CALL SIGNS

USN AEP

SOCIETY

Volume 5, Issue 2
Winter, 2014

A Publication of the United States Naval Aerospace Experimental Psychology Society

Contents

About the USN ★ AEP Society

As military transformation continues to affect today's and tomorrow's Department of Defense and the Navy Medical Service Corps, the need to promote the role of Aerospace Experimental Psychologists as leaders and innovators in aerospace psychology continues.

Naval Aerospace Experimental Psychologists offer a unique combination of education, knowledge, skills, and experiences to address current and emerging challenges facing the Navy, joint, and coalition environments.

The U.S. Naval Aerospace Experimental Psychology Society (USNAEPS) is an organization intent on:

- Integrating science and practice to advance the operational effectiveness and safety of Naval aviation fleet operators, maintainers, and programs
- Fostering the professional development of its members and enhancing the practice of Aerospace Experimental Psychology in the Navy
- Strengthening professional relationships within the community

AEP Specialty Leader
CDR Jim Patrey, NAWC-AD

USNAEPS President
LCDR Tatana Olson, NAMI

Vice President
LT Brennan Cox, NHRC

Treasurer
LCDR Will Wells, NAVAIR

Editor
LCDR Pete Walker, NMRC

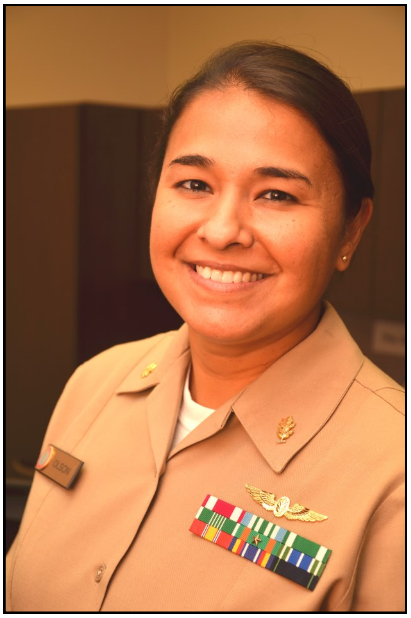
Co- Editor
LT Joe Geeseman, NAWC-AD

Historian / Layout Editor
LT Eric Vorm, NAMI

Message From The President

LCDR TATANA OLSON, AEP #126

Happy New Year! As we enter 2015, I am very thankful for all USNAEPS has accomplished in the past year and incredibly honored to have the opportunity to serve the dedicated and talented members of USNAEPS for a second term as the Society's President. I would like to express my sincere gratitude and appreciation to all of the outgoing Executive Committee (EXCOM) members who have supported me over the past year, and a warm welcome to the new EXCOM members (some of whom have returned for second and even third terms!).



In the upcoming year, the Society will continue to focus its efforts on two core areas: expanding USNAEPS membership and influence and preserving the rich history of our USNAEPS members and their contributions to the field of Aviation Psychology. Membership in the Society is overwhelmingly comprised of current, former, and retired Aerospace Experimental Psychologists (AEP) – not surprising, of course, given that the organization was founded by AEPs. However, we are a small community and only grow by two or three individuals a year at the most. In the interest of expanding the diversity of our member ranks, and hopefully, the breadth of our influence, 2015 will be the year of the "Professional Member." According to the Society's bylaws, individuals not designated as AEPs are eligible for Society membership if they can demonstrate significant contributions to the field of Aviation Psychology through research, publications, and leadership. We work with many of these individuals on a daily basis, individuals whose insights and commitment to advancing the field are in keeping with the "ethos" of our Society. If you know of such an individual, I encourage you to nominate them for membership in USNAEPS.

Although USNAEPS is only approaching its 6th birthday, we are fortunate to have members who served as the pioneers of Aviation Psychology from the 1940s through the 1960s. Their contributions helped to shape the field and represent precious history that we must preserve. After all, how can we know how far we have come if we don't remember where we started? To this end, the Society will be working hard to create biographies and historical profiles for our more senior members and collect important historical documents and pictures for our archives. If there is anything you would like to contribute, please contact the USNAEPS Historian, LT Eric Vorm (eric.vorm@med.navy.mil). Additionally, USNAEPS will continue to support the ongoing development of a display chronicling the history of Aerospace Medicine in the Navy at the National Naval Aviation Museum in Pensacola, Florida.

Without further ado, it is with great pleasure that I present our 10th (Winter, 2014) issue of Call Signs, the first under the leadership of our new Editor, and Society Founder, LCDR Pete Walker. In this issue, we focus on an area that has received a tremendous amount of attention in the media – Cybersecurity. As witnessed by several high profile cases over the past decade, threats to cybersecurity, both within and outside the military, represent a very real and complex problem. As noted by CAPT (ret) Mike Lilienthal in his article, *Cybersecurity and Human Systems Integration*, "the cyber domain is a combination of hardware, software, and human operators and maintainers." As such, there are tremendous opportunities for AEPs and other human factors professionals to apply their unique skills, education, and experience to address some key challenges. I would like to extend a special thanks to Dr. Dan Phelps, Associate Professor of Information Systems at Carnegie Mellon University in Qatar and Information Dominance Officer in the Navy Reserve, for providing an insightful and provocative introductory article. In this issue, we also bid "Fair Winds and Following Seas" to CAPT John Schmidt, AEP #93 and USNAEPS member, after more than 30 years of dedicated military service. Thank you for all you have done for the AEP community and the field!

In closing, I would like to thank you for your continuing support of the Society. As stated by prominent Industrial and Organizational Psychologist, Benjamin Schneider, "the people make the place," so please stay active, stay engaged, and don't hesitate to contact me with ideas, concerns, questions, etc. On behalf of the entire USNAEPS Executive Committee, happy New Year and we look forward to moving full speed ahead in 2015!

Information Systems Security for the Psychologist: An Introduction to the Field

BY DR. DANIEL C. PHELPS, CARNEGIE MELLON UNIVERSITY

Information and information processing are fundamental to any human endeavor, but modern technologies have increased the speed and volume with which information arrives. While military strategists from Sun Tzu to Clausewitz to Boyd have recognized the critical role information and information processing plays in any successful campaign, the use of modern technologies to produce, transmit, process, and store that information have introduced both new opportunities and threats to the organizations and nation-states that rely on them. As such, beginning with the revolution in military affairs (RMA) of the late 80's and early 90's, there has been an increased recognition of the need to identify how those threats and opportunities could be realized, both offensively and defensively.

Growing out of the RMA was the term Information Warfare, defined differently by several authors (e.g., Libicki, 1995; Arquilla and Ronfeldt, 1993), but ultimately encompassing the areas of military deception, electronic warfare, computer network operations, operational security and psychological operations. The goal was to combine these areas into one coherent effort aimed at gaining information dominance, protecting and enhancing one's own information while manipulating or denying information to the enemy, in any conflict.

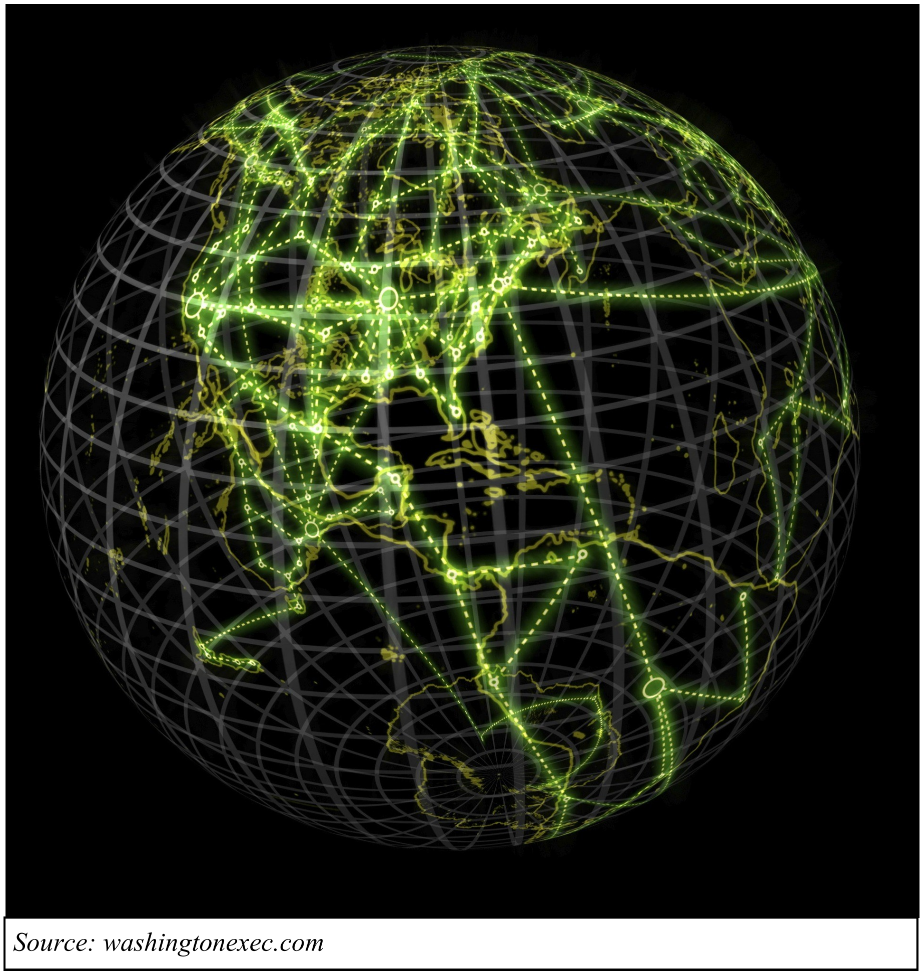
Information warfare was ultimately subsumed under the broader term Information Operations, which is defined in Joint Publication (JP) 3-13 as "[t]he integrated employment, during military operations, of information related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own (pg. GL-3)." Information operations take place in the information environment, which is the "aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information (pg. I-1)" and consists of physical, informational, and cognitive dimensions. While the physical and informational aspects are likely the first areas that come to mind when one hears the term information operations, arguably the cognitive dimension is the most important. In fact, while the highlight is mine, the primacy of the cognitive area is emphasized in JP 3-13 (pg. I-3):

"The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information. It refers to individuals' or groups' information processing, perception, judgment, and decision making. These elements are influenced by many factors, to include individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies. Defining these 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. As such, this dimension constitutes the most important component of the information environment."

Fortunately, the cognitive domain is also the area in which psychologists have critical expertise. Regardless of one's specialized subdiscipline of psychology, there are opportunities to make significant impacts on the understanding of cognitions and behaviors related to information operations. The literature on counterproductive work behaviors (CWB), for example, has informed research on the insider threat (Phelps et al., 2007; Shaw et al., 2009; Greitzer et al., 2010). From Ana Montes to Manning and Snowden, individuals with access to classified information have chosen to release that in-

Source: nationaldefensemagazine.org

formation for a variety of reasons. As protecting classified and sensitive unclassified information is critical to ensuring strategic, operational, and tactical initiatives are accomplished with minimal risk, identifying situations and behaviors which might indicate that an individual is more likely to disclose classified information, before the disclosure is made, would allow for interventions to channel the individual to more appropriate behaviors. As the literature related to CWB examines situational, individual, cognitive, and behavioral aspects that bear on information operations, it also provides context for highlighting the roles that various psychological perspectives can bring to bear on similar problems.


Source: washingtonexec.com

The domains of situational and individual factors associated with behaviors is an important area of research for examining the online environment. Perceived injustices perpetrated by the U.S. or U.S. organizations have already led to online attacks. In 2001, for example, the cracker 'Pimpshiz' admitted to defacing more than 200 websites in retaliation for the copyright infringement lawsuits against Napster, while more recently, the group Anonymous reportedly attacked the Church of Scientology in 2008 for "abuse of copyright laws" and Sony in 2011 for their roles in the prosecution of George Hotz (Meek, 2001; Singel, 2011; Poulsen, 2011). Additionally, both the Anonymous and Lulzsec groups reportedly targeted Visa, PBS, and other organizations in retaliation for the organizations' behaviors with regards to Wikileaks (Lee, 2011). These targeted attacks, with their overt political intent, have been termed "hacktivism," which is defined by Denning (2000) as the marriage of hacking and activism. Hactivism can be further divided based on origin and orientation into marginally normative behaviors, such as political coding and performative hacktivism, and non-normative behavior, such as political cracking. Political cracking, as described by Samuel (2004, p.51), includes behaviors such as "...site defacements, redirects, denial of service attacks, information theft, and sabotage" and is typically characterized by relatively small groups working with some degree of anonymity. Understanding what motivates such normative and non-normative behavior in the cyber domain can have important implications for cyber security. Collective behavior is defined by Turner and Killian (1987, p.3) as "...those forms of social behavior in which usual conventions cease to guide social action and people collectively transcend, bypass, or subvert established institutional patterns and structures." In examining collective behavior, many theories have been advanced to explain why individuals engage in what in other circumstances would be seen as non-normative behaviors. Central to many of these theories are the concepts of anonymity and deindividuation (LeBon, 1897; Zimbardo, 1969; Diener et al., 1980) and emotion (LeBon, 1897; Zimbardo, 1969), while others, such as Emergent Norm Theory (ENT) (Turner and Killian, 1972, 1987) posit that a precipitating event results in a normative crisis leading members of the collective, through interaction, to create new normative structures to guide their behavior.

Although ENT broke from the classical theories on crowd behavior and provides a foundation for understanding collective action, it doesn't sufficiently explain how collective action can occur without significant discussion. Social identity theory bridges this shortcoming and together with relative deprivation theory, intergroup emotion theory, and group efficacy can provide a strong foundation for understanding why groups attack an information system (Brunsting and Postmes, 2002; Van Zomeren et al., 2008; Van Zomeren and Iyer, 2009; Tausch et al., 2011; Mackie et al., 2008; Livingstone et al., 2011; Smith and Ortiz, 2002; Tajfel and Turner, 1979). In addition to group behavior, personality traits and the factors that affect how they are expressed remain important in the online environment. Issues related to how culture mediates the expression of personality traits can have important consequences for understanding and predicting how people from different regions might respond to issues online. For example, Lake (2011) examined the role of culture in an individual's propensity to engage in online cyber-harassment. Using the cultural dimensions of Power Distance, Individualism, Uncertainty Avoidance, Masculinity, and Time Perspective with individual needs for Power, Affiliation, and Achievement, Lake examined the frequency and intensity of response to an intentionally provocative website of individuals from different cultural regions.

Culture, too, plays a role in the effectiveness of different persuasion techniques (Ciccarelli, 2007). Issues related to social engineering and adherence to information security related policies is a continuing source of important information security research. While technological controls are often thought of as the first line of defense against attempts to subvert the security of an information system, it is the people that install, maintain, and use the systems that often introduce significant vulnerabilities. Influencing others based on an understanding of tendencies towards conformity, compliance, and obedience can lead to unintentional violations of security policy, which in turn can lead to a significant compromise of an information system. An annual study done by Infosecurity Europe (InfoSecEurope, 2004) has found that office workers are likely to give away their passwords in certain situations. In their 2004 survey, of the 172 surveyed, 37% were willing to give away their password when initially asked, and 34% more were willing to reveal their password with mild social engineering. The ubiquitous phishing attempt, in which an individual is sent a provocative email in the hopes that they will click the associated link, which often results in system compromise, is another example of a social engineering attack. Whaling and spear-phishing are even more highly targeted attempts of social engineering in which the attackers develop an email that appears to be legitimate and often includes more highly personalized information to entice the target to execute the payload. Understanding how social engineers manipulate can lead to effective training programs to help organization members recognize and respond to such attempts appropriately. The elaboration likelihood model of persuasion (Cacioppo and Petty, 1984) can inform research on phishing emails, for example, as understanding central versus peripheral route processing of information related to the email messages likely affects the success rate.

The domains of situational and individual factors associated with behaviors is an important area of research for examining the online environment.

Dr. Dan Phelps is an Associate Teaching Professor in the Information Systems Department of Carnegie Mellon University in Qatar. He received his doctorate in Information Studies from Florida State University in 2005 and is certified as an Information Systems Security Professional and Information Systems Security Officer. Additionally, LT Phelps is currently serving as an Information Warfare Officer in the U.S. Navy Reserve, prior to which he served as an Operational Intelligence Specialist in the U.S. Air Force Reserve from 2002 to 2006 and a Hospital Corpsman in the U.S. Navy Reserve from 1991 to 2002.

A significant corpus of research has also focused on issues related to computer abuse. Straub (1986, 1990) introduced the use of criminological theory to the examination of information system security management. Drawing from General Deterrence Theory, Straub focused on issues related to the individual and their perception of disincentives with respect to non-normative computer related behavior. General Deterrence Theory, with the constructs of certainty, severity, and celerity of sanction, continues to be used in various branches of the information security related literature.

Another promising area of research related to employee compliance with information security policies is the examination of compliance through process or stage models. While much research related to information security behavior has relied on static models of behavior, such as Protection Motivation Theory to examine the "knowing-doing gap" (Workman et al., 2008) or Deterrence Theory to examine issues related to computer abuse as discussed, process or stage models examine or model information security related behaviors as dynamic processes that change in response to various individual, situational, or environmental factors. Understanding the order of stages related to information security compliance, triggers that move people from one stage to another, and stage specific and independent factors related to each stage would help in predicting or targeting behavior (Siponen and Phelps, 2014).

In addition to compliance behavior, learning theories also play a significant role in understanding how systems are secured. Social Cognitive Theory, and self-efficacy in particular, has been used to examine the relationship between different types of training on how effectively a system administrator secures their system, as well as together with locus of control, in the examination of why people who know how to secure an information system may choose not to (Phelps et al., 2012; Phelps, 2004; Workman et al., 2008). This all leads to deeper questions regarding how people think about information systems and information systems security. Faulty heuristics or mental sets that negatively affect an individual's understanding of how an information system works can lead to problems both with securing an information system or identifying where significant flaws in an information system may exist.

While I have concentrated on observable and latent constructs associated with information security research, neuroscience studies related to information systems have also been on the rise. In 2010, an article in Information System Research proposed several areas in which cognitive neuroscience can inform IS research, to include localizing the neural correlates of IS constructs, complementing existing sources of IS data with brain data, and testing consequences of IS constructs, among others (Dimoka et al., 2011). The applicability of neuroscience and functional neuroimaging techniques to issues related to information security are just now being explored.

While this article is not meant to be a comprehensive review of the literature related to information security research focused on the individual and their role in relation to cybersecurity, it is clear that the Aerospace Experimental Psychology (AEP) community, with its expertise across a range of psychological disciplines and focus on understanding the relationship between humans and technology, is in a unique position to contribute valuable insights to these issues, particularly within the military context.

References

Arquilla, J. & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy, 12(2)*:141–165.

Brunsting, S. & Postmes, T. (2002). Social movement participation in the digital age. *Small Group Research, 33 (5)*:525.

Cacioppo, J. T. & Petty, R. E. (1984). The elaboration likelihood model of persuasion. *Advances in Consumer Research, 11(1)*:673–675.

Ciccarelli, S. K. & Meyer, G. (2007). *Psychology mypsychlab edition.* Prentice Hall.

Denning, D. (2000). Activism, hactivism and cyberterrorism. *Computer Security Journal, 16(3)*:15–36.

Diener, E., Lusk, R., DeFour, D., & Flax, R. (1980). Deindividuation: Effects of group size, density, number of observers, and group member similarity on self-consciousness and disinhibited behavior. *Journal of Personality and Social Psychology, 39(3)*:449.

Dimoka, A., Pavlou, P. A., and Davis, F. D. (2011). Research Commentary - Neurois: The potential of cognitive neuroscience for information systems research. *Information Systems Research, 22(4)*:687–702.

Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C., and Hohimer, R. (2010). *Identifying at-risk employees: A behavioral model for predicting potential insider threats*. Pacific Northwest National Laboratory.

InfoSecEurope (2004). *Office workers give away passwords for a chocolate bar.* Retrieved from http://www.iwar.org.uk/news-archive/2004/04-20.htm.

Lake, M. (2011). An exploratory study of culture and cyber harassment. *International Journal of Management and Decision Making, 11(5)*:387–396.

LeBon, G. (1897). *The crowd: A study of the popular mind*. Macmillian.

Lee, A. (2011). *Lulzsec, anonymous hacker groups declare war against governments, 'gluttons'.* Retrieved from http://www.huffingtonpost.com/2011/06/20/lulzsec-anonymous-war-_n_880637.html.

Libicki, M. C. (1995). *What is information warfare?* Technical report, DTIC Document.

Livingstone, A., Spears, R., Manstead, A., Bruder, M., and Shepherd, L. (2011). We feel, therefore we are: Emotion as a basis for self-categorization and social action. *Emotion, 11(4)*:754-767.

Mackie, D., Smith, E., and Ray, D. (2008). Intergroup emotions and intergroup relations. *Social and Personality Psychology Compass, 2(5)*:1866–1880.

Meek, J. G. (2001). *Digital graffiti: Were teen's exploits political or personal?* Retrieved from http://www.eweek.com/c/a/Security/Digital-Graffiti/.

Phelps, D. C. (2004). *Information system security: Self-efficacy and security effectiveness in Florida libraries*. Unpublished dissertation.

Phelps, D. C., Cappelli, D. M., Moore, A. P., Shaw, E. D., and Trzeciak, R. F. (2007). *Research methodology for the CERT Insider Threat Project: Modeling human behavior in cyberspace (FOUO)*. Technical report, CERT Program, Survivable Enterprise Management, Carnegie Mellon University.

Phelps, D. C., Gathegi, J. N., Workman, M., and Heo, M. (2012). Information system security: Self-efficacy and implementation effectiveness. *Journal of Information System Security, 8(1)*:3-21.

Poulsen, K. (2011). *Playstation network hack: Who did it?* Retrieved from http://www. wired.com/threatlevel/category/hacks-and-cracks/page/2/.

J. Pub 3-13 (2014). *Information Operations*. DOD US.

Samuel, A. (2004). *Hacktivism and the future of political participation*. PhD thesis, Harvard University Cambridge, Massachusetts.

Shaw, E. D., Fischer, L. F., and Rose, A. E. (2009). *Insider risk evaluation and audit*. Technical report, DTIC Document.

Singel, R. (2011). *War breaks out between hackers and scientology — there can be only one*. Retrieved from http://www.wired.com/threatlevel/2008/01/ anonymous-attac/.

Siponen, M. and Phelps, D. C. (2014). *Stage theory to explain employee compliance with IS security procedures in organizations*. Unpublished Research Proposal, National Priorities Research Program. Doha, Qatar.

Smith, H. and Ortiz, D. (2002). *Is it just me? The different consequences of personal and group relative deprivation*. Cambridge University Press.

Straub, D. W. (1986). *Deterring computer abuse: the effectiveness of deterrent countermeasures in the computer security environment*. PhD thesis, Indiana University.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1(3)*:255–276.

Tajfel, H. and Turner, J. (1979). An integrative theory of intergroup conflict. *The Social Psychology of Intergroup Relations, 33*:47.

Tausch, N., Becker, J. C., Spears, R., Christ, O., Saab, R., Singh, P., and Siddiqui, R. N. (2011). Explaining radical group behavior: Developing emotion and efficacy routes to normative and nonnormative collective action. *Journal of Personality and Social Psychology, 101 (1)*:129–48.

Turner, R. and Killian, L. (1972). *Collective behavior*. Prentice-Hall, Inc., Englewood Cliffs, NJ

Turner, R. H. and Killian, L. M. (1987). *Collective Behavior*. Prentice-Hall, Inc., Englewood Cliffs, NJ, 3rd edition.

Van Zomeren, M. and Iyer, A. (2009). Introduction to the social and psychological dynamics of collective action. *Journal of Social Issues, 65(4)*:645–660.

Van Zomeren, M., Postmes, T., and Spears, R. (2008). Toward an integrative social identity model of collective action: A quantitative research synthesis of three socio-psychological perspectives. *Psychological Bulletin, 134(4)*:504.

Workman, M., Bommer, W. H., and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24(6)*:2799–2816.

Zimbardo, P. (1969). *The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos*. In Nebraska symposium on motivation. University of Nebraska Press.

Cybersecurity and Human Systems Integration

BY CAPTAIN (RET) MIKE LILIENTHAL, AEP #71

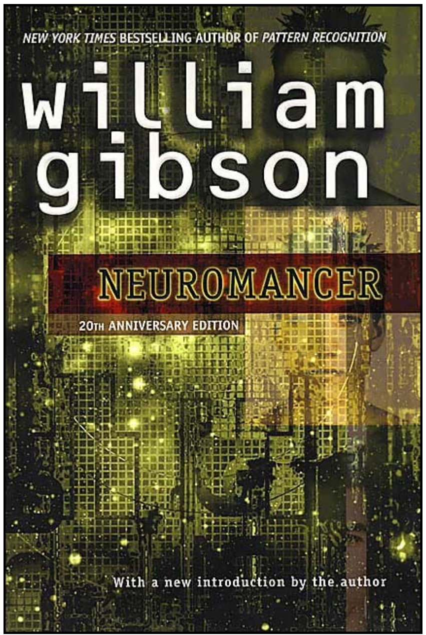
My current job is as a contractor in support of the Test Resource Management Center (TRMC), a Field Activity under the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD (AT&L)). One of my swim lanes is to work with Navy acquisition programs as they test and evaluate new systems under development to determine how effective they will operate in a cyber-contested environment. Because cyberspace is a warfare area that is totally manmade , there are opportunities for Aerospace Experimental Psychologists across the Human Systems Integration (HSI) spectrum to apply their unique skills, education, and experience.

The term "cyberspace" was identified in the science fiction novel, *Neuromancer*, by William Gibson, in 1984. In less than 30 years the concept is now a warfare domain - it has gone from concept to reality. For example, in 2008, a "worm" infected unclassified and classified networks by a Universal Serial Bus (USB) stick from infected computers in Afghanistan that reached DoD systems (Nakashima, 2011). More alarming, the Conficker worm enabled unknown attackers remote access to systems used by field combat units in 2009. (http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html)

This is a new and critical warfare domain with ubiquitous and rapidly evolving threats. The cadre of truly experienced personnel is small, and while it is growing, it will take years to fully develop. Program Managers (PMs) in charge of developing and fielding new and replacement weapon systems are often faced with making tradeoffs in a fiscally constrained environment. The Services have a lot of experience, training, and data to guide PMs in that decision making. Unfortunately, we do not have the same wealth of experience and data for cybersecurity.

We can start developing critical experience in two of the Human Systems Integration (HSI) domains, namely manpower and personnel. The Navy has, for years, strived to apply technology and improve processes to reduce the number of personnel needed to deploy on our new ships. The CVN-78 is designed to operate with 700 fewer crew members than the CVN-68 class aircraft carrier and the embarked air wing requires approximately 400 fewer personnel to deploy. The Littoral Combat Ship (LCS) has a key manning requirement of core personnel not to exceed 50 (Threshold requirement). The original requirements documents for both ship classes were developed before cyber was recognized as a warfare domain.

Are the numbers of human resources available on these ships sufficient to recognize and react to attacks on their computer systems and networks? More importantly, in order to avert an opportunistic kinetic attack, is the number of personnel sufficient to quickly restore a system (e.g. reload an operating system for the radar) that has been cyber–attacked? One way to address these questions is to collect observational data that combines the information a forensic investigator collects about the cyber-attacks with what an AEP would collect about the personnel (e.g. aptitude, training, knowledge, experience, and health) and the organization (e.g. structure, climate, and communication) that is under attack. The cyber domain is the combination of hardware, software, and human operators and maintainers. What can we glean from both the unsuccessful and successful cyber-attacks on systems in operation now? The same processes and tools for determining manpower for older warfare domains can be applied to this new one.


NEW YORK TIMES BESTSELLING AUTHOR OF PATTERN RECOGNITION
william gibson
NEUROMANCER
20TH ANNIVERSARY EDITION
With a new introduction by the author

William Gibson's novel, "Neuromancer" was the first to introduce the concept of cyberspace in 1984

This operator and maintainer viewpoint also feeds into questions about personnel selection criteria for cybersecurity. Are the selection criteria the same for those who will be cyber-defenders and those that are developing and deploying offensive cyber weapons? The flight physical determines whether or not a candidate is physically suited and psychologically adapted to the flight environment. The Navy's current Aviation Selection Test Battery (ASTB) is designed to predict how likely a candidate will successfully complete flight training. Both are based on decades of experience with the flight environment and the Navy's way of training - as well as the unforgiving nature of flight. Currently, the manpower requirements for the cyber environment are under revision. How could the experience with naval aviation selection be applied to cybersecurity selection? We can even extend the question to ask who makes the best cyber defenders and attackers? It is analogous to the question posed in the 1970s-what are the characteristics of the best fighter pilot? The data available to address that question included ground school grades, flight grades, peer evaluation, aircraft accident investigation, Top Gun results, the number of bolters, and which wire the tail hook grabbed during carrier training. It is difficult to find as objective a criterion as the arresting wire on a carrier in the cyber domain.

The cyber selection process and identifying the "top cyber-guns" is most likely more art than science at the moment. As I have seen from observing Computer Network Defense – Service Providers (CND-SP), the data related to team size, distribution of skill sets, team dynamics, and structure appears relevant and necessary to be collected, analyzed, and reported. As with aviation selection, a lot of data has to be collected, and some of it will prove to have little or no correlation to what makes a successful cyber defender or attacker. Devising and sustaining human systems integration research for this new warfare domain should be a priority for our community.

Source: nitrd.gov

Another Human System Integration domain is Safety which can also provide some insight into cybersecurity. One way to support the prevention of cyber-attacks is to look at the prevention of aircraft accidents. Some view an aircraft accident as a domino-effect series of events that culminates in an accident; take away one or more of the dominoes in that chain and the accident does not occur. For the most part, there are a series of sequential tasks that have to be accomplished by the cyber attackers. The general chain of events for an offensive cyber operations are: (1) Reconnaissance, (2) Weaponize, (3) Inject the malware, (4) Install the malware into the target system, (5) Exploit, (6) Command and Control the malware, and (7) Create the systems effects (the equivalent of an aircraft accident). How do we address each of the 6 steps to prevent step 7?

The first domino is Reconnaissance. Enemies try to identify vulnerabilities in the targeted network and systems, including credentials, software versions, and misconfigured settings. One method for gathering this information is through social engineering ploys, which fool end-users into surrendering data. This is often perpetrated through phishing (fraudulent email), pharming (fraudulent web sites), and drive-by pharming (redirected DNS settings on hijacked wireless access points). Not all approaches require the use of the internet. There is also a lot of information that can be found on the internet about new or deployed weapon systems. Electronic trade magazines, academic and professional journals (proceedings), social media (Facebook), professional networks (LinkedIn), contractor sites (both prime and subcontractor), government e-Commerce sites (Commerce Business Daily), and technical chat rooms all provide a wealth of data. Although a single piece of data may not provide insight into vulnerabilities, when added to other pieces of data, they may collectively provide the information needed to focus weaponization. The human is the most adaptable and dangerous weapon on the battlefield. It is also the weakest subsystem in the cyber warfare domain. The current recruits for the Navy and Marine Corps are comfortable using social media because most grew up with the capability. The Navy is developing and disseminating instructions and training in the hope that those who have been living online can suppress what they have been doing for years.

Engineers and computer science personnel are working on developing weapon systems, computer systems, firewalls, and expert software that they believe will protect against cyber-attacks. How will they address the insider threat issue? Some say they assume all personnel have been vetted and trained properly. This inadvertent insider threat who shares information that aids the first step in a cyber-attack will be the most difficult vulnerability to overcome. Ignoring the human-in–the-loop in the cyber contested environment leaves open a "backdoor" for cyber attackers. For the Navy to engineer out this vulnerability they will have to address the wealth of knowledge we have about individual and group human behavior. What could be brought to bear besides an annual mandated one-hour computer based training on social engineering? What feedback mechanisms could be put in place to enable personnel to self-correct their behavior? Does the augmented cognition community have any thoughts about the first domino?

If nothing else, I hope this generates more conversation within the AEP/HSI community.

Network Effects Emulation System (NE2S)/ Cyber Operational Architecture Training System (COATS): Training Non-Cyber Operators to Recognize and Respond to Simulated Cyber Attacks in the Operational Environment

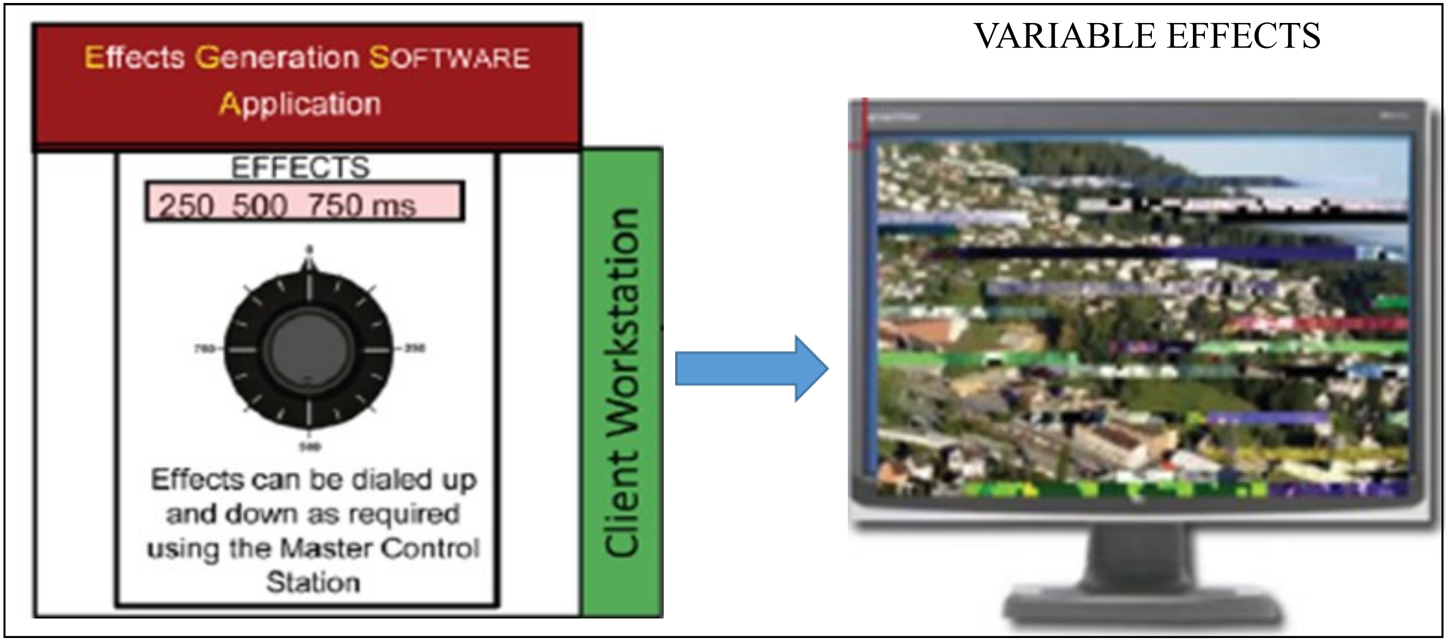
BY CDR HENRY PHILLIPS, AEP #119; DAVE KOTICK, AND AL PELUSO

Note: **The views expressed herein are those of the authors and do not necessarily reflect the official position of the Department of Defense or its components.**

Cyber attacks represent a consistent threat to US Forces that will only become more prevalent (DoD, 2011). Today, the Naval Air Warfare Center Training System Division (NAWCTSD) is employing a powerful new capability that has the potential to improve our warfighters' recognition and responsiveness to the indicators of cyber attacks in operational environments.

The Network Effects Emulation System (NE2S), managed by NAWCTSD, was originally developed by the Joint Staff J7. It is used in conjunction with the Cyber Operational Architecture Training System (COATS), a tool that enables an interoperable demonstration environment that was sponsored by the Office of the Secretary of Defense/Modeling and Simulation Coordination Office (OSD/MSCO). Together, NE2S/COATS provides seamless interoperability between what have traditionally been treated as distinct battle staff training and cyber range environments. NE2S/COATS makes it possible to integrate the elements of both to provide a richer training environment to help warfighters develop experience at coping with a broader range of integrated threats (NAWCTSD, 2014).

NE2S/COATS enables the integration of traditional military modeling and simulation (M&S), cyber range infrastructure, a cyber reference data exchange model, and most importantly, an M&S-based emulation of cyber effects on operator workstations. This affords operators the chance to train for coping with cyber threats in an operational environment, during training exercises that may not necessarily include a designated "cyber threat recognition" period. This helps operators of deployed systems – those outside the training environment - learn to recognize these threats without priming them to be temporarily hyper-vigilant for indicators of cyber activity.

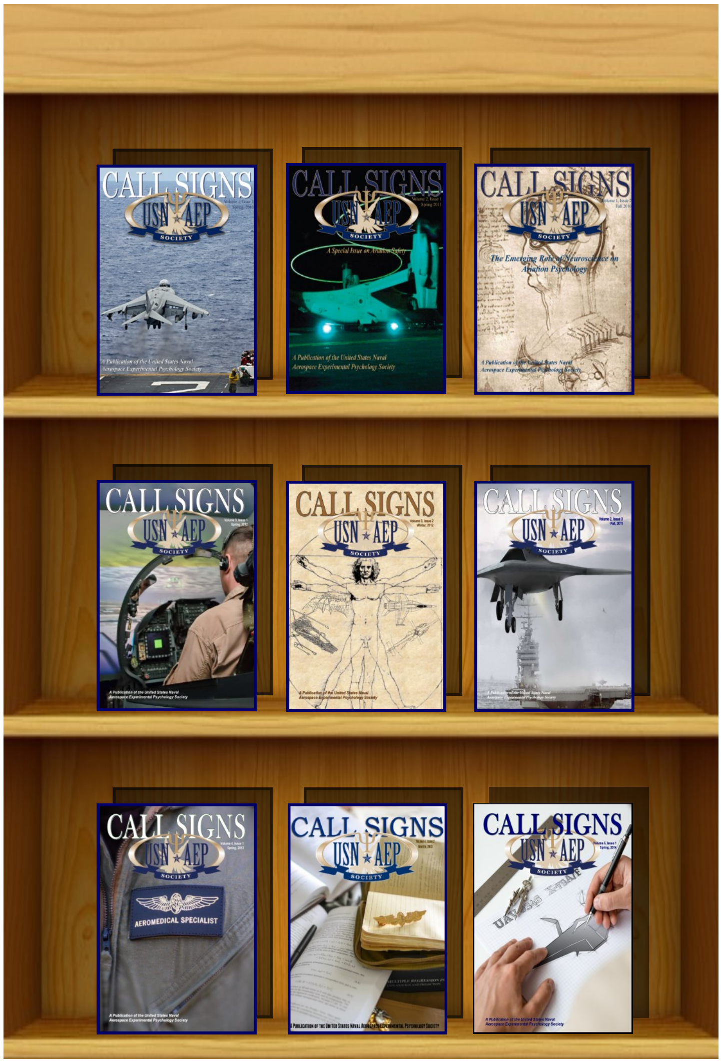

Effects Generation SOFTWARE Application
EFFECTS
250 500 750 ms
Effects can be dialed up and down as required using the Master Control Station
Client Workstation
VARIABLE EFFECTS

The NE2S Master Control Station affords centralized control of real-time, instructor-initiated effects and scheduled scenarios. The system uses a network-centric architecture that functions across operating systems and applications, and uses encrypted communications using standard network protocols (e.g. SSL, HTTPS, SSH). Authentication credentials are encrypted at rest.

This is a critical detail, since cyber threats in the operational environment will not typically be accompanied by a warning that a cyber attack is coming. In the real world, operators must be able to maintain a sustainable level of vigilance for and familiarity with the cues and indicators of a possible cyber attack. They must be prepared to speak up and take action to ascertain whether possible workstation anomalies are just bugs in their systems, or indicators of intentional attacks. These anomalies could be things as simple as screen flicker, entities whose characteristics or positions suddenly change, or even momentary failures of a mouse or controller, among others.

NE2S/COATS will improve integrated cyber operations during exercises by reducing gaps between existing traditional and cyber test and training architectures. Specifically, the system makes it possible to simulate operator-detectable indicators of a cyber attack, consisting of degraded live operator workstations. While the effects of the cyber activity on the simulated battle space are in play, operators can also incorporate synthetic operational entities used to model kinetic and non-kinetic activity. Operators can also introduce and manipulate the virtual threat effects, execute simulated attacks, and run scripted operational scenarios. The program accurately models and simulates synchronous traditional and cyber operations, as well as their interactions. Additionally, the system provides increased fidelity to traditional M&S training. Simulation models could use the NE2S data exchange protocol to communicate the effects of a cyber or kinetic attack, including but not limited to damage or degradation of entities due to loss of communications, intelligence, common operating picture, or sensors, etc.

NE2S/COATS makes it possible to execute traditional kinetic and cyber effects as part of the same exercise. An operator in an NE2S/COATS enabled exercise can get some sense of what it will be like to attempt to manage his or her sensors, relay information, and control operational assets in real time while coping with the degradations to his/her system that are likely to result from some types of coordinated cyber attack. NE2S/COATS can distribute realistic cyber effects to an entire battle staff. NAWCTSD is currently drafting interoperability guidelines for cyber-traditional federations. NE2S has already been demonstrated in numerous Combatant Commander (COCOM)-level distributed events (Castillo, 2014).



Call Signs is an electronic newsletter published on behalf of the United States Naval Aerospace Experimental Psychology Society (USNAEPS).

Call Signs is published two times annually with a biennial Summer Supplemental.

Send articles to the editor,
peter.walker.mil@mail.mil

2015 U.S. Naval Aeromedical Conference (USNAC)

BY LCDR TATANA OLSON, AEP #126

VADM Matthew Nathan, Navy Surgeon General, speaks at the 2015 USNAC conference in Pensacola, FL

The 2015 U.S. Naval Aeromedical Conference (USNAC) was held aboard Naval Air Station, Pensacola, FL from 12-15 January. Hosted by the Naval Aerospace Medicine Institute (NAMI) and the Society of U.S. Naval Flight Surgeons (SUSNFS), USNAC brought together Aeromedical officers from across the country to address the most important aeromedical issues facing the fleet. RADM Michael White, Commander, Naval Education and Training Command, and a naval aviator, delivered the opening remarks, emphasizing the critical role the aeromedical community plays in maintaining the health and safety of Naval aviators. Presentations covered a number of important areas identified in the Commander, Naval Air Forces' (CNAF) top 10 aeromedical priorities, to include spatial disorientation (SD), hypoxia, fatigue, and unmanned aircraft systems (UAS). Interestingly, a presentation by CDR Walt Dalitsch providing a historical perspective of the top 10 aeromedical priorities revealed that the aeromedical community continues to deal with many of the same issues identified in the 1940s, illustrating their tremendous complexity.

The conference featured a number of keynote speakers, to include RDML Roy Kelley, Chief of Naval Aviation Training (CNATRA), who addressed changes in naval aviation training and emerging challenges, and the Navy Surgeon General, VADM Matthew Nathan, who provided an inspirational speech about the unique expeditionary nature of the Navy medical community and its ability to respond quickly to any crisis around the world as America's "Away Team."

A common theme touched on throughout the conference was the increasing reliance on UAS and the challenges this poses for selection of UAS personnel, medical standards, training, and overall aeromedical support.

LCDR Tatana Olson, Operational Psychology Department Head at NAMI, briefed the group on the issues and considerations associated with developing a selection test for UAS personnel and provided an update on the Selection for UAS Personnel (SUPer) program sponsored by the Office of Naval Research. In addition to UAS, other topics of discussion included the need for real-time physiological monitoring to better address hypoxia, SD, and fatigue, revisiting the prevailing conceptualization of SD, and giving serious consideration to non-materiel solutions to combat SD.

Shipmates

International Engagement: NAMI Operational Psychology meets with Members of the Danish Defence Personnel Organization

BY LT MIKE NATALI, AEP #150 AND LCDR TATANA OLSON, AEP #126

On 16 December 2014, the Operational Psychology Department, Naval Aerospace Medical Institute (NAMI) in Pensacola, Florida hosted three members of the Recruitment Branch, Assessment and Selection from the Danish Defence Personnel Organization (DDPO).

The DDPO provides human resources support to all branches of the Danish Military and has oversight of the assessment and selection of personnel across 13 different occupational specialties, to include pilots, aircrew, and air traffic controllers. The primary purpose of the visit was to share best practices for aviation selection and potential opportunities for collaboration in the future. LCDR Tatana Olson, Operational Psychology Department Head, discussed the aviation selection process in the U.S. Navy, to include the Aviation Selection Test Battery (ASTB) and the flight training pipeline.

Captain Brian Jorgsholm (Air Force), the Deputy Director of Recruitment and Selection, Mr. Jimmie Andreasen, Aviation Psychologist, and Major Kresten Dam Andersen (Air Force), Tactical Air Command, provided an overview of the DDPO organization and a detailed brief on the pilot and air traffic controller selection programs. Although there were considerable similarities in the types of measures used to assess pilot aptitude, a key difference between the U.S. Navy and Danish Defence programs is scope.

While the U.S. Navy tests approximately 10,000 candidates a year for less than 2,000 pilot and flight officer slots, the DDPO assesses less than 600 candidates on average for 25 pilots slots (this year), which enables them to conduct more detailed assessments of each individual. For example, candidates undergo an intense, multiple hurdle testing process that includes 28 cognitive ability, psychomotor, and personality tests, a semi-structured interview, an individual planning exercise and group assignment, and various physical and mental health assessments.

Of particular interest to NAMI was the PILAPT test battery used by the Danish. Developed by a British company and used by commercial and military aviation organizations in several countries, the PILAPT is a psychomotor test that assesses information processing, complex coordination, spatial ability, workload capacity, decision making, and the ability to work under pressure. One potential opportunity for collaboration is an evaluation of the relationship between the ASTB's performance based measures test and the PILAPT.

Members of the NAMI Operational Psychology Department meet with personnel from the Danish Defence Personnel Organization (DDPO), Recruitment Branch. Pictured left to right: LT Mike Natali, NAMI; Capt Brian Jorgsholm (DDPO); LCDR Tatana Olson (NAMI); Mr. Jimmie Andreasen (DDPO); Ms. Sabrina Drollinger (NAMI); Maj Kresten Dam Andersen (Tactical Air Command Rep to DDPO); Mr. Cory Moclaire (NAMI).

Additionally, there was considerable discussion about the extent to which aviation selection methods would have to evolve to better address the challenges associated with the increasingly complex information management demands of platforms like the Joint Strike Fighter and unmanned aircraft systems.

At the conclusion of the meeting, Captain Jorgsholm presented LCDR Olson with a plaque bearing the crest of the DDPO's Chief, Major General Niels Bundsgaard. NAMI looks forward to continued collaboration with our international partners to improve our collective ability to select the best and brightest for military aviation.

Shipmates

Fair Winds & Following Seas: Captain John Schmidt

BY LCDR BRENT OLDE, AEP #122

The United States Navy and the USN AEPS would like to wish Fair Winds and Following Seas to CAPT John Schmidt following 32 years of active military service.

CAPT Schmidt began his military service as a 2nd LT in the US Army on 17 July 1981. Soon after receiving his commission, he accepted a graduate fellowship at the University of Houston. Upon branch qualification in the Army Medical Service Corps, CAPT Schmidt became an administrative officer in the Medical Exercise Group of the 75th Maneuver Area Command. He was responsible for administrative arrangement for large theater medical exercises to secure proper staffing, arrange for transportation, and handle on site logistics for 100-200 personnel at 2-3 exercises at different sites each year. During graduate school CAPT Schmidt taught psychology and human factors courses tied to human performance and system design; his thesis and dissertation both focused on accidents, their investigation, and prevention.

Captain John Schmidt, USA

After graduate school, CAPT Schmidt entered active duty and completed additional training at the US Army Academy of Health Sciences, Ft Sam Houston, TX before reporting to the US Army Human Engineering Laboratory, Aberdeen Proving Grounds, MD. He joined the lab's Aviation and Air Defense Directorate and conducted work on the assessment of mental workload in system operation and effectiveness design of tactical display symbology. During this tour he also completed aviation medicine and rotary- wing flight training through the US Army School of Aviation Medicine, Fort Rucker, AL, becoming the first Research Psychologist to earn the Flight Surgeon Badge. CAPT Schmidt returned to the lab and formed a joint effort with the Avionics Research and Development Activity at Ft Monmouth, NJ focused on digital map display integration into helicopters, which was later implemented in the OH58D Kiowa Warrior.

Desiring to stay involved in the application of human factors in aviation, CAPT Schmidt requested an inter-service transfer to the US Navy. He accepted a Navy Medical Service Corps commission on 12 DEC 89. He was assigned to the Naval Aerospace Medical Institute, NAS Pensacola, FL for training.

Upon completing aeromedical and fixed wing flight training, he was designated Naval Aerospace Experimental Psychologist #93 and received his Wings of Gold. CAPT Schmidt then moved on to the Naval Air Development Center, Warminster, PA where he supported ASW system development. He fleeted up as a branch head in the newly formed Naval Air Warfare Center overseeing aviation human factors S&T.

Captain John Schmidt is presented with certificates of retirement from the President of the United States, and the Chief of Naval Personnel by RADM Matthew Klunder, Chief of Naval Research. Captain Schmidt also received the Legion of Merit.

His next duty station was at the Naval Safety Center, NAS Norfolk, VA where CAPT Schmidt led human factors efforts to proactively address emerging aviation safety issues, which included the refinement and subsequent implementation of the Human Factors Accident Classification System in OPNAV 3750 Naval Aviation Safety Program. He also broke ground in identifying human error causes in unmanned aircraft, landing craft, and aircraft maintenance mishaps and developing tailored intervention for them. These efforts were cited as directly contributing to Naval Aviation experiencing its lowest mishap rate in history. CAPT Schmidt then joined the School of Aviation Safety staff with a joint appointment in Operations Research at the Naval Postgraduate School Monterey, CA. He taught human factors courses and supervised master's thesis work, receiving the Superintendent's Outstanding Instruction Award for high student evaluations and chairing 25 masters thesis committees. CAPT Schmidt also received joint research support from the Federal Aviation Administration and National Aeronautical and Space Administration to further develop his efforts to address human error in aviation maintenance. This effort led to the development and Fleet implementation of the Maintenance Climate Assessment Survey, adoption of the Maintenance Extension of the HFACS Taxonomy (HFACS ME) for inclusion in OPNAV 3750, and the development and adoption of Maintenance Resource Management training that was adopted by the Fleet Logistics Support Wing and the US Coast Guard. These FAA/NASA sponsored programs were acknowledged by the NTSB, and recognized as best practices for transition to the commercial airline industry, aircraft manufacturers, and heavy maintenance operations. CAPT Schmidt then rejoined the Naval Safety Center's staff to continue working on aviation safety issues and transition intervention strategies to afloat and ashore applications. His efforts in maintenance error reduction were successfully tested at the MCAS Cherry Point Depot to reduce Rolls-Royce F405 engine remanufacturing errors. NASA recognized the success of these products at the FLSW, MCAS Depot, and USCG and planned to partner with United Space Alliance to test them in Space Shuttle heavy maintenance operations; plans were being set to conduct the first study when the Space Shuttle Columbia mishap occurred. CAPT Schmidt was subsequently detailed to support the NASA Columbia Accident Investigation Board investigating the 3 M's: Management, Maintenance, and Materiel. He recognized the breakdown in organizational reliability and the need for NASA culture to adopt a proactive high reliability posture, which was a central theme in the final CAIB report.

When CAPT Schmidt was released by the CAIB and returned to the Nava Safety Center, he was appointed by Surgeon General as the 16th Specialty Leader for Naval Aerospace Experimental Psychology a position he held for a record six years after having been asked by the Director of the Medical Service Corps to extend. During this time he revamped initial community training, designed a matrix for career development, realigned career tracks, recruited heavily, and grew the size of the community to meet emerging Fleet requirements in selection, training acquisition, safety, and S&T.

Upon receiving orders to the Naval Aerospace Medical Institute, CAPT Schmidt spearheaded the redesign of the Aviation Selection Test Battery (ASTB) to reduce administrative requirements, associated costs, and scoring/recording/reporting time. The effort led to implementation of on-line

Captain John Schmidt is piped ashore, accompanied by his wife, Mary.

test delivery and automated scoring/recording/reporting that significantly cut cost per test and turnaround time. CAPT Schmidt also initiated efforts with the Army and Air Force to form consensus on test requirements and delivery; he established agreements for Naval Aviation to leverage the USAF computer based performance measures and USA adopting USN's on-line delivery system and parts of the ASTB.

CAPT Schmidt joined Naval Air Systems Command as the Military Director for Human Systems where he led the research and engineering efforts of over 800 personnel with a $140M operating budget supporting all Naval Aviation crew, training, and protective system acquisition and life-cycle sustainment at three CONUS sites for the Naval Aviation Enterprise. As human systems Technical Warrant Holder he skillfully supported systems engineering technical reviews for the H-53K Heavy Lift Helicopter and Broad Area Maritime Surveillance System ensuring HSI requirements were addressed. CAPT Schmidt coordinated Joint Strike Fighter HSI efforts to facilitate system development, risk reduction, and flight test; his efforts yielded timely insights into program risks and avenues for mitigation. Additionally, CAPT Schmidt played a pivotal role to establish a NAS Patuxent River satellite campus and served as core faculty for the new MS in Systems Engineering.

CAPT Schmidt rejoined the NPS Operations Research Faculty to develop and teach HSI courses, supervise eight Master's theses (bringing his total to 36), assist in the development of an online HSI Master's program, and serve as the Operations Research curriculum development committee HSI representative. He also provided consultative support on Navy acquisition activities. CAPT Schmidt chaired the NPS Institutional Review Board for human research protection, where he oversaw in-house and sponsored extramural human research. In this position, CAPT Schmidt managed 500 research protocols, streamlined processes to reduce review time by 82%, and increased compliance by 92%. His efforts led to the school being awarded its longest assurance renewal by the Department of the Navy Human Research Protection Program.

Prior to retiring, CAPT Schmidt served as the Military Deputy for Warfighter Performance supporting Dr. Terry Allard. He coordinated the planning and execution of a $200M+ S&T portfolio involving human performance, protection, and survival research with a team of 17 program officers and 24 staff members. He directed $110M division 6.1-6.3 investments addressing issues such as in-flight autonomous casualty care, high altitude monitoring systems, jet noise hearing protection, and modeling aircraft crash injury mechanisms. He also served as an expert on ethical conduct of human research in academia, acquisition, and operations; overseeing all Department of the Navy non-medical human research with a 9 member interdisciplinary staff and $3.6M budget. His efforts ensured proper alignment of department basic research, applied science, and advanced technology investments to meet emerging and sustained Naval requirements. Additionally, he provided oversight of 100+ sponsored division Principle Investigators that led to over 1,800 publications/ presentations, 17 developed products transitioning to acquisition, and 27 patent awards.

On behalf of the AEP community, CAPT Schmidt's friends and colleagues throughout the military, and the soldiers, sailors, marines, and airmen whose performance and safety he has influenced for the better, we thank CAPT Schmidt for his dedicated service and wish him all the best in his future endeavors.

Fair winds and following seas!

Shipmates

United States Naval Aerospace Experimental Psychology Society Annual Meeting, December 2014

BY: LT JOE GEESEMAN, AEP #148

On Thursday, 11 December, 2014, the United States Naval Aerospace Experimental Psychology Society held their annual meeting at Dan & Brad's Restaurant in the Hilton in Arlington, VA. The meeting began with the proverbial changing of the guard, detailed in the table below.

After positions were identified, conversation suggested that the current annual change of personnel is unsustainable and a vote to modify bi-laws to change positions from one-year to two-year appointments is pending.

LCDR Will Wells, USNAEPS treasurer, reminded the group that lifetime membership costs are only $200. Currently, 23 members have paid their annual dues. There are normally 37 paid members, and the goal for this year is to pass 40 paying members. Remember that these dues are applied to recruiting, awards, and many other facets of USNAEP functionality.

The new USNAEPS historian, LT Eric Vorm, provided information about the new aeromedical display in development at the National Naval Aviation Museum, Pensacola, FL, that showcases all AMO training and billets - including both enlisted and officer information. The display has been in production for nearly 18 months and the final product will be a whopping two-sided, interactive 50' exhibit. Significant milestones and achievements in aviation history of all aeromedical officer and enlisted personnel will be highlighted in the display. The AEP website (http://navyaep.com/) will have more information on this display as it approaches completion.

The following were awarded for their contributions to the USNAEPS community:

CAPT John Schmidt received the CAPT Paul R. Chatelier Lifetime Achievement Award

CAPT Schmidt's exemplary career spans more than 30 years and is marked by significant contributions to aviation safety, personnel assessment and selection, human factors, education, and leadership. His efforts have had a profound influence on the safety and performance of Sailors and Marines, both within and outside of the aviation community, and his dedication to teaching has instilled a commitment to science and research in service to the greater good among the numerous students, peers, and colleagues he has mentored throughout his career. His innovations in safety research and assessment have changed the scope and focus of squadron-level safety climate assessments across the Navy. His development of the now ubiquitous Maintenance Climate Assessment Survey (MCAS), based on the Swiss Cheese Model of mishap occurrence developed and championed by James Reason (1990), was a seminal contribution to the conceptualization and measurement of safety within the aviation maintenance domain. MCAS was the first tool of its kind designed to evaluate the safety climate among the aircraft maintenance population. Since its introduction, a significant body of research has shown MCAS to be an excellent predictor of safety problems and incidents at the squadron level.

LT Stephen Eggan received the CDR Robert S. Kennedy Award for Excellence in Aviation Research from LCDR Tatana Olson, USNAEPS President

LT Stephen Eggan received the CDR Robert S. Kennedy Award for Excellence in Aviation Research

LT Stephen M. Eggan received the CDR Robert S. Kennedy

Award for Excellence in Aviation Research in recognition of his significant and outstanding contributions to the field of Aerospace Psychology over the past year.

LCDR Chris Foster received the CAPT Michael G. Lilienthal Award for Leadership from LCDR Tatana Olson, USNAEPS President

During this period, LT Eggan executed $2.5M in research funds as the lead or co-investigator of several aeromedical research programs focused on the use of dEEG to address pilot spatial disorientation, the impact of pharmaceuticals on physical and cognitive performance, the identification of biomarker relationships to stress resilience, the use of working memory training to enhance cognitive readiness and increase fatigue resistance, and the evaluation of new color vision screening tests for special duty candidate selection. Additionally, LT Eggan played a critical role in organizing a Joint service Unmanned Aerial Systems (UAS) human factors workshop addressing research needs for future unmanned aviation capabilities. LT Eggan's dEEG research will be used to identify techniques to improve theoretical models of spatial disorientation, motion sickness, mishap analysis, and flight simulation, as well as develop countermeasures to mitigate the risks of aviation-related spatial disorientation mishaps. As part of a joint research program with the Air Force, LT Eggan's research on biomarker relationships to stress resilience has the potential to minimize aircrew time-to-train, reduce Naval aviation attrition rates, and enhance flight safety.

As the co-lead of the Human Factors Functional Area and the Helmet Design Working Group for the U.S. Special Operations Command (SOCOM) Tactical Assault Light Operator Suit (TALOS) initiative, LT Eggan provides biomedical, cognitive psychology, and human systems integration expertise, helping to ensure that the operator remains more important than the hardware in the development of this revolutionary warfighting system designed to enhance survivability, improve performance, and increase situational awareness.

LCDR Chris Foster received the CAPT Michael G. Lilienthal Award for Leadership

As the Assistant Specialty Leader, LCDR Foster played a critical role in recruiting high-quality talent to the AEP community and promoting awareness of AEP activities and accomplishments, while effectively managing community manning and assignment requirements during a period of significant fiscal challenges. Additionally, he led the team responsible for the design, implementation, and analysis of the Aeromedical Aviation Conditional Incentive Pay (ACIP) survey, the results of which demonstrated the impact that the loss of flight pay would have on recruiting and retention of Aeromedical officers.

In addition to these achievements, he promoted awareness and engagement of the AEP community through a number of different efforts. LCDR Foster led the development and implementation of the new ASTB-E at over 290 test sites worldwide, which included the training of over 430 examiners and the distribution of 350 peripherals. The new ASTB-E is anticipated to yield over $42M in cost avoidance each year due to training attrition, an increase of $10.4M over the previous version of the ASTB. He was asked by the Navy Special Warfare Center (NSWC) to lead a review of current SEAL instructor performance and evaluate the process used to assign instructors to various phases of training and provided critical subject matter expertise to help shape the aviation selection component of the Office of Naval Research's (ONR) Unmanned Aerial System Interface, Selection, and Training Technologies (UASISTT) Program. Additionally, LCDR Foster served as the President of the US Navy Aerospace Experimental Psychology Society (USNAEPS), Chair of the Selection and Classification Sub-TAG of the Human Factors Engineering Technical Advisory Group, and as the AEP representative to the Senior Aerospace Medicine Leader (SAML) group.

LCDR Foster's exemplary leadership and dedication to the advancement of Aerospace Experimental Psychology, both as a science and a community, will have lasting impacts on the operational readiness of Navy and Marine Corps Aviation for years to come.

Calendar: Mark These Dates Down!

Society for Industrial and Organizational Psychology Annual Meeting

- April 23-25; Philadelphia, Pennsylvania

Aerospace Medical Association Annual Meeting

- May 10-14; Lake Buena Vista, Florida

International Conference on Applied Human Factors and Ergonomics

- July 26-30; Las Vegas, NV

Human Computer Interaction international conference

- August 2-7; Los Angeles, CA

American Psychological Association annual convention

- August 6-9; Toronto, Canada

Society for Neuroscience annual meeting

- October 17-21; Chicago, IL

Human Factors and Ergonomics Society annual meeting

- October 26-30; Los Angeles, CA