thereby abusing user credentials to overcome defenses. Having applied the power of deception through an information operation, the spearphishing attacker becomes a malicious internal user. As Edward Snowden and Bradley Manning demonstrated, finding a malicious internal user can be quite difficult. As was disclosed in the SEC's investigation of a $100 million security fraud that operated for five years, attackers rely on the fact that they can penetrate systems at will to maintain a long term presence despite defensive remediation efforts.[62] The Criminal Complaint against Su Bin, the Chinese spy who stole secret information about the C-17, F-22 and F-35, illustrates the use of repeated infiltrations and anti-forensics to accomplish a long term presence in the targeted systems.[63]

Illustration 7 provides a perspective of spearphishing that goes beyond data processing to include the realities of the human element of the system. This broader view of the system shows the need to apply a Human Systems Integration (HSI) analysis to the spearphishing problem.[64] Human Factors (HF) is the HSI discipline that is applicable to the exploitation of cognitive vulnerabilities in a spearphishing attack.

> The discipline of Human Factors (HF) is devoted to the study, analysis, design, and evaluation of human-system interfaces and human organizations, with an emphasis on human capabilities and limitations as they impact system operation…HF focuses on those aspects where people interface with the system. NASA, Systems Engineering Handbook, NASA/SP-2007-6015, Rev1, page 246.

HF employs four tools to improve human performance, reduce errors and improve system tolerance to errors.[65] These tools are:

1. personnel selection,
2. system, interface, and task design;
3. training; and
4. procedure improvement.

Spearphishing defenses currently emphasize personnel selection (in this case de-selection) and training while ignoring system, interface and task design; and procedure improvement. The failure to recognize the cognitive limitations of email users, particularly the habitual nature of email processing, is a fundamental breakdown of HF engineering.

Choosing to substitute a series of assumptions about human cognition in place of human performance research has resulted in a system that is highly vulnerable to attacks against human cognitive processes. In the measures-countermeasures cybersecurity engagement, attackers have focused their attacks on HF while defenders have not. Because the attackers leverage the capacities and performance limitations of the human targets and defenders do not, it is clear that email is a system which favors the attackers, not the defenders.

How will the training reinforced with loss of security clearances, dismissal and court-martial change the HSI analysis of spearphishing? Training and punishment will not improve the HSI limitations of email.[66] Training and punishment will not correct the limitations of the human cognitive process.[67] Training and punishment will change the Compliance Budget calculation as users see careers cut short by spearphishing emails and conclude that interacting with email is professional Russian Roulette. When interacting with an email becomes a bet-your-job/freedom decision, users will be far less likely to enjoy the productivity benefits of email. Abandoning a highly efficient means of communication undermines Information Superiority.

Section 6. Using Human Factors to Disrupt the Spearphishing Information Operation

> ***information superiority.*** *The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.*
>
> -Joint Publication 2-0, *Information Operations*[68]

Spearphishing yields information superiority to the APT attacker. The successful spearphishing attack gives the attacker access to information and can be used to disrupt the victim's information processing systems. A defensive response that reduces the utility of email is a less devastating shift of information superiority as the fear of spearphishing denies prospective victims the use of a very efficient means of disseminating information.

NASA provides this model, Illustration 8, of HF analysis.[69] The model depicts how people and systems interact, illustrating the flow of information between people and the machine components of the system. This Human Factors Interaction Model provides a different perspective of a spearphishing attack.

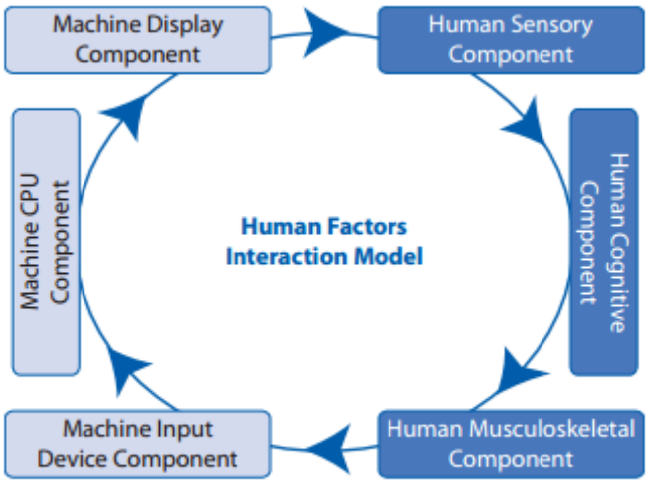


Figure 7.4-1 Human factors interaction model
Illustration 8

Step 1. Machine CPU Component. The attacker's deceptive email is received.

Step 2. Machine Display Component. The deceptive email is displayed to the target audience.

Step 3. Human Sensory Component. The target audience sees the deceptive email (**See** step of military deception).

Step 4. Human Cognitive Component. The target audience is deceived in the information operation through the use of the cognitive factors discussed above (**Think** step of military deception).

Step 5. Human Musculoskeletal Component. The user operates the keyboard according to the directions of the attacker (**Do** step of military deception).

Step 6. Machine Input Device Component. The user's keystrokes are converted to machine instructions that implement the attacker's will.

In the spearphishing engagement, the attacker uses the HF tool of system, interface, and task design to engineer the HSI result of a compromised system. In response, none of the HF tools are being used effectively by the defenders. In order to take email back from the attackers, defenders must address the HSI factors that make email a malicious interface. [70]

It is possible to leverage intelligence and existing email technologies to create an email interface which allows users to adopt new email processing habits which quickly and easily unmask attempts to infiltrate using stolen trust.[71] This simulated inbox demonstrates an inbox that

provides differential marking of trusted senders.[72]

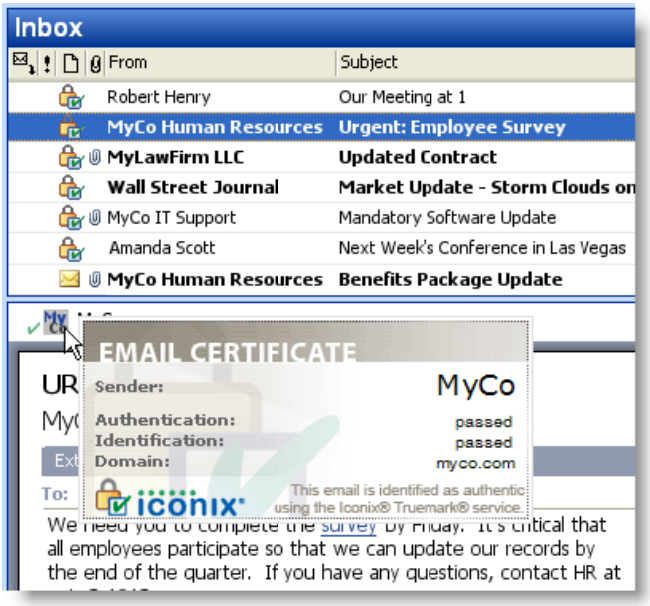


Illustration 12

In this example, all of the senders that information assurance deems trustworthy have a trust indicator in the inbox. This trust indicator is reinforced in the message with additional iconography and a hover-over information window. The last message in the inbox is a spearphishing attack in which the attacker is attempting to be perceived as the HR Department. The display now integrates the knowledge of information assurance (the attacker is not the trusted HR Department) with the perception of the victim (the sender is the trusted HR Department), thereby revealing the Spearphishing Incongruity and uncovering the attack. The security information is presented without a large Compliance Budget task cost and can quickly become the foundation of improved email processing habits.

This interface uses the tools of: (1) improved system, interface, and task design; and (2) procedure improvement to address the malicious interface issues of email. The improved system, interface and task design tools are implemented in the modified interface which augments previously difficult to determine trust information with trust determinations from IT professionals, thereby simplifying the task of decoding email trustworthiness. The procedure improvement consists of placing IT's trust determinations in the user's screen display, shifting the complex technical decisions from users to IT professionals. Instead of a vague admonition to avoid suspicious emails at the risk of your job or your freedom, the user is now provided with actionable warning intelligence that permits the intended victim to identify and report the attack rather than being tricked into compromising the system.

Applying the Human Factors Interaction Model to the modified interface demonstrates the benefits of this improved interface and process.

Step 1. Machine CPU Component. The attacker's deceptive email is received. The email processing systems uses the widely deployed standards-based email authentication system to apply IT trust determinations to the email.

Step 2. Machine Display Component. The email is displayed to the target audience with IT trust determination information.

Step 3. Human Sensory Component. The target audience sees the deceptive email without a trust indicator (**See** step of military deception).

Step 4. Human Cognitive Component. The target audience is not deceived in the information operation because the cognition task is now consistent with user cognitive processes (**Think** step of military deception).

Step 5. Human Musculoskeletal Component. The user does not operate the keyboard according to the directions of the attacker (**Do** step of military deception).

Step 6. Machine Input Device Component. There are no user keystrokes to be converted to machine instructions that implement the attacker's will.

The enhanced user interface is built on implementing the principles of HSI. In order to undermine the modified interface, a single-stage spearphishing attack requires the compromise of the trusted sender's DNS records, a technical task far more challenging than sending a well-crafted work of military deception. A multi-stage attack requires a first stage compromise in order to take control of an email account for multi-stage operations. Of course, users are still able to make compromising decisions in the enhanced interface. However, incorporating security information into the user interface will help users avoid the allure of military deception.

The enhanced user interface improves the HSI of email, making the user less likely to be deceived.

About the Authors

John Zager

John Zager is a psychologist with a penchant for systems analysis. He holds a BA degree in Psychology and an MA degree in Industrial Organizational Psychology from Hofstra University While completing his undergraduate studies, he served as an intern for U.S. Senator Kirsten Gillibrand (D, NY). He is currently a financial analyst at PepsiCo, Inc. in White Plains, New York.

Robert Zager

Robert Zager is an inventor and entrepreneur. He has been granted eleven United States patents in the areas of computer networking and email. He holds a BA degree from the University of California, Berkeley and a JD degree from Santa Clara University. He is currently a security researcher at Iconix, Inc. in San Jose, California.

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

References and Notes

[1] 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

[2] Johnson, Jeh, *Statesmen's Forum: DHS Secretary Jeh Johnson*, Center for Strategic & International Studies, 8 July 2015. Web. 20 June 2016, https://www.csis.org/events/statesmen%E2%80%99s-forum-dhs-secretary-jeh-johnson at 26'50"

[3] CERT Insider Threat Center. *Unintentional Insider Threats: A Review of Phishing and Malware Incidents by Economic Sector* (CMU/SEI-2014-TN-007). Software Engineering Institute, Carnegie Mellon University, 2014. Web. 08 June 2015, http://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_297777.pdf

[4] Libicky, Martin; Ablon, Lillian; and Webb, Tim, *The Defender's Dilemma: Charting a Course Toward Cybersecurity*, RAND, 2015.

[5] *United States of America v. Su Bin Criminal Complaint*, 27 June 2014. Web. 1 July 2014, https://www.documentcloud.org/documents/1216505-su-bin-u-s-district-court-complaint-june-27-2014.html

[6] Williams, Katie Bo, *OPM underestimated number of fingerprints stolen in hack by millions*, The Hill, 23 September 2015. Web. 20 June 2016, http://thehill.com/policy/cybersecurity/254620-opm-underestimated-number-of-fingerprints-stolen-in-hack

[7] Chang, Frederick R., Ph.D., *Guest Editor's column*, The Next Wave, Vol. 19, No. 4, 2012. Web. 20 June 2016, https://www.nsa.gov/resources/everyone/digital-media-center/publications/the-next-wave/assets/files/TNW-19-4.pdf

[8] Libicky, Martin; Ablon, Lillian and Webb, Tim, (n 4), Page 32.

[9] Return Path, "The Sender Reputation Report: Key Factors that Impact Email Deliverability," available by registering at http://www.returnpath.net/landing/reputationfactors/index.php?campid=701000000005fQf

[10] Li, Qing and Clark, Gregory. *Security Intelligence*. Indianapolis: Wiley, 2015. Page 251.

[11] Joint Publication 6-0, *Joint Communications Systems*, Page I-2.

[12] The physical dimension is composed of command and control (C2) systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. It is the dimension where physical platforms and the communications networks that connect them reside. The physical dimension includes, but is not limited to, human beings, C2 facilities, newspapers, books, microwave towers, computer processing units, laptops, smart phones, tablet computers, or any other objects that are subject to empirical measurement. The physical dimension is not confined solely to military or even nation-based systems and processes; it is a defused network connected across national, economic, and geographical boundaries. JP 3-13, page I-2.

[13] The informational dimension encompasses where and how information is collected, processed, stored, disseminated, and protected. It is the dimension where the C2 of military forces is exercised and where the commander's intent is conveyed. Actions in this dimension affect the content and flow of information. JP 3-13 page I-3.

[14] JP 3-13, Page I-1.

[15] JP 3-13, Page I-3.

[16] Kahneman, Daniel and Tversky, Amos. *Choice, Values, Frames*. New York: Russell Sage Foundation, 2000.

[17] JP 3-13, Page I-3.

[18] JP 2-01.3, Page I-3.

[19] JP 3-13, Page I-2.

[20] JP 3-13, Page I-5.

[21] Rogers, Michael, ADM., *Briefing with Admiral Michael Rogers, Commander of U.S. Cyber Command*, Wilson Center, 08 September 2015, at 42'20". Web. 21 June 2016, https://youtu.be/1ZjsT4Ew_Sg

[22] JP 3-13, Page II-1.

[23] Ubiquiti Networks, Inc., Form 8-K, 06 August 2015. Web. 10 October 2015, https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm;

[24] FBI, *Business E-Mail Compromise*, 22 January 2015. Web. 02 November 2015, http://www.ic3.gov/media/2015/150122.aspx

[25] *New Dridex Botnet Drives Massive Surge in Malicious Attachments*, Proofpoint, 23 December 2014. Web. 21 June 2016, https://www.proofpoint.com/us/threat-insight/post/New-Dridex-Botnet-Drives-Massive-Surge-in-Malicious-Attachments

[26] Proofpoint, *Is Your Cybersecurity Strategy Ready for the Post-Infrastructure Era?*, available by registering at https://event.on24.com/eventRegistration/EventLobbyServlet?target=registration.jsp&eventid=1079889&sessionid=1&key=2D23A89FB3DB3AB91B464510750709BD&sourcepage=register

[27] The Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541, et seq.)

[28] Defense Science Board. "Resilient Military Systems and the Advanced Cyber Threat," *Department of Defense*, January 2013, Page 34. Web. 01 March 2013, http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf

[29] Kyzer, Lindy, *Phishing Fools Would Lose Clearance if DISA CISO Gets His Way*, ClearanceJobs.com, 23 September 2015. Web. 15 November 2015, https://news.clearancejobs.com/2015/09/23/phishing-fools-lose-clearance-disa-ciso-gets-way/

[30] Berman, Dennis, (n 1).

[31] Moore, Jack, *If You Fall For A Phishing Scam, Should You You're your Security Clearance?*, Nextgov, 18 September 2015. Web. 21/June 2016, http://www.nextgov.com/cybersecurity/2015/09/if-you-fall-phishing-scam-should-you-lose-your-security-clearance/121427/

[32] Richtel, Matt and Kopytoff, Verne, *E-Mail Fraud Hides Behind Friendly Face*, The New York Times, 02 June 2011. Web. 21 July 2015, http://www.nytimes.com/2011/06/03/technology/03hack.html?_r=0

[33] Vishwanath, Arun., Herath, Tejaswini., Rao, Raghav., Chen, Rui. and Wang, Jingguo. "Why Do People Get Phished? Testing Individual Differences in Phishing Susceptibility Within an Integrated Information-Processing Model" *Paper presented at the annual meeting of the International Communication Association, Suntec Singapore International Convention & Exhibition Centre, Suntec City, Singapore*, 22 June 2010. Web. 22 June 2016, http://citation.allacademic.com/meta/p400353_index.html

[34] Caputo, Deanne, MITRE; Pleeger, Shari, Dartmouth College; Freeman, Jesse, MITRE and Johnson, M. Eric, Vanderbilt University, *Going Spear Phishing: Exploring Embedded Training and Awareness*, Jan-Feb 2014. Web. 03 August 2014, http://www.computer.org/csdl/mags/sp/2014/01/msp2014010028-abs.html

[35] JP 3-13, Page I-3.

[36] Beautement, Adam; Sasse, M. Angela; and Wonham, Mike, "The compliance budget: managing security behaviour in organisations," *Proceedings of the 2008 workshop on new security paradigms*. ACM, 2009.

[37] Beautement, Adam; Sasse, M. Angela; and Wonham, Mike, (n 36), Page 6.

[38] KnowBe4, Web. 29 June 2015, http://cdn2.hubspot.net/hubfs/241394/Knowbe4-May2015-PDF/SocialEngineeringRedFlags.pdf?t=1435267515481

[39] CERT Insider Threat Center, (n3).

[40] Jakobsson & Ramzon. *Crimeware: Understanding New Attacks and Defenses.* Stoughton, MA: Pearson Education, Inc., 2008. Page 582.

[41] Silicon Valley United States Representative Anne Eshoo uses this email address: Anna Eshoo <Congresswoman.Eshoo@address-verify.com>. The domain is address-verify.com.

The IRS uses this email address: Guidewire <irs@service.govdelivery.com>. The domain is govdelivery.com.

These examples are not to suggest that the Congresswomen or the IRS are engaged in improper email practices. Rather, these examples of appropriate email practices show how hard it is for email recipients to determine what email domains are legitimate. Why would a careful email recipient conclude that real emails from the U.S. Government are sent from dot com domains?

[42] Leber, Rebecca, *Trick Websites Dupe Democrats Into Donating To Republicans*, ThinkProgress, 03, February 2014. Web. 12 December 2015, http://thinkprogress.org/justice/2014/02/03/3242381/republicans-trick-voters-donating-democratic-candidates/

[43] Miller, Zeke, *People Are Gobbling Up Hillary Clinton Websites*, TIME, 14 March 2014. Web. 21 June 2016 https://web.archive.org/web/20150430052552/http://time.com/24480/hillary-clinton-websites-2016

[44] Lilley, Kevin, *Army flagged OPM breach notice as phishing attempt*, ArmyTimes, 26 July 2015. Web. 24 March 2016, http://www.armytimes.com/story/military/2015/07/25/army-flagged-opm-breach-notice-phishing-attempt/30529623/

[45] Rasmussen, Rod, *Global Phishing Survey: Trends and Domain Name Use in 1H2011*, Anti-Phishing Working Group, November 2011. Web. 20 June 2015, http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2011.pdf, Page 15.

[46] Blake, Adam; Nazarian, Meenely and Castel, Alan, "The Apple of the mind's eye: Everyday attention, metamemory, and reconstructive memory for the Apple logo," *The Quarterly Journal of Experimental Psychology*, Volume 68, Issue 5, 2015.

[47] Ayal, Shahar and Beyth-Marom, "The effects of mental steps and compatibility on Bayesian reasoning," *Judgment and Decision Making*, Volume 9, Number 3, May 2014, pp. 226-242.

[48] Rubinstein, Ariel, "Response time and decision making: An experimental study," *Judgment and Decision Making*, Volume 8, Number 5, September 2013, pp. 540-551.

[49] *Enterprise Protection: Antispam Effectiveness*, Proofpoint, Web.21 June 2016, https://www.proofpoint.com/us/anti-spam-effectiveness

[50] Parasuraman, R.; Molloy, R. and Singh, I., "Performance Consequences of Automation-Induced Complacency," *The International Journal of Aviation Psychology*, vol. 3, no. 1 (1993), pp. 1–23.

Bagheri and G. and Jamieson, A., "Considering Subjective Trust and Monitoring Behavior in Assessing Automation Induced "Complacency," *Proceedings of the Human Performance, Situation Awareness and Automation Conference*. (Marietta, GA: SA Technologies, 2004).

[51] Lu, Xi; Xie, Xiaofei and Liu, Lu, "Inverted U-shaped model: How frequent repetition affects perceived risk," *Judgment and Decision Making*, Volume 10, Number 3, May 2015, pp. 219-224.

[52] Vishwanath, et al., (n 33).

[53] Duhigg, Charles. *The Power of Habit: Why We Do What We Do in Life and Business*. New York: Random House, 2012.

Simon, Carmen. *Impossible to Ignore: Creating Memorable Content to Influence Decisions*. New York: McGraw-Hill Education, 2016.

[54] JP 3-13.4, Page IV-2.

[55] Macalintal, Ivan, *Xtreme RAT Targets Israeli Government*, 29 October 2012, Web. 01 August 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/xtreme-rat-targets-israeli-government/

[56] Zager, Robert and Zager, John, "Combat Identification in Cyberspace," *Small Wars Journal*, 25 August 2013. Web. 1 August 2014, http://50.56.4.43/jrnl/art/combat-identification-in-cyberspace

[57] Schultz, Wolfram. "Behavioral theories and the neurophysiology of reward."*Annu. Rev. Psychol.* 57 (2006): 87-115.

[58] Vishwanath, et al., (n 33).

[59] Zager and Zager, (n 56).

[60] Hutchins, Eric M.; Cloppert, Michael J.; Amin, Rohna M, Ph.D., *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Web. 1 August 2014. http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

[61] Acronymns:

ACL: Access Control List
AV: Anti-Virus
DEP: Data Execution Prevention
DNS: Domain Name Service
HIDS: Host-based Intrusion Detection System
Honeypot: A trap set to detect or otherwise counteract attempts at unauthorized system usage.
NIDS: Network Intrusion Detection System
NIPS: Network Intrusion Prevention System
Tarpit: A system that delays network connections to slow down network abuses such as spamming and broad scanning.

[62] U.S. v. Turchynov, Indictment, 06 August 2015. Web. 11 November 2015, http://online.wsj.com/public/resources/documents/DNJIndictment.pdf

[63] U.S. v. Su Bin, Criminal Complaint, (n 5).

[64] See, for example, Department of Defense Handbook, Human Engineering Program Process and Procedures, MIL-HDBK-46855A.

[65] NASA, Systems Engineering Handbook, NASA/SP-2007-6015, Rev 1, Page 246.

[66] Zager and Zager, (n 56).

[67] Vishwanath, et al. (n 33).

[68] JP 3-13, Page GL-3.

[69] NASA, (n 65), Page 247.

[70] Conti, Gregory and Sobiesk, Edward; "Malicious Interfaces and Personalization's Uninviting Future;" *IEEE Security and Privacy*, May/June 2009.

[71] Zager, Robert and Zager, John, *Deploying Deception Countermeasures in Spearphishing Defense*, Science of Security, 10 March 2015. Web. 21 June 2016, http://cps-vo.org/node/18422

[72] These innovations are covered by one or more of the following patents held by Iconix: U.S. Patents 7,413,085; 7,422,115; 7,457,955; 7,487,213; 7,801,961; 8,073,910; 8,621,217; 8,903,742; 9,137,048; 9,325,528.