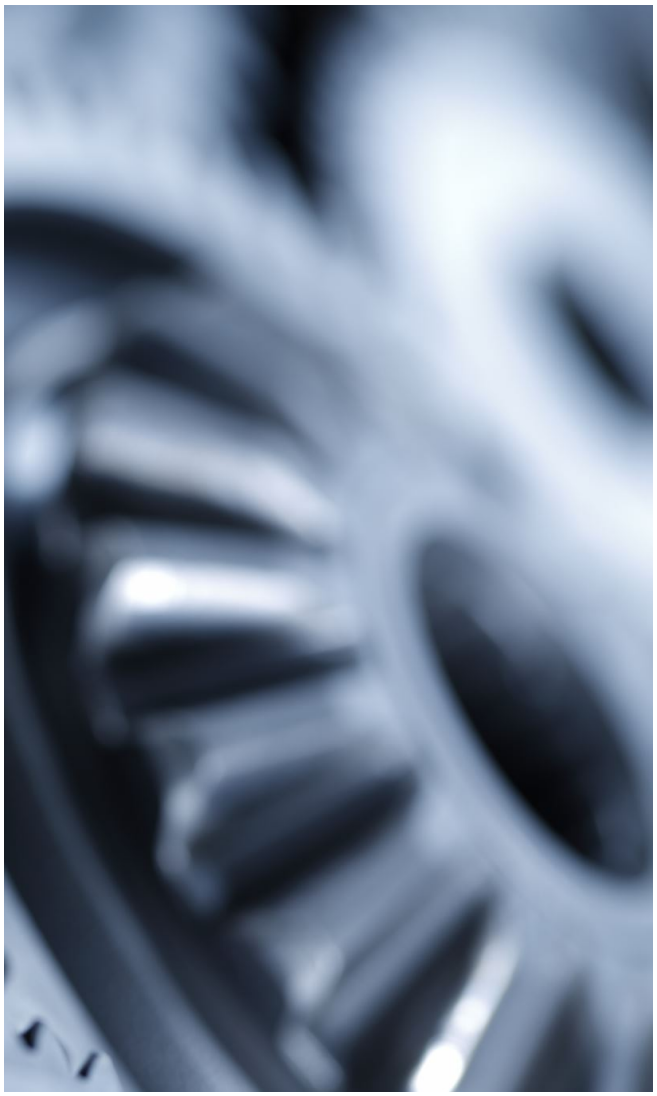
Operational Cyberpsychology: Adapting a Special Operations Model for Cyber Operations



JUNE 2021

STRATEGIC MULTILAYER ASSESSMENT

Author:
Jason A. Spitaletta, PhD, Johns Hopkins University Applied Physics Laboratory

Series Editor: Ali Jafri, NSI Inc.

Jason A. Spitaletta, PhD, Johns Hopkins University

Applied Physics Laboratory; MAJ, USMCR

Jason Spitaletta is a Major in the US Marine Corps Reserve (USMCR) and an operational psychologist with primary research experience in applied, experimental, political psychology, and cognitive neuroscience, as well as operational experience in Psychological Operations (PSYOP)/Military Information Support Operations (MISO) and intelligence assignments in the US Marine Corps and Joint and Special Operations communities. He has deployed to the Western Pacific, Iraq, and Uganda. In civilian life, he is a researcher at Johns Hopkins University Applied Physics Laboratory, as well as an adjunct faculty member at National Intelligence University and The Catholic University of America. He holds a bachelors' degree in biochemistry from Franklin & Marshall College, a master's degree in human factors from Embry-Riddle Aeronautical University, and a master's degree and PhD in applied experimental psychology from The Catholic University of America. He also holds a graduate certificate from Stanford University's Summer Institute for Political Psychology.

Operational Cyberpsychology: Adapting a Special Operations Model for Cyber Operations

Jason A. Spitaletta, PhD, Johns Hopkins University Applied Physics Laboratory[1]

This paper conceptualizes operational cyberpsychology as a field that supports missions intended to project power in and through cyberspace (Joint Staff, 2018) by leveraging and applying expertise in mental processes and behavior in the context of interaction amongst humans and machines (Norman, 2017). Operational psychologists can improve the effectiveness of cyber operations by contributing to (1) supporting online psychological operations (PSYOP), (2) facilitating and supporting online intelligence operations, (3) assessment and selection of personnel, (4) operationally focused mental health support, and (5) hostage negotiations (Staal & Stephenson, 2013). The US government's cyberpsychology initiative applies operational psychology to cyber operations (LaFon & Whalen, 2017) and should serve as the foundation for a broader operational cyberpsychology capability. Operational cyberpsychology can be a force multiplier for an increasingly critical operational capability in support of US national security, but its maturation will require additional resourcing to ensure that the research and development, as well as the operational integration and evaluation, are conducted with not only the appropriate understanding of the problem but also the perspective of those actively engaged in addressing it.

Introduction

Operational psychology is a "specialty within the field of psychology that applies behavioral science principles to enable key decision makers to more effectively understand, develop, target, and/or influence an individual, group or organization to accomplish tactical, operational, or strategic objectives within the domain of national security or national defense" (Staal & Stephenson, 2013, p. 97). Operational psychology is dominated by, but not exclusive to, clinical psychologists, but the specialty benefits from an array of psychological expertise ranging from social to cognitive to industrial/organizational that can contribute to a variety of mission support roles. Operational psychologists have been closely integrated into the US (and allied) special operations and intelligence communities since World War II but less so in the cyber domain[2]. While cyber operations are more

[1] *Contact Information*: Jason.Spitaletta@jhuapl.edu, Jason.A.Spitaletta@coe.ic.gov

[2] An interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers where intelligence, information, criminal, and/or military operations may be conducted (Crowther, 2017).

reliant on technology than special operations, considering the former as occurring within a set of sociotechnical systems comprised of multiple human-machine teams, the need for psychological perspectives becomes evident.

Cyberpsychology is the study of mental processes and behavior in the context of interaction and communication of both humans and machines (Norman, 2017). Operational psychologists support the employment and/or sustainment of personnel to achieve military, intelligence, and/or law enforcement objectives by leveraging and applying psychological expertise (Staal & Stephensen, 2006). This is done through (1) psychological operations (PSYOP), (2) facilitating and supporting intelligence operations by identifying enemy capabilities, personalities, and intentions, (3) assessment and selection of personnel, (4) operationally focused mental health support, and (5) hostage negotiations (Staal & Stephenson, 2013). While each of these applications are relevant to operational cyberpsychology, they require adaptation to the different requirement of the cyber domain. For example, both human source intelligence (HUMINT) support and hostage negotiations require domain specific techniques and assessment methods. This is becoming increasingly evident in ransomware negotiations (the cyber equivalent of a hostage situation (LaFon, 2021)) as the integration of technological and psychological leverage must converge.

This paper conceptualizes operational cyberpsychology as a field that supports missions intended to project power in and through cyberspace (Joint Staff, 2018) by leveraging and applying expertise in mental processes and behavior in the context of interaction amongst humans and machines (Norman, 2017). The US government's cyberpsychology initiative applies operational psychology to cyber operations (LaFon & Whalen, 2017) and should serve as the foundation for a broader operational cyberpsychology capability. The paper outlines both research and development as well as operational support concepts to make operational cyberpsychology a core capability within US cyber operations. As LaFon and Whalen (2017) indicate, much of this capability exists; it simply needs to be applied, tailored, and reinforced to better support cyber operations.

Operational Psychology Support to Cyber Influence

PSYOP has historically integrated collection and analysis methods employed in social and behavioral science to change the minds of others (Linebarger, 1954). Given the advances in cyber technology and the increasingly prominent threat of small groups and super-empowered individuals (Spitaletta, 2020), the logical medium through which to conduct influence is cyberspace (Spitaletta, 2014a). Cyber influence requires a rich contextual understanding of the conditions specific to each operating environment, as well as those key individuals whom the US would like to influence (Spitaletta, 2016). Traditionally, effective PSYOP methods were employed in political science, anthropology, sociology, and social psychology for target audience analysis, product development, and operational assessment (Phases II, IV, and VII of the doctrinal process). Synthesizing these traditional methods with recent advances in neuroscience, cyberpsychology, and captology (the study of computer assisted persuasive

technology) can result in an advanced set of personalized persuasion tactics (Spitaletta, 2013). Neuroscience and technology (neuro S/T) can further contribute to PSYOP by providing greater insight into the ability to enable access, assessment, and engagement (targeting) (Giordano, 2012a; Giordano, 2012b; Giordano, 2014) with the target audience (Giordano & Wurzman, 2011; Giordano et al., 2014; Wurzman & Giordano, 2014). Giordano's (2012a; 2012b; 2014) framework provides a useful model through which to examine the tactical utility of biopsychosocial approaches, particularly when combined with Post's (2011) concept of actor-specific tailored deterrence. The synthesis of approaches requires the fusion of scientific intelligence, technical intelligence, and academic research to develop actor-specific models that can be compared with the extant literature to develop tailored themes, messages, and delivery mechanisms (Spitaletta, 2013). Specifically employing biopsychosocial models when considering assessing and influencing (Spitaletta, 2013; Cabayan et al., 2014; Giordano, 2016; Spitaletta, 2016) can enable more precise access, assessment, and targeting (Giordano, 2012a; Giordano, 2012b; Giordano, 2014). Some of these concepts have been applied to Target Audience Analysis (TAA) previously, some with an application to an individual as a TAA (Spitaletta, 2014b).

Cyber influence requires themes, messages, and dissemination mechanisms that are specifically tailored to an individual's psychological vulnerabilities and/or susceptibilities[3] and delivered to the device at the time when the effect will be greatest (Spitaletta, 2014a). Both personalized and persuasive technologies[4] attempt to influence behavior (Berkovsky et al., 2012; Fogg, 2002). Synthesizing elements from each, in conjunction with established methods of social influence, hold potential to deter and influence in cyberspace. Contemporary microtargeting incorporates open-source aggregation to develop a demographic profile (Korolova, 2011), but few techniques take the intermediate step of creating an actor-specific model, then tailoring the message accordingly (Hirsch et al., 2012). Operational cyberpsychology can help address this capability gap by creating an actor-specific model based on social, behavioral, and/or neural target data to enable greater precision. Translating concepts from clinical psychology, such as risk factors, long used in psychology to assess the likelihood of symptom reoccurrence and/or relapse (Buckman et al., 2018), as well as dangerousness (Buchanan, 1999), may be combined with techniques from digital phenotyping (Onnela & Rauch, 2016; Insel, 2018) to provide novel remote behavioral assessment approaches (Spitaletta, 2018). Digital phenotyping uses a wide variety of data collected from smart devices to develop a rich contextual understanding of

[3] Vulnerabilities are the needs, wants, or desires that arise from the conditions within the operational environment (Spitaletta, 2013). Vulnerabilities are traditionally social but can be extended to include cognitive and neurobiological. Vulnerabilities may be exploited through both the message content, as well as the dissemination mechanism. Susceptibility is the degree to which a particular message is likely to influence a target audience (Spitaletta, 2013).

[4] Personalized technologies improve user experience by tailoring the interaction based on an individual's set of system preferences, interests, and/or other relevant data (Berkovsky et al., 2012). This approach can also be employed to change perception, objective reasoning, and behavior of a user (Spitaletta, 2013). Persuasive technologies advance personalized technologies by employing human-centered design, along with user-defined settings and social influence principles, to alter behavior (Fogg, 2002).

individual behavior in order to track markers of mental disorders (Onnela & Rauch, 2016, Insel, 2018; Stark, 2018; Birk & Samuel, 2020). These data can also include both traditional personality assessments administered online as well as derivative measures developed from online data sets (Marengo & Montag, 2020), making them well suited to remote assessment (Spitaletta, 2018) of online social movements (Spitaletta, 2020). The approach is not without technological challenges and ethical concerns (Huckvale et al., 2019), and thus greater scrutiny and additional applied research is required. However, given the degree to which contemporary conflict is facilitated through online networks (Spitaletta, 2020), the combination of psychological risk factors and digital phenotyping may be the solution to the requirement for personalized influence tactics (Spitaletta, 2013).

Since cyberspace is a sociotechnical—and thus interactive—system, and interactive influence tactics differ from traditional broadcast techniques (Guadagno & Cialdini, 2005), the target audience and/or individual becomes an active participant in the assessment process (Spitaletta, 2014a). This interaction, and the digital exhaust (McFedries, 2013) it produces, yields raw data that can be subjected to some of the aforementioned content analytic methods. Cyber influence can thus incorporate cooperative dynamics that reciprocally engage the human-computer system (Giordano & Wurzman, 2011; Howlader & Giordano, 2013; Rossi et al., 2013; Wurzman & Giordano, 2014). The same cyber technology that has increased the connectivity amongst individuals can facilitate access to a particular target. Cyber technology provides greater anonymity, lower emphasis on physical attractiveness, and greater control of the time of interaction all without geographical restrictions (Guadagno & Cialdini, 2005). In cyber influence, access must extend beyond the device to the user since the target is not only the technology but also the human-computer system, and therefore, offensive cyber operations that deter or influence need to extend beyond the technological to the biological, psychological, behavioral, and social. This requires exquisite precision (Wurzman & Giordano, 2014) to ensure positive identification of a potential target across devices (Spitaletta, 2014a). The precision is vital to both HUMINT and PSYOP executed through cyberspace.

Finally, operational cyberpsychology can contribute to the assessment and/or evaluation of cyber influence. Planning online PSYOP requires concepts of operations, specific objectives, themes to emphasize/avoid, target audiences, identifications of authorities, attribution methods, means of dissemination, funding sources, and finally, measures of effectiveness (MOE). Refining assessment criteria is the eighth and final step of target audience analysis; however, evaluation (Phase VII of the PSYOP process) can be considered a continuous task when operating in cyberspace. MOE development should provide a systematic means of assessing and reporting the impact a particular operation has on enemy and/or allied situational awareness and intentions (Seese et al., 2018) and is a task well-suited to operational psychology support. This can be accomplished not only by focusing the data collection (through intelligence, surveillance, and reconnaissance [ISR]) on factors that will indicate the extent to which the objective is being met, but also by ensuring the measures employed possess the requisite

validity (Seese et al., 2018). MOE is particularly challenging for more sensitive activities[5] where operational security requires fewer individuals being aware of the effort (Rid, 2020). Rigorous assessments feed into precision targeting, and the more rigorous the evaluative methods, the more refined predictions become during the next planning evaluation. This rigor can yield a more robust comparison with other means of offensive cyber operations to provide a commander a set of more flexible options.

The US should also invest in both academic and industrial research and development efforts in the science of persuasion. Cyberpsychology and cyberneurobiology are both interdisciplinary fields that examine the interaction of humans and emerging cyber technology; the former focuses on the psychological (cognitive, affective, behavioral) aspects while the latter concentrates on the biological (genetic, anatomical, endocrinological). Recently released white papers have suggested biopsychosocial models when considering assessing and influencing (Reynolds & Lyle, 2013; DiEuliis, Casebeer, Giordano, & Wright, 2014; Giordano, 2016; Spitaletta, 2016). Bio-psycho-social approaches can enable more precise access, assessment, and targeting (Giordano, 2012a, b, 2014). While existing neuroscience-based technology has great potential to influence and/or deter targets in cyberspace, further research will allow planners to rely upon firmly established linkages between perception and actions when developing both their intelligence requirements and the desired psychological actions and effects (Spitaletta, 2014). There are compelling findings among published cyberpsychology and neuroscience research (Frith & Frith, 2012; Kaptein et al., 2010) whose methods can be adapted and incorporated into research designs to test some of the ideas presented in recent white papers (Reynolds & Lyle, 2013; DiEuliis, Casebeer, Giordano, & Wright, 2014; Giordano, 2016; Spitaletta, 2016). The psychological theories, research, and practices that support PSYOP (to include cyber-enabled influence) are also readily applicable to HUMINT as both fundamentally entail understanding and influencing human behavior (Burkett, 2013).

Operational Psychology Contributions to Intelligence Support to Cyber Operations

Operational cyberpsychology can play a critical role in online intelligence operations, specifically in post-mission debriefing, the remote assessment of foreign leaders and human source intelligence (HUMINT). Post-mission debriefing is a standard military intelligence practice (Borum, 2006) that can be significantly improved with the integration of an operational psychologist (Kennedy & Zillmer, 2012). Cyber operations should not be any different than an infantry squad patrol or a strike/fighter sortie; there is intelligence value in what was observed from the perspective of those conducting the

[5] Sensitive Activities are planned and executed so the role of the United States government is not apparent or acknowledged publicly (Alvarez et al., 2015).

operations. The servicemember-as-sensor should be extended to cyber operations as those on the keyboards have a unique perspective on the cyber ecology from the design and functions of systems to the users. Educing the latter, particular when aided by an operational psychologist, can contribute significant intelligence value on a regular basis and should be incorporated into tactical standard operating procedures. The insight into the human factors of both adversary and friendly networks is something that requires greater attention from both operational as well as research and development organizations.

The term "human factors" has a broad set of interpretations in industry and academia, but the intelligence community considers human factors analysis (HFA) as the evaluation of psychological attributes (motivation, thinking style, beliefs, and personality), cultural attributes (values, beliefs, and norms that influence behavior), behavioral attributes (responses to context or stimuli independent of personality), and the neural correlates of those attributes in order to influence decision-making (how individuals and groups select a course of action), information flow (how individuals and groups acquire information required to make a decision), reasoning (how individual and groups process information they receive), neurobiological changes to or away from specific states, and ultimately, behavior of individuals and groups in any state or organization (Spitaletta, 2016). HFA can be subdivided into three types of assessment: group and population analysis (GPA), social network analysis (SNA), and individual and leadership analysis (I&LA).

A legacy from the former Office of Strategic Services (OSS) during World War II that is currently used by operational psychologists is a remote behavioral assessment, or the I&LA component of HFA. These approaches, largely developed in clinical, and later, political psychology, have long been used by US intelligence agencies (Spitaletta, 2018) and can be readily adapted to support cyber operations. The first remote psychological profile of a foreign leader was led by the OSS, and its target was Adolf Hitler (Langer at al., 1943). The techniques have evolved to include a variety of approaches, ranging from psycholinguistic to psychodynamic. Trait/motivational approaches rely on early psycholinguistic approaches by Weintraub (1986) and have extended to Winter's (2003) motivational analysis of political behavior, interpersonal behavioral preferences (Immelman, 2005), and Hermann's (1980) trait analysis of leadership style. Regardless of the approach, the data are collected from interviews and analyzed, or content-coded. Then, a profile is developed that can be compared with the baseline scores developed for the database of leader scores (Spitaletta, 2018). Adapting these methods to the forms of communication evidenced in online communities is not necessarily straightforward and requires research to validate whether analyzing corpora of online communications can yield the same insight that more traditional sources of data provide.

Cognitive approaches may allow for a better interpretation of online behavior. The integrative complexity approach to political personality assessment is an extension of operational code analysis as it is more rooted in cognitive psychology and social cognition than in personality psychology

(Immelman, 2005). Content analytical measures of integrative complexity can be applied to multiple forms of communication to assess the extent to which the individual can differentiate and integrate multiple perspectives on a particular issue (Simonton, 2006). Similar to the trait/motivational approaches, valid cognitive approaches would also require applied research to validate the technique for specific applications; however, the behaviors that might be subjected to such analyses may extend beyond the verbal and written, thus potentially furthering the scientific understanding of individuals remotely and developing advanced tradecraft to support cyber operations.

While psychodynamic approaches to psychotherapy are less prevalent today than in the mid-20th century, there is still potential for contemporary application to remote behavioral assessment. From Langer's team's initial work through today, remote psychodynamic assessments have been employed to determine "what makes a leader tick" (Langer et al., 1943; Murray, 1943). Post's (2010) integrated political personality is rooted in the object relations school of psychodynamic theory and entails (a) a psychobiographical discussion to put the subject's life in the appropriate political context, (b) an analysis of the individual's personality using any number of remote assessment methods (many of which are discussed in this paper), (c) the subject's worldview (an attempt to describe the contemporary operating environment from the subject's perspective), (d) leadership style or how the subject goes about his or her duties, and (e) outlook (an intelligence-based approach to assessing how the subject is likely to behave in specific, operationally-relevant, circumstances) (Post, 2010). Post's (2010) integrated political personality profiling method, while more laborious, allows for the incorporation of multiple remote assessment methods and can be readily applied in support of cyber operations.

Remote assessment methods might also be applied in support of HUMINT, specifically operational psychology support to asset validation or the process used to determine the asset authenticity, reliability, utility, suitability, and degree of control the case officer or others have (Happel et al., 2015; Wolmetz, et al., 2015). Operational psychologists are often involved in credibility assessment to include initial employee screening for specific positions as well as a variety of HUMINT tasks, including source operations, interrogation, and debriefing (Happel et al., 2015; Wolmetz et al., 2015). Credibility assessment is a vital component of asset validation, the process of determining whether a potential source has the requisite access and placement for recruitment based on specified priorities (Wolmetz et al., 2015), and remains one of primary capability gaps in the intelligence community and is thus an ongoing research topic of interest (Spitaletta et al., 2017). While HUMINT-related research can be perceived as controversial (Shumate & Borum, 2006), the IC and Department of Defense (DoD) have become reliant on technological means of collecting intelligence at the expense of HUMINT (Kaminski, 2011), and thus more resources need to be dedicated not only to developing tactically sound techniques for gaining compliance and/or educing information but also to developing evaluative frameworks to ensure those techniques are appropriately understood, trained, applied (Spitaletta et al., 2017), and ultimately extended to cyber operations.

Operational Psychology Support to Assessment and Selection of Cyber Operators

While personnel evaluation is typically a topic area within industrial/organizational psychology, much of the research on assessment and selection of special operations forces (SOF) and/or high-risk personnel is more appropriately categorized as operational psychology (Picano et al., 2006; Picano et al., 2017). While broad in scope, operational psychology places greater emphasis on human factors within complex social systems than hardware (Windle & Vallance, 1964), making it a natural fit for SOF. Assessment and selection of military personnel, particularly those in SOF, rely heavily on psychological measures (Banks, 2006 many of which involve personality and intellectual assessments that date back to the OSS during World War II (Banks, 1995; Picano et al., 2006; Picano et al.; 2017). Since Special Forces Assessment and Selection (SFAS) was established in 1988, the Army has sought to identify measures that have greater predictive validity, as well as greater efficiency (Brooks & Zazanis, 1997, Cotty et al., 2005; Faunce, 2016). The added specificity that empirically based measures provide to such specialized selection criteria has helped advance existing methods (Bartone et al., 2008; Beal, 2010). The incorporation of performance measures such as cognitive tests along with personality and intellectual assessments can provide a more comprehensive predictor of performance. Cognitive testing, in particular, presents an opportunity to develop both internally and ecologically valid, computer-based tests for prospective cyber operators.

There is a growing body of research on assessment and selection of personnel for assignment to cyber billets both in the military (Canali et al., 2017) and civilian organizations (Svenmarck, 2020). That work has included both tests of military and scientific knowledge (ability), as well as those that better determine their suitability for tasks to which the individual has heretofore not been exposed (aptitude) (Campbell et al., 2016). The latter is particularly useful for offensive cyber positions to which few might have firsthand exposure prior to seeking such an assignment (Harris, 2014). This challenge is similar to what the OSS Staff (1948) faced when developing criteria for those to be assigned to the Special Operations (SO) and Morale Operations (MO) branches. The criteria for the former focused mainly on physical fitness, intelligence, and personality assessment (including projective assessments). This was appropriate as the SO branch was composed of mostly younger males preparing to infiltrate occupied enemy territories and organize, train, equip, and employ guerrilla forces. The MO branch operated both alongside SO and in clandestine fronts outside of military chains of command, something with which the US had little experience at that time (Laurie, 1996). The OSS Staff (1948) developed a measure entitled “Propaganda Skills” where they were provided a scenario depicting enemy propaganda and asked to produce a two-minute radio advertisement and a leaflet. Given the OSS’s emphasis on psychological warfare, this test was administered to all candidates but weighted more heavily for those whose principal assignment was in MO (OSS Staff, 1948; Laurie, 1996). These types of domain-specific criteria, currently used for SOF (Cotty et al., 2005; Banks, 2006; Picano et al., 2006; Picano et al., 2017),

may be applied to cyber operations, particularly within the Military Occupational Specialties (MOS), as the field becomes increasingly technically/methodologically diverse and sophisticated.

The OSS Staff (1948) found selecting for the MO branch more challenging for numerous reasons ranging from the ignorance of the mission requirements for MO to the lack of an existing personnel pool in the US military from which to select. It was particularly difficult to predict success for individuals who might be assigned to such a team since the psychologists weren't cleared to understand the operational requirements and/or mission parameters (OSS Staff, 1948). Input from operational psychologists experienced in both assessment and selection methods and the operational conduct of cyber operations may yield more contextualized recommendations and/or refined methods to assess and select elite cyber operators.

Mental Health Support for Cyber Operations

Cyber operations do not place the same physical or psychological demands on personnel as special operations, and thus the physical requirements need not be identical. That said, there is still a requirement to maintain the physical fitness standards of one's respective service and/or agency and, more importantly, ensure the individual is physically and psychologically fit for the demands of cyber operations. The principal component of a resilient cyber system is a workforce of resilient cyber operators, and the unique demands of the cyber operations mission (Paul & Dykstra, 2017; Paul & Dykstra, 2018) may exacerbate long-recognized negative mental health ramifications (Smith et al., 1992). An increasing interest is being placed on the development and maintenance of technically-resilient systems or those sets of technologies with the capability to withstand, recover, and adapt to deliberate attempts to deny, disrupt, degrade, and/or destroy them (Kott & Linkov, 2019). Unfortunately, there hasn't been an equivalent focus on the resilience of those who operate within said systems. Psychological resilience, or the ability to persevere through and recover from the psychological and physiological effects of stress (Stanley et al., 2011), contributes to assessment and selection (Bartone et al., 2008) and should be a consideration of preventative mental health and/or training. Those mission-specific demands required tailored intervention, which should be informed by operational cyberpsychology and include presentation/training, treatment, and/or program development/management (the measures used pre/post treatment can also be incorporated into the aforementioned assessment and selection methods).

Military cyber operators tend to experience higher rates of emotional exhaustion and cynicism, increasing their risk for clinical manifestations, than their civilian counterparts (Chappelle et al., 2013). The sources of which may be attributed to rotating and/or inconsistent shift work as well as long hours that tend to decrease their time spent off-duty with family and/or exercising (Chappelle et al., 2013). These occupational stressors can exacerbate the cognitive demands placed on cyber operators while

on duty. Cyber operations require sustained attention[6] (Dykstra & Paul, 2018) and attentional ability correlates with working memory capacity[7] (Kiyonaga & Egner, 2014), which tends to deteriorate under prolonged stress (Stanley & Jha, 2009) yet responds favorably to appropriate training and/or treatment (Jha, Stanley, Kiyonaga, Wong, & Gelfand, 2010). Numerous programs have been developed to improve the fitness of elite operators (Williams et al., 2008; Kelly et al., 2013), such as the Tactical Human Optimization, Rapid Rehabilitation and Reconditioning (THOR3) Program; the Naval Special Warfare Command's Tactical Athlete Program (TAP); the US Marine Corps' High Intensity Tactical Training (HITT); and the 101st Airborne's Eagle Tactical Athlete Program (ETAP) (Sell et al., 2009a; Sell et al., 2009b). While some of these programs do include cognitive performance components, they focus primarily on physical rather than mental performance (Kelly et al., 2013; Loney, 2016), which has limited their effectiveness (Kelly et al., 2013). Approaches developed by sports psychologists can help establish individual psychological goals in support of physical, social, tactical, or other types of objectives (Turner, 2016; Loney, 2016) identified by cyber operators. Given the cognitive demands of cyber operations (Paul & Dykstra, 2017), a comparable but cyber-peculiar program should not ignore the physical, but it should place considerably more emphasis on the domain-specific cognitive requirements. As attention and working memory utilize the same neural substrate (Jha, Krompinger, & Baime, 2007; Kiyonaga & Egner, 2014) and both are necessary for sustained cyber operations, DoD's Warfighter Brain Health Initiative and Strategy, which is focused on not only the identification and treatment of brain injury but also on the neural correlates of human performance (Lee et al., 2020) should consider cyber-peculiar requirements and/or cyber operational cohorts as their strategy is implemented.

Suicide remains a clinical, scientific, and operational challenge in the US military (Bongar et al., 2017), and cyber operators are not immune. Existing suicide prevention programs are often viewed as required administrative training, typically lack long-term skill-building, and do not extend beyond the individual into the operational units. Essentially, the training lacks operational utility as it fails to convince the trainees of both the individual and unit-level effects of psychological issues. These issues encompass not only the negative states associated with the stress of their mission (Paul & Dykstra, 2018), but also the daily effects of one's psychological state on performance. Cyber operators who do not see the value of mental health are often reluctant to use traditional behavioral health resources for fear of losing their status on an operational team, or worse, being considered weak within a culture that values strength (Marcellino & Tortorello, 2014; Simons, 1998).

[6] Attention is the conscious focus on and/or prioritization of a particular task despite other distractions within a particular environment (Wikens & Hollands, 2000).

[7] Working memory is the function of actively retaining discrete pieces of information required to perform complex cognitive tasks such as reasoning, comprehension, learning, and decision-making for relatively brief durations (Wickens & Hollands, 2000). Working memory is an important component of general fluid intelligence as well as the ability to control attention (Engle, 2002).

US Special Operations Command (USSOCOM) established the Preservation of the Force and Family (POTFF) initiative that has prioritized the de-stigmatization of help-seeking behaviors by engaging operators, leaders, and their families, but the culturally-ingrained resistance has been difficult to overcome (Bongar et al., 2017). A similar program might be created for US Cyber Command (USCYBERCOM) to tailor training and management and to inform treatment of those assigned to its subordinate formation. Integrating it with the Warfighter Brain Health Initiative and Strategy will allow for both a short-term focus on human performance and a long-term focus on psychological health. These efforts should tie into the assessment and selection criteria and be combined with advances in digital health to develop a cyber-peculiar human performance program. Analysis of fitness tracking data, contextualized within baseline assessments, can yield novel psychological insights of behavior in SOF (Saxon et al., 2020) and may provide different, but equally as useful, utility to cyber operations. Programs that seek to achieve and proactively maintain good mental health, rather than allowing mental health to decline before attempting to repair it, would be particularly helpful for personnel who must maintain high performance in the face of consistent stress such as those identified by Paul and Dykstra (2017; 2018). Whatever form a program takes, it could benefit considerably from the perspective that operational cyberpsychology can provide.

Ransomware Negotiations

Ransomware negotiations are the operational cyberpsychology equivalent of a hostage situation (LaFon, 2021). Ransomware is the term for malicious code that employs encryption to prevent access to a system or files on that system until the victim either performs a service and/or pays a fee to the attacker (Maigida et al., 2019). These operations have increased significantly since the 2017 *WannaCry* and *NotPetya* attacks (Hofmann, 2020) and have become a US Department of Justice priority on par with terrorism (Bing, 2021). The increased prevalence has led to a cottage industry of ransomware negotiation firms as well as technological (Tan et al., 2020) and ethical (Hofmann, 2020) considerations. Specific operational cyberpsychology tradecraft has yet to emerge, but proven tactics from hostage negotiation research and practice may be adapted, validated, and ultimately applied.

Ransomware negotiations can benefit from both collaborative and adversarial approaches to operational psychology with the former focusing on optimizing personnel performance in high-risk operations and the latter on facilitating deceptive and coercive operations (Arrigo et al., 2012). Hatcher and colleagues (1998) identify four roles for operational psychologists in hostage negotiations: (a) the consultant/advisor, (b) the integrated teammate, (c) the primary negotiator, and (d) the primary controller. The consultant/advisory role is one where operational psychology can contribute to the assessment and selection of hostage negotiators, negotiation planning, and/or post mission debriefs. This role, while collaborative, is not without ethical challenges, as there is often a preference for a single psychologist to serve as both a planner and a debriefer; however, that presents some ethical challenges and thus is not recommended (Kennedy & Williams, 2011). The other roles provide opportunities for both collaborative and coercive support with the expert determining which is appropriate, given a

particular situation. Much like operational psychologists who support elite law enforcement organizations, the operational cyberpsychologist must not only be proficient in his/her scientific field but also sufficiently familiar with the technology and tactics that are employed in such situations. Conceptualizing the tradespace as an interactive, sociotechnical system, ransomware negotiation is a combination of technological and/or psychological tactics to produce a specific behavior. This necessitates an understanding of the psyches of malware creators, cyber criminals, and victims, along with the technological means by which the malware is delivered and/or removed.

There is scant literature on the psychology of ransomware negotiations, but unfortunately, as the problem continues to evolve and adapt, there will be plenty of opportunities to study and learn from these events. Operational cyberpsychological considerations should be included among the cybersecurity, counterintelligence, and/or physical security concerns of such events, as well the concomitant research and development. Ransomware negotiation is an emerging priority area for operational psychologists supporting cyber operations.

Conclusion

This paper conceptualizes operational cyberpsychology as a field that supports missions intended to project power in and through cyberspace (Joint Staff, 2018) by leveraging and applying expertise in mental processes and behavior in the context of interaction amongst humans and machines (Norman, 2017). Operational psychologists can improve the effectiveness of cyber operations by contributing to: (a) online PSYOP, (b) the facilitation and support of online intelligence operations, (c) the assessment and selection of cyber personnel, (d) operationally-focused mental health support, and (5) hostage negotiations (Staal & Stephenson, 2013). Operationalizing the concepts described herein may require a cultural shift within the cyber operational formations; however, a reasonable blueprint does exist but needs to be adapted from SOF and/or the IC and appropriately applied.

The psychological theories, research, and practices that support HUMINT are also readily applicable to PSYOP, as both fundamentally entail understanding and influencing human behavior (Burkett, 2013). HUMINT and PSYOP through cyberspace must extend access beyond the device to the user, and therefore, offensive cyber operations that deter or influence need to extend beyond the technological to the biological, psychological, behavioral, and social and require exquisite precision (Wurzman & Giordano, 2014) to ensure positive identification of a potential target across devices (Spitaletta, 2014a). The precision is vital to both HUMINT and PSYOP executed through cyberspace and thus can benefit from additional research, application, and/or evaluation from emerging sociotechnical approaches developed for clinical applications, such as digital phenotyping (Insel, 2018; Stark, 2018; Birk & Samuel, 2020; Marengo & Montag, 2020), to address the requirement for personalized influence tactics (Spitaletta, 2013).

The criticality of cyber operations, particularly at the national level (Gilad et al., 2021), necessitates an assessment and selection program. The body of research on the assessment and selection of personnel for assignment to cyber billets (Harris, 2014; Campbell et al., 2016; Canali et al., 2017; Svenmarck, 2020) needs to be expanded, tested, and evaluated. Input from operational psychologists experienced in both assessment and selection methods and the operational conduct of cyber operations may yield more contextualized recommendations and/or refined methods to assess and select elite cyber operators.

Resilient cyber systems require resilient cyber operators who can thrive amidst the unique operational and mental demands of the cyber domain (Paul & Dykstra, 2017; Paul & Dykstra, 2018). Programs that seek to achieve and proactively maintain good mental health, rather than allowing mental health to decline before attempting to repair it, would be particularly helpful for personnel who must maintain high performance in the face of consistent stress, such as those identified by Paul and Dykstra (2017; 2018). Cyber operations require sustained attention (Dykstra & Paul, 2018) and attentional ability correlates with working memory capacity (Kiyonaga & Egner, 2014), which tends to deteriorate under prolonged stress (Stanley & Jha, 2009) yet responds favorably to appropriate training and/or treatment (Jha et al., 2010). A translational approach whereby effective treatments are integrated into training may provide both a protective effect from psychological injuries (Bongar et al., 2017) and improve performance, an objective consistent with those of DoD's Warfighter Brain Health Initiative and Strategy (Lee et al., 2020).

Ransomware negotiations are the operational cyberpsychology equivalent of a hostage situation (LaFon, 2021) and afford the opportunity to apply both collaborative and adversarial approaches, depending on the specific role of the operational psychologist (Arrigo et al., 2012). There is scant literature on the psychology of ransomware negotiations, but unfortunately, as the problem continues to evolve and adapt, there will be plenty of opportunities to study and learn from these events. Ransomware negotiation should be a research and development priority for operational psychologists supporting cyber operations.

The US government's cyberpsychology initiative applies operational psychology to cyber operations (LaFon & Walen, 2017) and should serve as the foundation for a broader operational cyberpsychology capability. Operational cyberpsychology can be a force multiplier for an increasingly critical operational capability in support of US national security, but its maturation will require additional resourcing to ensure the research and development, as well as the operational integration and evaluation, are conducted with not only the appropriate understanding of the problem but also the perspective of those actively engaged in addressing it.

References

Alvarez, J., Nalepa, R., Wyant, A. M., & Zimmerman, F. (2015). *Special Operations Forces reference manual*. MacDill AFB, FL: Joint Special Operations University Press.

Arrigo, J. M., Eidelson, R. J., & Bennett, R. (2012). Psychology under fire: Adversarial operational psychology and psychological ethics. Peace and Conflict: Journal of Peace Psychology, 18(4), 384.

Banks, L. M. (1995). The Office of Strategic Studies psychological selection program (Accession No. ADA299376) [Master's thesis, Army Command and General Staff College]. Master's thesis collection 2 Aug 94-2 Jun 95.

Banks, L. M. (2006). The history of special operations psychological selection. In D. A. Mangelsdorff (Ed.), *Psychology in the service of national security* (pp. 83-95). Washington, DC: American Psychological Association.

Bartone, P. T., Roland, R. R., Picano, J. J., & Williams, T. J. (2008, January 25). Psychological hardiness predicts success in US Army Special Forces candidates. *International Journal of Selection and Assessment, 16*(1), 78-81.

Beal, S. A. (2010). The roles of perseverance, cognitive ability, and physical fitness in the U.S. Army Special Forces assessment and selection (Research report 1927). U.S. Army Research Institute for the Behavioral and Social Sciences.

Berkovsky, S., Freyne, J., & Oinas-Kukkonen, H. (2012). Influencing individually: Fusing personalization and persuasion. *ACM transactions on interactive intelligent systems*, *2*(2), Article 9.

Bing, C. (2021). Exclusive: U.S. to give ransomware hacks similar priority as terrorism. *Reuters*. https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/

Birk, R., & Samuel, G. (2020). Can digital data diagnose mental health problems? A sociological exploration of 'digital phenotyping.' *Sociology of Health & Illness*, *42*(8), 1873-1887.

Bongar, B., Maslowski, K., Hausman, C., Spangler, D., & Vargo, T. (2017). The problem of suicide in the United States Special Operations Forces. In B. Bongar, G. Sullivan, & L. James (Eds.), *Handbook of military and veteran suicide: Assessment, treatment, and prevention*. New York, NY: Oxford University Press.

Borum, R. (2006). Approaching truth: Behavioral science lessons on educing information from human sources. In N. D. I. College (Ed.), *Educing Information* (pp. 17-43). Washington, DC: NDIC Press.

Brooks, J. E., & Zazanis, M. M. (1997). Enhancing U.S. Army Special Forces: Research and applications. In *ARI Special Report, 33*. Alexandria, VA: U.S. Army Research Institute for the Behavioral and Social Sciences.

Buchanan, A. (1999). Risk and dangerousness. *Psychological Medicine*, *29*(2), 465-473.

Buckman, J. E. J., Underwood, A., Clarke, K., Saunders, R., Hollon, S. D., Fearon, P., & Pilling, S. (2018). Risk factors for relapse and recurrence of depression in adults and how they operate: A four-phase systematic review and meta-synthesis. *Clinical Psychology Review, 64*, 13-38.

Burkett, R. (2013). An alternative framework for agent recruitment: From MICE to RASCLS. *Studies in Intelligence*, *57*(1), 7-17.

Cabayan, H., DiEuliis, D., Casebeer, W., Giordano, J., & Wright, N. (Eds.), (2014). Leveraging neuroscientific and neurotechnological (NeuroS&T) developments with focus on influence and deterrence in a networked world [White paper]. Department of Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.

Campbell, S. G., Saner, L. D., & Bunting, M. F. (2016). Characterizing cybersecurity jobs: Applying the cyber aptitude and talent assessment framework. In *Proceedings of the Symposium and Bootcamp on the Science of Securit*y, 25-27.

Canali, K. G., Wind, A. P., & Willford, J. C. (2017). *Cyber selection test research effort for U.S. Army new accessions*. Fort Belvoir, VA: Army Research Institute for the Behavioral and Social Sciences.

Chappelle, W., McDonald, K., Christensen, J., Prince, L., Goodman, T., Thompson, W., & Hayes, W. (2013). *Sources of occupational stress and prevalence of burnout and clinical distress among US Air Force Cyber Warfare Operators*. School of Aerospace Medicine Wright Patterson AFB OH. https://apps.dtic.mil/sti/pdfs/ADA584653.pdf

Cotty, W., Bluestein, B., & Thompson, J. (2005). The whole-man concept: Assessing the SF soldier of the future. *Special Warfare, 17*(4), 18-21.

Crowther, G. (2017). The cyber domain. *The Cyber Defense Review, 2*(3), 63-78. http://www.jstor.org/stable/26267386

DiEuliis, D., Casebeer, W., Giordano, J., Wright, N. & Cabayan, H. (Eds.)(2014). *White paper on Leveraging Neuroscientific and Neurotechnological (NeuroS&T) Developments with Focus on Influence and Deterrence in a Networked World*. Department of Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.

Dykstra, J., & Paul, C. L. (2018). Cyber operations stress survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations. https://www.usenix.org/system/files/conference/cset18/cset18-paper-dykstra.pdf

Faunce, J. (2016). A history of assessment and selection. *Special Warfare, 29*(2), 12-18.

Fogg, B. J. (2002). Persuasive technology: Using computers to change what we think and do. Palo Alto, CA: Morgan Kaufmann.

Frith, C. D., & Frith, U. (2012). Mechanisms of social cognition. *Annual review of psychology*, *63*, 287-313.

Gilad, A., Pecht, E., & Tishler, A. (2021). Intelligence, Cyberspace, and National Security. *Defence and Peace Economics*, *32*(1), 18-45.

Giordano J. (2012a). Use of neuroscience and technology (neuro S/T) to affect human decision-making: Implications for neuro-ecology. Department of Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.

Giordano, J. (2012b). Neurotechnology as demiurgical force: Avoiding Icarus' folly. In J. Giordano (Ed.), *Neurotechnology: Premises, potential and problems* (pp. 1-14). Boca Raton, FL: CRC Press.

Giordano, J. (2012c). Integrative convergence in neuroscience: Trajectories, problems and the need for a progressive neurobioethics. In A. Vaseashta, E. Braman, & P. Sussman (Eds.), *Technological innovation in sensing and detecting chemical, biological, radiological, nuclear threats and ecological terrorism (NATO science for peace and security series A: Chemistry and biology)*. Springer.

Giordano J. (Ed.). (2014). Neurotechnology in national security and defense: Practical considerations, neuroethical concerns. Boca Raton, FL: CRC Press.

Giordano, J. (2016). A Biopsychosocial Approach to Understanding and Mitigating Aggression and Violence: Groundwork for Operationalization of New Tools and Methods. In J. Spitaletta (Ed.) (2016). *Bio-psycho-social applications to cognitive engagement* [White paper]. Department of

Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.
Giordano, J., Kulkarni, A., & Farwell, J. (2014). Deliver us from evil? The temptation, realities and neuroethico-legal issues of employing assessment neurotechnologies in public safety initiatives. *Theoretical Medicine and Bioethics, 35*(1), 73-89.
Giordano, J., & Wurzman R. (2011). Neurotechnology as weapons in national intelligence and defense. *Synesis, 2*(2), 138-151.
Guadagno, R., & Cialdini, R. (2005). Online persuasion and compliance: Social influence on the Internet and beyond. In Y. Amichai-Hamburger (Ed.), *The social net: Understanding human behavior in cyberspace*. Oxford University Press.
Happel, M. D., Spitaletta, J. A., Hwang, G. W., & Wolmetz, M. (2015). *Detecting deception and concealed information: Evaluation of the state of the practice (REDD-2015-532).* Laurel, MD: Johns Hopkins University Applied Physics Laboratory.
Harris, S. (2014). *@War: The rise of the military-internet complex*. Houghton Mifflin Harcourt.
Hatcher, C., Mohandie, K., Turner, J., & Gelles, M. G. (1998). The role of the psychologist in crisis/hostage negotiations. *Behavioral sciences & the law*, *16*(4), 455-472.
Headquarters, Department of the Army. (2005). *Field Manual 3-05.3 Psychological Operations*. Washington, DC: Department of the Army.
Hermann, M. G. (1980). Explaining foreign policy behavior using the personal characteristics of political leaders. *International Studies Quarterly*, *24*(1), 7-46.
Hirsch, J. B., Kang, S. K., & Bodenhausen, G. V. (2012). Personalized persuasion: Tailoring persuasive appeals to recipients' personality traits. *Psychological Science, 23*(8), 1-4.
Hofmann, T. (2020). How organisations can ethically negotiate ransomware payments. *Network Security*, *2020*(10), 13-17.
Howlader, D., & Giordano, J. (2013). Advanced robotics: Changing the nature of war and thresholds and tolerance for conflict – implications for research and policy. *J Phil Sci Law, 13*(2), 1-19.
Huckvale, K., Venkatesh, S., & Christensen, H. (2019). Toward clinical digital phenotyping: A timely opportunity to consider purpose, quality, and safety. *NPJ digital medicine*, *2*(1), 1-11.
Immelman, A. (2005). Political psychology and personality. In S. Strack (Ed.), *Handbook of personology and psychopathology* (pp. 198-225).
Insel, T. R. (2018). Digital phenotyping: A global tool for psychiatry. *World Psychiatry*, *17*(3), 276.
Jha, A.P., Krompinger, J., & Baime, M.J. (2007). Mindfulness training modifies subsystems of attention. *Cognitive, Affective & Behavioral Neuroscience, 7*(2), 109-119.
Jha, A.P., Stanley, E.A., Kiyonaga, A., Wong, L.,& Gelfand, L. (2010). Examining the protective effects of mindfulness training on working memory capacity and affective experience. *Emotion, 10* (1), 54-64.
Joint Staff. (2006). Joint Publication 3-13: Joint Doctrine for Information Operations. Joint Warfighting Center Doctrine Division: Fort Monroe, VA
Joint Staff. (2018). *Joint Publication 3-12: Cyberspace Operations*. Joint Warfighting Center Doctrine Division: Fort Monroe, VA
Kaminski, P. (2011). Report of the Defense Science Board Task Force on defense intelligence counterinsurgency (COIN) intelligence, surveillance, and reconnaissance (ISR) operations. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics. https://dsb.cto.mil/reports/2010s/ADA543575.pdf

Kaptein, M. C., Markopoulos, P., de Ruyter, B., & Aarts, E. (2010). Persuasion in ambient intelligence. *Journal of Ambient Intelligence and Humanized Computing, 1*(1), 43-56.

Kelly, T. K., Masi, R., Walker, B., Knapp, S., & Leuschner, K. J. (2013). An assessment of the Army's tactical human optimization, rapid rehabilitation and reconditioning program. Santa Monica, CA: RAND Corporation.

Kennedy, C. H., & Williams, T. J. (Eds.), (2011). *Ethical practice in operational psychology: Military and national intelligence applications* (pp. xiv-154). American Psychological Association.

Kennedy, C. H., & Zilmer E.A. (2012). *Military psychology: Clinical and operational applications, 2nd Ed*. New York: Guilford Press.

Kiyonaga, A., & Egner, T. (2014). The working memory Stroop effect when internal representations clash with external stimuli. *Psychological Science*, 0956797614536739.

Korolova, A. (2011). Privacy violations using microtargeted ads: A case study. *Journal of Privacy and Confidentiality, 3*(1), 27-49.

Kott, A., & Linkov, I. (Eds.), (2019). *Cyber resilience of systems and networks* (pp. 381-401). Springer International Publishing.

LaFon, D. (2021). Personal communication.

LaFon, D., & Whalen, G. (2017). Leveraging human science in an information operations environment: An age old use of bio-psycho-social sciences in a new era. In J. A. Spitaletta (Ed.), *Bio-psycho-social applications to cognitive engagement.* Department of Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.

Langer, W. C., Murray, H. A., Kris, E., & Lawin, B.A. (1943). *A psychological analysis of Adolph Hitler: His life and legend*. Washington, DC: Office of Strategic Services.

Laurie, C. D. (1996). The propaganda warriors: America's crusade against Nazi Germany. University Press of Kansas.

Linebarger, P. M. A. (1954). *Psychological warfare (2nd ed.)*. Washington, DC: Combat Forces Press.

Lee, K. M., Khatri, T. L., & Fudge, E. R. (2020). US Department of Defense Warfighter Brain Health Initiative: maximizing performance on and off the battlefield. *Journal of the American Association of Nurse Practitioners*, *32*(11), 720-728.

Loney, B. (2016). Initiating mental performance programming with Army Special Operations Forces Operators. In J. G. Cremades & L. S. Tashman (Eds.), *Global practices and training in applied sport, exercise, and performance psychology: A case study approach*. New York: Psychology Press.

Maigida, A. M., Olalere, M., Alhassan, J. K., Chiroma, H., & Dada, E. G. (2019). Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms. *Journal of Reliable Intelligent Environments*, *5*(2), 67-89.

Marcellino, W. M., & Tortorello, F. (2014). "I don't think I would have recovered": A personal and sociocultural study of resilience among U.S. Marines. *Armed Forces & Society, 40*(3), 1-23.

Marengo, D., & Montag, C. (2020). Digital phenotyping of big five personality via Facebook data mining: A meta-analysis. *Digital Psychology*, *1*(1), 52-64.

McFedries, P. (2013). Tracking the quantified self. *IEEE Spectrum, 50*(8), p. 24.

Murray, H. A. (1943). Analysis of the personality of Adolf Hitler: With predictions of his future behavior and suggestions for dealing with him now and after Germany's surrender. Harvard Psychological Clinic.

Norman, K. L. (2017). Cyberpsychology: An introduction to human-computer interaction. Cambridge University Press.

Onnela, J. P., & Rauch, S. L. (2016). Harnessing smartphone-based digital phenotyping to enhance behavioral and mental health. *Neuropsychopharmacology*, *41*(7), 1691-1696.

OSS Assessment Staff. (1948). Assessment of men: Selection of personnel for the Office of Strategic Services. New York, NY: Rinehart.

Pacepa, I. M., & Rychlak, R. J. (2013). Disinformation: Former spy chief reveals secret strategy for undermining freedom, attacking religion, and promoting terrorism. Washington, DC: WND Books.

Paul, C. L., & Dykstra, J. (2017). Understanding operator fatigue, frustration, and cognitive workload in tactical cybersecurity operations. *Journal of Information Warfare*, *16*(2), 1-11.

Paul, C. L., & Dykstra, J. (2018). Stress & hacking. National Security Agency Central Security Service. https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/1606258/measuring-stress-in-a-high-risk-environment/

Picano, J. J., Williams, T. J., & Roland, R. R. (2006). Assessment and selection of high-risk operational personnel. In C. H. Kennedy & E. A. Zilmer (Eds.), *Military psychology: Clinical and operational applications*. New York, NY: Guilford Press.

Picano, J. J., Williams, T. J., Roland, R. R., & Bartone, P. T. (2017). Assessment of elite operational personnel. In S. V. Bowles & P. T. Bartone (Eds.), *Handbook of military psychology: Clinical and organizational practice*. Washington, DC: Springer Books.

Post, J. M. (Ed.). (2010). The psychological assessment of political leaders: With profiles of Saddam Hussein and Bill Clinton. Ann Arbor, MI: University of Michigan Press.

Post, J. M. (2011). Actor-specific behavioral models of adversaries: A key requirement for tailored deterrence. In B. R. Schneider & P. D. Ellis (Eds.), *Tailored deterrence: Influencing states and groups of concern.* Maxwell Air Force Base, AL: U.S. Air Force Counterproliferation Center.

Reynolds, M. & Lyle, D. (Eds.) (2013). Topics for Operational Considerations: Insights from Neurobiology & Neuropsychology on Influence and Extremism—An Operational Perspective. Department of Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.

Rossi, J., Novotny, P., Paulick, P., Plischke, H., Kohls, N. B., & Giordano J. (2013). Decision technologies: Engineering capabilities and neuroethical considerations. *Ethics in Biology, Engineering and Medicine, 6*(4), 6-17.

Saxon, L., DiPaula, B., Fox, G. R., Ebert, R., Duhaime, J., Nocera, L., Tran, L., & Sobhani, M. (2020). Continuous measurement of reconnaissance Marines in training with custom smartphone app and watch: Observational cohort study. *JMIR mHealth and uHealth*, *8*(6):e14116.

Shumate, S., & Borum, R. (2006). Psychological support to defense counterintelligence operations. *Military Psychology*, *18*(4), 283-296.

Simons, A. (1998). How ambiguity results in excellence: The role of hierarchy and reputation in U.S. Army Special Forces. *Human Organization*, *57*(1), 117-123.

Simonton, D. K. (2006). Presidential IQ, openness, intellectual brilliance, and leadership: Estimates and correlations for 42 U.S. chief executives. *Political Psychology, 27*(4), 511-526.

Seese, G., Linera, R., & McQuagge, E. (2018). Effects-based psychological operations measures of effectiveness: Measuring change and impact. In M. Yager (Ed.), What do others think and how do we know what they are thinking? [White paper]. Department of Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.

Sell, T. C., Abt, J. P., Crawford, K., Lovalekar, M., Nagai, T., Deluzio, J. B., Smalley, B. W., McGrail, M. A., Rowe, R. S., Cardin, S., & Lephart, S. M. (2009a). Warrior model for human performance

and injury prevention: Eagle tactical athlete program (ETAP) part I. *Journal of Special Operations Medicine*, *10*(4), 2-21.

Sell, T. C., Abt, J. P., Crawford, K., Lovalekar, M., Nagai, T., Deluzio, J. B., Smalley, B. W., McGrail, M. A., Rowe, R. S., Cardin, S., & Lephart, S. M. (2009b). Warrior model for human performance and injury prevention: Eagle tactical athlete program (ETAP) part II. *Journal of Special Operations Medicine, 10*(4), 22-33.

Smith, M. J., Carayon, P., Sanders, K. J., Lim, S. Y., & LeGrande, D. (1992). Employee stress and health complaints in jobs with and without electronic performance monitoring. *Applied Ergonomics*, *23*(1), 17-27.

Spitaletta, J. (2013). Neuropsychological operations: A concept for counter-radicalization. In M. Reynolds & D. Lyle (Eds.), Topics for operational considerations: Insights from neurobiology & neuropsychology on influence and extremism—An operational perspective. Department of Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.

Spitaletta, J. A. (2014a). Use of cyber to affect neuroS/T based deterrence and influence. In D. DiEuliis, W. Casebeer, J. Giordano, N. Wright, & H. Cabayan (Eds.), Leveraging neuroscientific and neurotechnological (neuroS&T) developments with focus on influence and deterrence in a networked world [White paper]. Department of Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.

Spitaletta, J. A. (2014b). Leadership Trait Analysis. In H. Cabayan & N. Wright (Eds.), A multi-disciplinary, multi-method approach to leader assessment at a distance: The case of Bashar Al-Assad parts I & II. Department of Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.

Spitaletta, J. A. (2014c). Comparative psychological profiles: Baghdadi & Zawahiri. In H. Cabayan & S. Canna (Eds.), *Multi-method assessment of ISIL*. Department of Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.

Spitaletta, J. A. (2015). Terror as a psychological warfare objective: ISIL's use of ritualistic decapitation. In J. Giordano & D. DiEuliis (Eds.), *Social and* cognitive neuroscience underpinnings of ISIL behavior and implications for strategic communication, messaging, and influence [White paper]. Department of Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.

Spitaletta, J. A. (Ed.). (2016). *Bio-psycho-social applications to cognitive engagement* [White paper]. Department of Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.

Spitaletta, J. (2018). Remote behavioral assessment: Political psychology methods. In M. Yager (Ed.), *What do others think and how do we know what they are thinking?* [White paper]. Department of Defense; Strategic Multilayer Assessment Group- Joint Staff/J-3/Pentagon Strategic Studies Group.

Spitaletta, J., Greenberg, A., Bos, N., & Kopecky, J. (2017). *The role of test and evaluation in intelligence community sponsored social and behavioral science research*. Submitted to the Committee on a Decadal Survey of Social and Behavioral Sciences and Applications to National Security, National Academies of Sciences, Engineering, and Medicine. http://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_177316.pdf

Spitaletta, J., Seese, G., & McCulloh, I. (2017). The need for intelligence community sponsored influence research. Submitted to the Committee on a Decadal Survey of Social and Behavioral Sciences for Applications to National Security, National Academies of Sciences, Engineering, and Medicine. http://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_177316.pdf

Spitaletta, J. A. (2020). Human factors considerations of undergrounds in cyber resistance. In K. Ryan (Ed.), *Resistance and the cyber domain*. Fort Bragg, NC: U.S. Army Special Operations Command.

Staal, M. A., & Stephenson, J. A. (2006). Operational psychology: An emerging subdiscipline. *Military Psychology*, *18*(4), 269-282.

Staal, M. A., & Stephenson, J. A. (2013). Operational psychology post-9/11: A decade of evolution. *Military Psychology, 25*(2), 93-104.

Stanley, E.A., & Jha, A.P. (2009) Mind fitness: Improving operational effectiveness and building warrior resilience. *Joint Forces Quarterly, 55,* 144-151.

Stanley, E. A., Schaldach, J. M., Kiyonaga, A., & Jha, A. P. (2011). Mindfulness-based mind fitness training: A case study of a high-stress predeployment military cohort. *Cognitive and Behavioral Practice*, *18*(4), 566-576.

Svenmarck, P. (2020). Recruitment, selection and training of IT/cyber personnel. In *Human Systems Integration Approach to Cyber Security* (TR-HFM-259), 6-1–6-8. NATO Science and Technology Organization.

Tan, M. K. S., Goode, S., & Richardson, A. (2020). Understanding negotiated anti-malware interruption effects on user decision quality in endpoint security. *Behaviour & Information Technology*, 1-30.

Turner, M. J. (2016). Rational emotive behavior therapy (REBT), irrational and rational beliefs, and the mental health of athletes. *Frontiers in psychology, 7*, 1-16.

Weintraub, W. (1986). Personality profiles of American presidents as revealed in their public statements: The presidential news conferences of Jimmy Carter and Ronald Reagan. *Political Psychology*, *7*(2), 285-295.

Wickens, C.D. & Hollands, J.G. (2000). *Engineering psychology and human performance, 3rd ed.* Upper Saddle River, NJ: Prentice Hall.

Williams, E., Abarbanel, D., Brenner, M., Despain, A., Drell, S., Dyson, F., Joyce, G., Lewis, N., Press, W., Vesecky, J., & Woodin, H. (2008). *Human performance.* Washington, DC: Office of Defense Research and Engineering.

Windle, C., & Vallance, T. R. (1964). The future of military psychology: Paramilitary psychology. *American Psychologist, 19*(2), 119-129.

Winter, D. G. (2003). Personality and political behavior. In D. O. Sears, L. Huddy, & R. Jervis (Eds.), *Oxford handbook of political psychology* (pp. 110-145). New York, NY: Oxford University Press.

Wolmetz, M., Pohlmeyer, E. A., Spitaletta, J. A., Scholl, C. A., Greenberg, A. M., Hwang, G. W., & Happel, M. D. (2015). *Detecting deception and concealed information: Evaluation of the state of the art* (REDD-2015-533). Laurel, MD: Johns Hopkins University Applied Physics Laboratory.

Wurzman, R., & Giordano, J. (2014). *"*NEURINT" and neuroweapons: Neurotechnologies in national intelligence and defense. In J. Giordano (Ed.), *Neurotechnology in national security: Technical considerations, neuroethical concerns.* Boca Raton, FL: CRC Press.