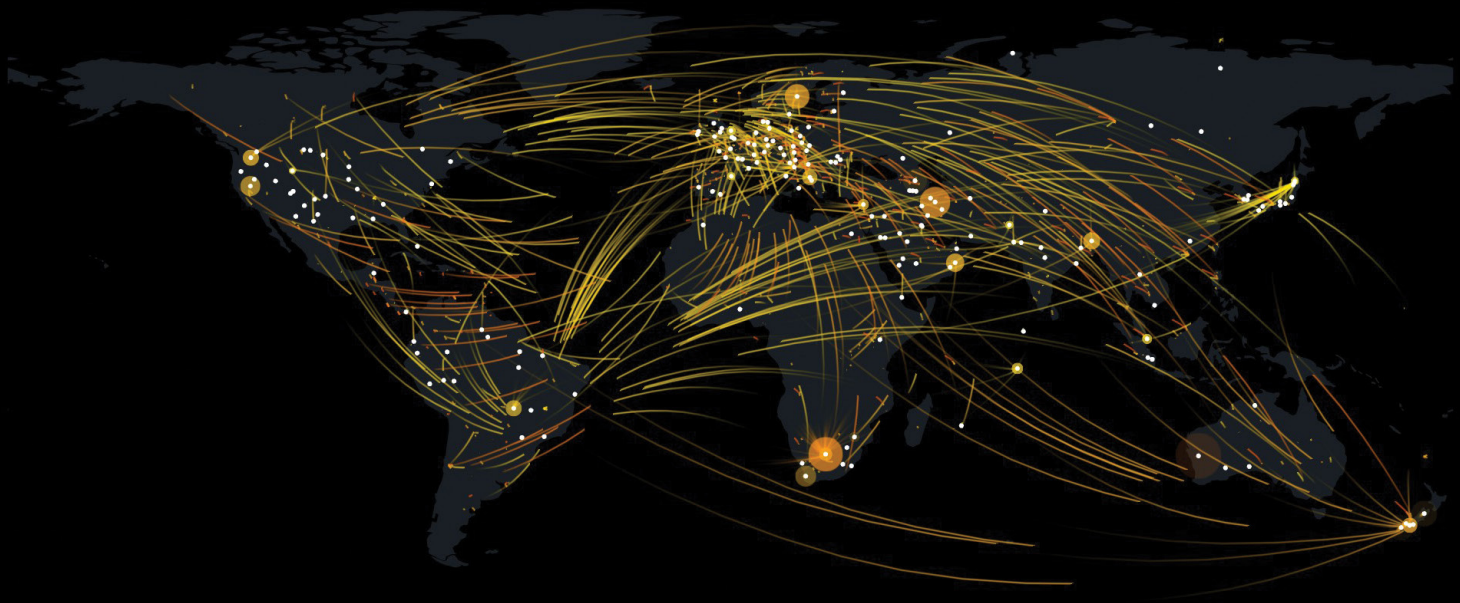

Cyber Considerations of a Resistance Operating Concept

The Subversive Potential of Persuasive Technology

Jason A. Spitaletta, PhD
Maj. Michael B. Matthaeus, U.S. Army
Michael Guadian

Taken 14 November 2024 at 14:44 (UTC -1hr), this NETSCOUT map is displaying real-time distributed denial of service attacks across the globe. Hundreds of attacks are actively occurring almost every minute of the day. (Screenshot from NETSCOUT Cyber Threat Horizon)

The maze of war psychology has not been illuminated yet by scientific knowledge, and therefore strategists make their way blindly in the dark.

—Evgeny E. Messner

Military policy, doctrine, and logic require a collective understanding of the type of conflict in which the joint force is operating.[1] Evgeny Messner's concept of subversion war is an appropriate theoretical framework to comprehend the contemporary operational environment defined by great power competition (GPC) amidst innumerable irregular conflicts, both civil and transregional.[2] A particularly prescient component of Messner's subversion war is the "vulgarization" of conflict, which includes working by, with, and through resistance movements to subvert the political status quo.[3] Initiating, co-opting, or even fabricating resistance movements through cyberspace has been operationalized by Iran, China, Russia, North Korea, and nonstate actors to achieve strategic advantage.[4] Those efforts have transformed cyberspace into the preeminent domain through which Messner's concepts can be applied. The blueprint developed by Messner during the Cold War is evident in contemporary GPC, including the enduring relevance of resistance warfare within the U.S. *National Security Strategy*.[5] The United States should not only understand but also operationalize its version of subversive resistance warfare in cyberspace through an updated *Resistance Operating Concept* as a component of a national cyber strategy.

Operationalizing the competencies necessary to formalize and implement a subversive cyber strategy requires themes, messages, and dissemination mechanisms specifically tailored to an individual's psychological vulnerabilities and/or susceptibilities and delivered when the effect will be greatest. Therefore, among the capability requirements is psychological targeting, a set of processes that combines two interrelated facets: the automated assessment of psychological states and/or traits from digital footprints (psychological profiling) and the development and implementation of content to shape perception, objective reasoning, and behavior (psychologically informed interventions).[6] The cyber domain affords the opportunity to apply psychological targeting to conduct precise engagements at scale, not simply mass persuasion, contributing to the subversive nature of cyberspace operations.[7] The associated psychological targeting research, discussed later, is the centerpiece of the argument for greater special operations forces (SOF) and Cyber Mission Force (CMF) integration from training to education to operations to strategy.

This article (1) contextualizes the role of persuasive technology in resistance warfare, (2) identifies and describes the relevant concepts, (3) articulates training and education requirements, (4) suggests potential research collaborations for SOF and CMF students, and (5) suggests a strategic manifestation of those concepts.

Resistance Warfare and Persuasive Technology: Contextualizing the Problem

Resistance warfare is predominantly a fight for influence, waged in complex human environments using traditional and nontraditional means to achieve strategic advantage.[8] Cyberspace is such a complex human environment, and one that is becoming increasingly vital to resistance warfare.[9] The convergence of accessible technology, a social trend toward increased online sharing, and the ability to organize virtually and share experiences in real time via social media have

Jason Spitaletta, PhD, is an operational psychologist and an adjunct professor at National Intelligence University.

Maj. Michael Matthaeus, U.S. Army, is a senior faculty researcher at the University of Maryland's Applied Research Laboratory for Intelligence and Security with a research focus in cognitive security and disinformation. He is a psychological operations officer assigned to U.S. Cyber Command where he conducts integrated cyber, information, cryptographic, and electronic warfare operations.

Michael Guadian is a Department of the Army civilian who has spent the last decade working at the tactical level of U.S. Cyber Command (USCYBERCOM). During that time, he became USCYBERCOM's first master-qualified target digital network analyst and has spent the last several years developing and teaching new tradecraft to analysts under his charge.

fundamentally changed how resistance movements emerge, organize, and mobilize.[10] Cyberspace, especially in its increasingly surveilled state, affords opportunities for subversion as organizations (state and nonstate alike) can leverage persuasive technologies to achieve direct effects or to employ them as part of a disinformation campaign to obfuscate protagonists' true identity and/or intent.[11] The manipulation of existing or complete fabrication of social movements can have profound economic, political, and psychological effects even at the societal level and these effects often rely on some form of persuasive technology as it can take the form of media, tool, and/or social actor.[12]

> The repressive application of surveillance technologies undermines civil liberties, subverts human rights and democratic principles, and decreases trust in public institutions.

To serve as a tool, a technology must increase a human's ability to perform a desired task either through decreasing the (physical or mental) difficulty or restructuring the task; for example, pairing subcutaneous implants and a smartphone application to monitor blood glucose.[13] Persuasive technologies can also function as media through which the combination of interactivity and narrative afford rehearsal, empathy, and/or exploring nonintuitive causal relationships.[14] Social media platforms are persuasive by design, affording a degree of interaction and connectivity not seen with previous telecommunications technology and mass media and, in doing so, blur the boundary between the technological and human.[15] Persuasive technologies can also serve as a social actor whereby the technology is designed to cue and/or elicit social responses.[16] These systems can be rudimentary rule-based systems such as automated helplines or highly sophisticated multimodal sensors that incorporate artificial intelligence (AI) to rapidly process input, compare it against a database, and make therapeutic recommendations.[17] The development of persuasive technologies, initially influenced by the confluence of social psychology and user-centered design, has accelerated over the past decade thanks to advances in software engineering and data science.[18] Machine-learning methods, which are better suited to the large volumes of data than traditional statistical methods used in psychological research, have enabled the capability to develop individual profiles at scale and exploited them as a means to financial, social, and/or political ends.[19] AI, digital phenotyping, and psychoinformatics have transformed persuasive technologies from bespoke solutions in healthcare and assistive technologies to malign influence ecosystems.[20] This new environment has become the decisive battleground for political and psychological warfare.[21]

Subversion is a well-established method of psychological warfare that has evolved considerably within malign influence ecosystems.[22] Employed by resistance movements and states alike, subversion's reliance on exploitation distinguishes it from warfare and diplomacy, as does its indirect relationships between belligerents and clandestine modes of interaction.[23] Subversive operations exist along a spectrum from overt propaganda to covert disinformation and extend to organized violence, including sabotage and assassination.[24] Traditionally, a type of politically sensitive operation conducted by SOF and/or intelligence organizations, subversion has reemerged as instrument of statecraft thanks to the ability to connect with, understand, and manipulate populations through cyberspace.[25] Cyber operations provide low-risk, low-cost, and precise options for subversion, sabotage, political interference, and/or economic disruption.[26] Consequently, cyber operations afford the opportunity to undermine oppressive regimes, including the technological extension of those regimes. That technological extension, or digital authoritarianism, is the malicious use of the internet and digital surveillance technologies to increase social and political control over a population.[27] The intent is to make public life more observable to the state thus reducing opportunities for nonviolent action and inverting the concept of the internet as an engine of human

liberation.[28] The repressive application of surveillance technologies undermines civil liberties, subverts human rights and democratic principles, and decreases trust in public institutions.[29] The very phenomena digital authoritarianism seeks to quell have been recommended as foreign policy objectives and described as the raison d'être of the Army Special Forces profession.[30]

SOF and CMF should consider digital authoritarianism in the twenty-first-century analogous to Communist International export of subversive ideology in the mid-twentieth century and organize, train, and equip to understand then undermine this global threat.[38] These technological developments and citizens' resistance to them should stimulate the reconsideration of cyberspace from simply a complicated suite of technologies to a complex sociotechnical system.[39] Consequently, the operational understanding of the cyber domain must evolve to embrace this complexity.

"As cyberspace has become the principal domain for the conduct of psychological warfare, persuasive technologies provide the opportunity to access, assess, and influence resistance movements."

The export of digital authoritarianism is a form of foreign malign influence, a threat the White House considers a global priority.[31] The World Economic Forum conceptualizes the export of digital authoritarian norms as a malevolent cycle: the risk of misinformation devolves into widespread control of information that, in turn, leaves citizens vulnerable to political repression and domestic disinformation.[32] The intentional spread of disinformation using botnets, for example, has become a common tactic by state and nonstate actors, forcing political opponents to respond to false information putting them at an information disadvantage and preventing them from anticipating the effect of any emerging narrative or subsequent operation.[33] Botnets, while varying in scope and complexity, can be implemented as social actors for the public good.[34] However, botnets can also be used as an inexpensive and unattributed means of amplifying propaganda or, in effect, "jamming" the attempts of an adversary to disseminate their messaging.[35]

The combination of government suppression of information and actively manipulating the population through the dissemination of disinformation is an infringement on the universal human right of the consent of the governed. Consequently, the repressive application of surveillance technologies increases the number of oppressed peoples and, counterintuitively, the number of nascent resistance movements.[36] Cyber partisans have emerged in Belarus, Ukraine, the Middle East, and Venezuela, all of which present political opportunities for both the United States and its adversaries.[37] These nascent resistance movements can be enabled (or disabled) by persuasive technologies to achieve strategic advantage.

Applying Persuasive Technologies: Psychological Targeting and Resistance Warfare

As cyberspace has become the principal domain for the conduct of psychological warfare, persuasive technologies provide the opportunity to access, assess, and influence resistance movements.[40] Psychological targeting presents significant applied research opportunities to develop, refine, and validate, along with considerable operational challenges to implement. Spotting, assessing, and recruiting insurgents, as well as influencing the populace's behavior, are fundamental requirements of cyber resistance.[41] As those tasks rely on similar underlying social psychological concepts, both military information support operations (MISO) and human source intelligence (HUMINT) can benefit from psychological targeting.[42] Psychological targeting is the center of gravity of persuasive technology and refers to the practice of influencing the behavior of large groups of people through psychologically tailored interventions.[43] Psychological targeting combines software and analytic techniques that adapt content to the user's vulnerabilities (needs, wants, desires), susceptibilities

(propensity to receive and act on a message), psychographics, and/or previous online behavior.[44] Mood and emotion have been predicted from spoken language, video data, wearable devices, smartphone sensor metadata, and an individual's exposure to weather.[45] Research also suggests that personality can be predicted from personal websites, Facebook and Twitter profiles, blogs, language use, financial transaction records, and pictures.[46] This data can also include both traditional personality assessments administered online and derivative measures developed from online datasets, making them well suited to remote assessment.[47] Psychological targeting doesn't require a user interacting with a particular technological system, affording the clandestine modes of interaction preferred in subversion.[48]

Psychological targeting affords the opportunity to exploit psychographics to segment an audience into a set of psychologically homogeneous groups that allow for a more tailored approach to developing arguments that garner emotionally laden attention. These segments, however, need not be geographically collocated as online communities can be developed solely from these shared psychological characteristics.[49] Psychological profiling has been used to locate and target specific voters through lookalike modeling, which uses data-rich models of current supporters to identify likely supporters who exhibit similar signatures.[50] Cambridge Analytica implemented psychological targeting techniques to identify American voters with latent authoritarian preferences and thus framed its arguments accordingly.[51] The resultant microtargeting exacerbated the veracity problem on many social media platforms as different audiences received different information and/or different interpretations on ambiguous information.[52] Foreign malign influence to disrupt or corrupt electoral processes remains a global threat whose complexity evolves every election cycle and such, the subversion potential of persuasive technologies such be considered an enduring threat.[53] Addressing said threat requires both defensive and offensive methods. Subversion requires nuance which implies a need for exquisite detail on target audiences.[54] MISO, a core activity of SOF, should be conducted against target audiences as narrow as can be assessed, and the intelligence collected through cyberspace affords opportunities for such precision.[55] The operational application of persuasive technologies is most pertinent to MISO and HUMINT as both involve understanding and influencing human behavior.[56] Both also happen to be critical in cyber resistance as MISO and HUMINT are becoming increasingly reliant on cyberspace as a medium to spot, assess, recruit, train, and influence individuals, organizations, and populations.[57] The cyber domain affords the opportunity to conduct precise engagements (whether to recruit or manipulate) at scale, contributing to the subversive nature of cyberspace operations.[58]

Psychoinformatics, the confluence of computer science and psychology, has developed potentially applicable methods some of which may be implemented at scale. Psychoinformatics adapts tools and techniques from computer science to improve the collection and analysis of psychological data by prioritizing the direct assessment of behavior derived from human-machine interaction on an operating system level.[59] Psychoinformatics incorporates statistical techniques from both psychological and computer science but relies more heavily on the latter. Machine learning, a subfield of AI, employs algorithms to "learn" from the data ingested. Machine learning can be supervised or unsupervised with the former referring to approaches where the model is trained on human-labeled data to ultimately predict unlabeled data and the latter referring to approaches without any external intervention. Applied research that incorporates the combination of self-report and smartphone sensor data in larger samples over time will yield further insight into the psychological inferences that can be obtained from operating system information alone. This operational system data exists within various collection databases and could be mined and compared with other reporting and/or assessments.

Digital phenotyping uses data collected from smart devices to track markers of mental disorders.[60] Mobile sensing technologies enable the continuous measurement of physiological and behavioral data, the combination of which can provide unique insight into an individual's susceptibility to a particular intervention. The combination of technologies and techniques afford clinicians the opportunity to implement precision medicine through the combination of objective assessments and precisely calibrated treatments. Digital phenotyping typically entails application, computing, sensing, and conceptual layers.[61] The conceptual layer or the clinical formulation of mental health and

well-being is the interaction among biological factors, emotional factors, behavioral traits, social factors, and cognitive ability.[62] The sensing layer is the combination of contextual sensing capabilities of the smartphone, paired wearable sensors, social media platforms, and/or an electronic health record.[63] The computing layer is the hardware and software instantiations of psychoinformatics, including psychometric analysis, behavioral anomaly detection, social analytics, and biomarkers.[64] The application layer is the purpose of the project or product and could be a means to evaluate and/or diagnose, monitor, intervene, prevent, and/or support a patient.[65] The combination is a holistic, or multiform organismic, approach to understanding an individual in an operational context.[66]

Psychological targeting research suggests that psychological profiling is a reliable means of inferring state and trait characteristics.[67] Algorithmic approaches to personality assessment, when compared with other psychometrics, have the most empirical support in the scientific literature and the most compelling operational applications, particularly when enriched with other types of digital footprints.[68] Research incorporating the combination of self-report and smartphone sensor data in larger samples over time will yield further insight into the psychological inferences that can be obtained from operating system information alone.[69] This operating system data exists within various collection databases and could be mined and compared with other reporting and/or assessments to provide more refined target audience analysis to support a range of subversive cyber operations. Adapting and applying the psychological targeting research methods using more operationally relevant data sources is feasible, but ground truth is necessary for comparing and validating the algorithmic extraction methods. However, the research on psychologically informed interventions is insufficient to suggest it is effective in diminishing symptoms of various mental disorders. That said, the science is evolving methodologically and technologically and warrants attention, but little can currently be applied to time-sensitive targeting without additional exploration. The penultimate section will address this issue in greater detail.

“Operationalizing the capability for strategic subversion could serve as an unconventional deterrent to complement offensive and defensive cyber operations to defend the U.S. electoral process. Doing so, however, requires advanced training in both human and technological systems, and the confluence thereof seems to be a pedagogical gap in military and intelligence curricula.”

Persuasive technologies attempt to influence behavior; synthesizing elements from each in conjunction with established methods of social influence thus holds potential to deter and influence in cyberspace.[70] Operationalizing the capability for strategic subversion could serve as an unconventional deterrent to complement offensive and defensive cyber operations to defend the U.S. electoral process.[71] Doing so, however, requires advanced training in both human and technological systems, and the confluence thereof seems to be a pedagogical gap in military and intelligence curricula.

Training and Education Requirements for Persuasive Technologies

U.S. Cyber Command (USCYBERCOM) emphasizes training cyber operators in the technological aspects of networking and system vulnerabilities, focusing on critical work roles that enable access and conduct operations, with little emphasis on the cognitive domain. Furthermore, there is limited understanding (within both cyber operators and cyber operations planners) of psychological warfare concepts and their applicability to cyber effects operations.[72] While there is little doubt that technologically competent personnel are essential to the CMF, it is necessary to have

a thorough understanding of the more complex and ambiguous node of the network: the user.[73]

Computer networks conform to standards established by the Institute of Electrical and Electronics Engineers Standards Association, giving all networks a degree of similarity that provides a common analytic baseline.[74] The users of those networks, however, vary considerably and thus require human factors analysis (HFA) to perceive, comprehend, and project.[75] The current paradigm within the CMF prioritizes access operations from a purely technological standpoint with little to no emphasis on human factors.[76] Decades of interdisciplinary cybersecurity research have demonstrated the human to be the most significant vulnerability in any computer network, yet the application of social science to cybersecurity lags.[77] Cybersecurity is, however, psychologically distinct from cyber operations, and it is the latter that requires greater pedagogical attention as there is even less applied social and behavioral science research dedicated to it.[78] The CMF is equipped with a unique set of authorities, accesses, and capabilities to support resistance warfare.[79] Presently, the established intelligence and cyber curricula do little to address and/or further explore resistance warfare in cyberspace. The existing coursework provides a rudimentary understanding of basic cyber architecture and function with little in the way of advanced intelligence or psychological training necessary to understand cyberspace as the complex sociotechnical system it is.[80] For example, as previously noted, algorithmic approaches to psychometric assessment have potential operational utility.[81] This is particularly so when those analyses are enriched by data collected via signals intelligence (SIGINT). SIGINT can provide insight to MISO, but precision messaging requires personalization that can be objectified, quantified, and contextualized through open-source intelligence.[82] As MISO becomes increasingly reliant on the internet to not only conduct target audience analysis but also disseminate messages the intelligence support, particularly SIGINT, must adapt.[83]

SIGINT enables targeting at all fulcrums of assessment within HFA, and the nature of the accesses provide reliability that other intelligence disciplines cannot.[84] As cybersecurity practices are increasingly adapting psychological research findings and integrating them into their defenses, similar translations must be made to cyber operations and their SIGINT support.[85] This translation needs to begin at the basic qualification courses. The U.S. Army's Cyber Center of Excellence is the home of the Cyber School, an institution critical to training SIGINT and cyber personnel for an increasingly prominent role in contemporary military operations.[86] The Cyber Center of Excellence, however, has been slow to adopt more comprehensive conceptualizations of both cyberspace and how best to apply cyber capabilities as an instrument of statecraft. Consequently, neither cyber resistance nor the more complex conceptualization of cyberspace that emphasizes the cognitive domain have been integrated into the curriculum. Cyberspace is a complex dynamic sociotechnical system and thus, a shift in cyber and intelligence training is necessary to address the skill deficit in HFA to better support operations once the individual is assigned to the CMF.[87]

The current model for intelligence certification implements a three-tier system of basic, senior, and master levels. While the initial training is sufficient, it is typically focused on the relevant technologies that comprise computer networks. Counterintuitively, there is less differentiation as one progresses to senior and master levels. Better integration of more advanced psychological training is necessary for the progression to senior and, ultimately, master. Fundamental changes must be implemented, particularly for the intelligence personnel specializing in persona analysis within SIGINT better support cyber operations.[88] Psychological targeting methods can be translated for operational application; however, it will require the tactical integration of social and behavioral scientists and more advanced training for intelligence personnel supporting both SOF and CMF. While some coursework will need to be created for and tailored to specific units within the CMF, there may also be opportunities to share resources and/or cross-train with SOF to better achieve both service and joint force training objectives.[89]

The U.S. Army John F. Kennedy Special Warfare Center and School recently established the Psychological Warfare (PSYWAR) School, which marks a significant development in training SOF to focus on resistance movements during multidomain operations.[90] Specifically, the PSYWAR School has an opportunity to institutionalize the assimilation of

persuasive technology and resistance warfare through cyberspace into joint SOF and CMF formative training. While the PSYWAR school is designed to improve the initial and advanced training experiences of psychological operations personnel, it is not postured to train and educate CMF personnel.[91] However, by allowing CMF personnel who meet the requisite criteria to enroll, the PSYWAR School can embody the fifth SOF Truth and provide the intellectual foundation for warfare psychologically waged through cyberspace.[92]

Joint Special Operations University (JSOU) offers a spectrum of courses relevant to both CMF and SOF requirements of modern warfare.[93] Courses such as the National Resistance Course, Joint Unconventional Warfare Operations Course, SOF Sensitive Activities Foundation Course, and the pilot program for SOF Influence and Operations in the Information Environment incorporate instruction on both cyber operations and resistance movements, to include their confluence.[94] These courses are designed to enhance the understanding and operational skills of personnel in multidomain environments, which are increasingly influenced by cyber dynamics. Furthermore, JSOU has specific sections devoted to integrating cyberspace operations within the scope of special operations, exemplified by Cyberspace and Special Operations Forces and the Theater Special Operations Command Cyber Planner Course.[95] These courses lay the practical foundation for the integration of emergent, accessible, and low-cost technology in cyber operations, crucial for modern resistance warfare. While portions of the instruction include emergent and influential technologies like generative AI, there remains no unifying theme as to the applications for SOF in cyber operations or for CMF integration into resistance warfare. Critical for any SOF and CMF training evolution is a focus on how multidomain environments are shaped by cyber dynamics. Additionally, reframing these cyber actions in a subversive warfare context adds a coherent framework for developing resistance movements to subvert great powers.

The National Intelligence University (NIU) Anthony G. Oettinger School of Science and Technology Intelligence prepares students for careers at the forefront of science and technology intelligence.[96] The school offers cyber intelligence and information and influence intelligence concentrations, both of which provide the interdisciplinary scientific and technological underpinnings of contemporary conflict and the research skills necessary to conduct the necessary applied research. NIU can provide both the advanced educational and research opportunities to SOF and CMF personnel to explore the psychological, technological, legal, operational, and strategic implications of operationalizing persuasive technologies.

Applied Research in Persuasive Technologies

The U.S. Army John F. Kennedy Special Warfare Center and School can provide the necessary introductory training along with some advanced training, while JSOU can address the latter. The respective curricula described herein can then be augmented through advanced education at NIU. Both advanced training and education should include CMF and SOF to develop the necessary shared understanding. NIU can then develop (or refine existing) programs where students conduct research within their academic and operational expertise alongside students with different expertise to understand different aspects of a shared problem set.

A potential research collaboration among the U.S. Special Operations Command, USCYBERCOM, JSOU, and NIU might be to develop digital phenotypes of malicious cyber actors (MCAs) so that intelligence professionals can better understand the psychological characteristics as cybersecurity analysts understand their technical characteristics. Cybersecurity research and intelligence firms attribute advanced persistent threats (APT) based on observed tactics and even threat profiling, and the assessments can be enriched by incorporating psychological targeting data from individuals affiliated with said APTs.[97] Some APTs function like more traditional reconnaissance units, gaining access, observing, and reporting.[98] Others are a contemporary manifestation of Messner's crypto-covert forces, who operate surreptitiously across a broad spectrum of activities ranging from reconnaissance to sabotage to psychological warfare.[99] APTs like Sandworm combine technological and psychological effects as part of a broader cyber-psychological approach to information confrontation.[100] These cyber-psychological approaches may create distinct digital footprints that can be used as both indication and warning signals, and attack surfaces to subvert.

Digital phenotypes of operational phenomena, for example MCAs, could be developed using similar methods and technologies. Translating concepts from clinical psychology such as risk factors, long used to assess likelihood of symptom reoccurrence and/or relapse as well as dangerousness, may be combined with techniques from digital phenotyping and cyber threat intelligence analysis to develop digital phenotypes of MCA.[101] The conceptual layer of this model would be less about mental health or well-being and more about propensity to engage in malicious cyber activity, but the remaining aspects (biological factors, emotional factors, behavioral traits, social factors, and cognitive ability) would still apply.[102] The application layer would also be for nonclinical purposes, such as accessing and assessing, but the sensing and computing layers would remain.

The challenge of translating a clinical paradigm to an operational one has concomitant risks, namely the assumption that persons of interest will exhibit some form of observable behavior that has discriminant validity.[103] The research to date, while promising, often fails to include healthy controls against which the behavior of patients can be compared. Using such approaches to develop signatures risks false positives and thus collecting on individuals whose behavior is close enough to the target of interest but otherwise irrelevant. Like any composite profile, there are individuals who may not exhibit any of the characteristics described. The concomitant behavioral correlates of the attributes of interest must be identified and validated. The diagnosticity of the approach in an operational context requires a comparison of existing device-level data, observed behavior, and/or other psychological assessments. Consequently, additional applied research by teams of scientists, CMF, and SOF is required. Upon graduation, NIU alumni can then apply what they've learned to novel operational designs through more coherent cyber doctrine, policy, strategy, and offensive and defensive tactics included in an updated *Resistance Operating Concept* (*ROC*).[104]

Operationalizing Persuasive Technologies in the Next ROC: Developing a Subversive Cyber Strategy

Cybersecurity researchers and cyber operators (inclusive of both SOF and CMF) could benefit from this type of integration and applied research as it applies directly to establishing subversion as an element of a cyber strategy.[105] USCYBERCOM's mandate is to "Direct, Synchronize, and Coordinate Cyberspace Planning and Operations—to Defend and Advance National Interests—in Collaboration with Domestic and International Partners," which, in practice, means access operations instead of incorporating full-spectrum operations into planning and execution.[106] Cyber operations tend to be viewed as systems-focused and defensive or as a contemporary form of fire support whereby the operational objective is the degradation and/or destruction of adversary information systems.[107] This latter application has had only technological and/or tactical success and thus the role of strategic cyber operations warrants reconsideration.[108]

The *2023 Cyber Strategy* identifies malicious cyber activity, to include foreign malign influence efforts, as a threat to the Nation and USCYBERCOM has the mission to deter, disrupt, manipulate, and defeat adversary cyber and malign influence actors.[109] Despite cyber threats being as psychological as they are technological, USCYBERCOM prioritizes the latter at the expense of the former.[110] Consequently, there is insufficient institutional recognition that cyber operations should be integrated into a larger psychological strategy.[111] Training and educating SOF and CMF together in advanced venues could help dissolve cultural resistance to the others' concepts and develop better integrated operational approaches.

The *ROC* served as a blueprint for Ukrainian resistance to the 2022 Russian invasion and occupation.[112] While the 2022 Russian invasion of Ukraine was less adherent to Messner's concept than their 2014 invasion, both employed resistance movements in the cyber domain in attempt to create a strategic advantage.[113] The United States must update and advance the *ROC* to better account for cyberspace and its concomitant complexities. This requires not only more integrated training but also an ideological convergence of SOF and CMF. Developing a subversive resistance warfare thrust within a national cyber strategy could facilitate the convergence.

The separation between the training of SOF and CMF has limited the strategic effectiveness of military operations, particularly in subverting great powers by, with, and through cyber resistance movements.[114] As

adversaries increasingly resort to subversive tactics, traditional power gaps are bridged through cheap, accessible cyber tools to achieve strategic advantage.[115] SOF and CMF are critical in GPC, yet do not maintain a coherent and reproducible mission alignment. Adversary actions in cyberspace underscore the necessity for a collective understanding and operational capability in subversion, propaganda, covert disinformation, organized violence, and cyber operations—integral components of contemporary resistance warfare.[116]

“Adversary actions in cyberspace underscore the necessity for a collective understanding and operational capability in subversion, propaganda, covert disinformation, organized violence, and cyber operations—integral components of contemporary resistance warfare.”

CMF and SOF collaboration is necessary to develop contemporary concepts for resistance warfare in the cyber domain, and there are practical similarities between CMF and SOF that warrant tactical through strategic partnerships.[117] Integrated training between CMF and SOF should focus on several key areas. The first is interoperability. In practical terms, training programs must emphasize operational integration in which cyber and special operations personnel conduct joint missions, leveraging each other's strengths in real-time operational contexts. Resistance warfare calls for operationalizing resistance movements, propaganda, sabotage, espionage, and destructive actions, all while focusing on the asymmetric cognitive impacts for strategic advantage.[118] Cyberspace operations facilitate these actions in a cheap, accessible, and repeatable fashion without the need for full-time physical presence.[119] Additionally, full interoperability between CMF and SOF brings a course of action development flexibility. Lessons from Ukraine and Israel reinforce the idea that capabilities must be developed prior to crisis and conflict.[120] SOF has a unique remit to conduct battlefield preparation, partner force training, and developing resistance networks in foreign countries.[121] Cyber resistance is the logical evolution and extension of this responsibility.

SOF and CMF must also integrate and curate persuasive technologies to develop asymmetric advantage in a strategic context. A development pathway must provide comprehensive exposure to advanced technologies such as AI, digital phenotyping, and psychoinformatics, which are crucial for the development of sophisticated cyber operations and psychological warfare tactics.[122] Critical for this joint development is how cognitive impacts may be created from resistance warfare tactics in and through cyberspace.

Finally, an integrated CMF and SOF capability must share operational design. Drawing on information from the modern operational environment, the defense industrial base, U.S. allies and partners, and adversary cyber campaigns, a resistance operating concept in cyberspace is an evolving but durable concept. The cognitive impact of cyber operations is undeniable but understudied. If a society or its people are reliant on digital technology, then that behavior can be exploited.[123] Iran, Russia, and China have already demonstrated both the capability and intent to operationalize cyber resistance movements to achieve a political objective.[124] A joint CMF and SOF design for resistance movements in cyberspace utilizes the strengths of both forces to affect combined arms integration.

Conclusion

Messner places the psychological dimension of conflict at the center of a strategy to influence the psyche of the enemy.[125] There are few operational environments more conducive to such approaches than the cyber domain.[126] Messner's concept of subversion war is an appropriate theoretical framework to understand contemporary resistance warfare in cyberspace.[127] While the U.S. strategy of persistent engagement does not cite Messner, his principles of subversion war underlie the U.S. approach to cyber operations.[128] The United States should embrace this and develop a cyber strategy with subversion at its core accentuated by

persuasive technologies and a well-trained and well-educated force to operationalize them.

The methods identified in the psychological targeting literature are adaptations and extensions of approaches developed in clinical and political psychology combined with statistical methods used in computer science.[129] These indirect assessments have long been used in the intelligence community and can be readily adapted within the next *ROC*.[130] Doing so, however, requires the capability for precision influence at scale that requires considerable applied research.

A joint operational design between CMF and SOF incorporates dynamic and targeted operations, influences activities, and coordinates actions. Engaging directly with adversaries online or covertly exposing malicious behavior to various audiences provides a methodology to counter MCAs. MISO should be conducted against target audiences as narrow as can be assessed, and SIGINT affords such opportunities to do so in support of CMF.[131] Cyber targeting is unique in that, often, one can strike a single target multiple times from multiple approaches with the same desired effect. Correspondingly, allies and partners likely prioritize similar adversary cyber targets, which unites SOF and CMF communities. Increased coordination with partners and allies is not only an operational priority but also a strategic imperative. NIU could provide CMF and SOF students the opportunity to conduct such exploratory and applied studies to advance our understanding of the limits of these approaches and their potential operational utility. A research priority should be developing digital phenotypes of MCAs, a potential focal point of the next *ROC*.

> While the U.S. strategy of persistent engagement does not cite Messner, his principles of subversion war underlie the U.S. approach to cyber operations. The United States should embrace this and develop a cyber strategy with subversion at its core accentuated by persuasive technologies and a well-trained and well-educated force to operationalize them.

To compete with and/or deter great powers and maintain proficiency in resistance warfare, the U.S. must give primacy to subversion in future cyber strategy.[132] Doing so requires not only the adoption of subversion as a national strategy for cyber but also integrating training and education of CMF and SOF so that the subversive potential of persuasive technologies can be operationalized through an updated *ROC*. The updated *ROC* will serve as a blueprint for a more egosyntonic, and thus subversive, national cyber strategy. ■

The views expressed in this article are the authors' and do not imply endorsement by the Director of National Intelligence or any other U.S. government agency.

Notes

Epigraph. Evgeny E. Messner, "The Face of Contemporary War," in *Strategiya: The Foundations of the Russian Art of Strategy*, ed. Ofer Fridman (New York: Hurst, 2021), 265.

1. Michael J. Forsyth, "The Perfect Storm: How Civil-Military Relations in the United States Affect Policy and Strategy Development" (PhD diss., Royal Military College of Canada, 2022), https://espace.rmc.ca/jspui/bitstream/11264/924/1/Composite%20Dissertation%20Post_Defense%20Final.pdf; Clyde H. Coombs and George S. Avrunin, *The Structure of Conflict* (New York: Psychology Press, 2013); George Dimitriu, "Clausewitz and the Politics of War: A Contemporary Theory," *Journal of Strategic Studies* 43, no. 5 (2020): 645–85, https://doi.org/10.1080/01402390.2018.1529567; Alexandra Chinchilla et al., "Irregular Warfare in Strategic Competition," *Defence Studies* 24, no. 1 (2024): 148–58, https://doi.org/10.1080/14702436.2023.2279620.

2. Oscar Jonsson, *The Russian Understanding of War: Blurring the Lines Between War and Peace* (Washington, DC: Georgetown University Press, 2019).

3. Evgeny E. Messner, *The Worldwide Subversion War* (Buenos Aires, AR: South American Division of the Institute for the Study of

the Problems of War and Peace Named After Prof. General N. N. Golovin, 1971); Ofer Fridman, *Russian "Hybrid Warfare": Resurgence and Politicization* (Oxford: Oxford University Press, 2018); Jonsson, *Russian Understanding of War*.

4. Amos C. Fox, "Comparative Proxy Strategies in the Russo-Ukrainian War," *Comparative Strategy* 42, no. 5 (2023): 605–20, https://doi.org/10.1080/01495933.2023.2236488; Mark Grzegorzewski, "Russia's 2022 Cyber-Enabled Warfare Against Ukraine: Why Russia Failed to Perform to Expectations," in *The Great Power Competition: The Russian Invasion of Ukraine and Implications for the Central Region*, ed. Adib Farhadi, Mark Grzegorzewski, and Anthony J. Masys, vol. 5 (Cham, SU: Springer, 2023), 47–73; Oliver Beatson et al., "Automation on Twitter: Measuring the Effectiveness of Approaches to Bot Detection," *Social Science Computer Review* 41, no. 1 (2021): 181–200, https://doi.org/10.1177/08944393211034991; Hadi Ajili and Mahsa Rouhi, "Iran's Military Strategy," *Survival* 61, no. 6 (2019), 139–52, http://dx.doi.org/10.1080/00396338.2019.1688575; Paul Charon and Jean-Baptiste Jeangène Vilmer, *Chinese Influence Operations: A Machiavellian Moment* (Paris: Institute for Strategic Research, 2021), https://www.irsem.fr/report.html; Patrick M. Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Force Quarterly* 79, no. 4 (2015): 46–53, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/621123/strategic-development-of-special-warfare-in-cyberspace/; Kong Ji-Young, Lim Jong In, and Kim Kyoung Gon, "The All-Purpose Sword: North Korea's Cyber Operations and Strategies," in *2019 11th International Conference on Cyber Conflict (CyCon)* (New York: Institute of Electrical and Electronics Engineers [IEEE], 2019), 1–20, https://doi.org/10.23919/CYCON.2019.8756954; Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation Is Arming Tomorrow's Terrorists* (New York: Oxford University Press, 2019).

5. Fridman, *Russian "Hybrid Warfare"*; Laura Jones, "The Future of Warfare Is Irregular," *Fletcher Forum of World Affairs* 46, no. 2 (2022): 107, https://www.fletcherforum.org/s/Jones-2a_APPROVED.pdf; Brandon Turner and Paul Bailey, "The Joint Force–SOF Relationship," *Marine Corps Gazette*, January 2020, 12–20, https://www.mca-marines.org/wp-content/uploads/The-Joint-Force%E2%80%93SOF-Relationship.pdf.

6. Sandra C. Matz, Ruth E. Appel, and Michal Kosinski, "Privacy in the Age of Psychological Targeting," *Current Opinion in Psychology* 31 (2020): 116–21, https://doi.org/10.1016/j.copsyc.2019.08.010.

7. Lennert Maschmeyer, *Subversion: From Covert Operations to Cyber Conflict* (New York: Oxford University Press, 2024).

8. Arnel P. David et al., "Why We Need a Modern Theory of Special Warfare to Thrive in the Human Domain," Wavell Room, 14 May 2020, https://wavellroom.com/2020/05/14/why-we-need-a-modern-theory-of-special-warfare-to-thrive-in-the-human-domain/; Michael McClintock, *Instruments of Statecraft: U.S. Guerrilla Warfare, Counterinsurgency, and Counterterrorism, 1940–1990* (New York: Pantheon Books, 1992), https://www.statecraft.org.

9. Spitaletta, "Human Factors Considerations of Undergrounds in Cyber Resistance."

10. Ibid.

11. Michael Wrana, Diogo Barradas, and N. Asokan, "The Spectre of Surveillance and Censorship in Future Internet Architectures," preprint, submitted 29 January 2024, https://arxiv.org/abs/2401.15828; Jill Kastner and William C. Wohlforth, "A Measure Short of War: The Return of Great-Power Subversion," *Foreign Affairs*, July-August 2021, 118–31, https://www.foreignaffairs.com/articles/world/2021-06-22/measure-short-war.

12. Romy Kraemer, Gail Whiteman, and Bobby Banerjee, "Conflict and Astroturfing in Niyamgiri: The Importance of National Advocacy Networks in Anti-Corporate Social Movements," *Organization Studies* 34, no. 5-6 (2013): 823–52, https://doi.org/10.1177/0170840613479240.stat; B. J. Fogg, *Persuasive Technology: Using Computers to Change What We Think and Do* (Palo Alto, CA: Morgan Kaufmann, 2002).

13. Fogg, *Persuasive Technology*; Ghasem Yadegarfa et al., "The FreeStyle Libre Flash Glucose Monitoring System: How It Has Improved Glycaemic Control for People with Type 1 Diabetes in Eastern Cheshire, UK," *Cardiovascular Endocrinology & Metabolism* 9, no. 4 (2020): 171–76, https://www.doi.org/10.1097/XCE.0000000000000216.

14. Fogg, *Persuasive Technology*.

15. Alex Beattie, "From Poacher to Protector of Attention: The Therapeutic Turn of Persuasive Technology and Ethics of a Smartphone Habit-Breaking Application," *Science, Technology, & Human Values* 47, no. 2 (2022): 337–59, https://doi.org/10.1177/01622439211042667.

16. Fogg, *Persuasive Technology*.

17. Judith Prochaska et al., "A Therapeutic Relational Agent for Reducing Problematic Substance Use (Woebot): Development and Usability Study," *Journal of Medical Internet Research* 23, no. 3 (2021): e24850, https://doi.org/10.2196/24850.

18. Fogg, *Persuasive Technology*; Ruth E. Appel and Sandra C. Matz, "Psychological Targeting in the Age of Big Data," in *Measuring and Modeling Persons and Situations*, ed. Dustin Wood et al. (New York: Academic Press, 2021), 193–222.

19. Appel and Matz, "Psychological Targeting in the Age of Big Data"; Davide Marengo and Christian Montag, "Digital Phenotyping of Big Five Personality via Facebook Data Mining: A Meta-Analysis," *Digital Psychology* 1, no. 1 (2020): 52–64, https://doi.org/10.24989/dp.v1i1.1823; Vian Bakir, "Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting," *Frontiers in Communication* 5, no. 67 (2020): 116, https://doi.org/10.3389/fcomm.2020.00067.

20. Matz, Appel, and Kosinski, "Privacy in the Age of Psychological Targeting"; Kit Huckvale, Svetha Venkatesh, and Helen Christensen, "Toward Clinical Digital Phenotyping: A Timely Opportunity to Consider Purpose, Quality, and Safety," *npj Digital Medicine* 2 (2019): 88, https://doi.org/10.1038/s41746-019-0166-1; Tal Yarkoni, "Psychoinformatics: New Horizons at the Interface of the Psychological and Computing Sciences," *Current Directions in Psychological Science* 21, no. 6 (2012): 391–97, https://doi.org/10.1177/0963721412457362; Miriam Cabrita et al., "Persuasive Technology to Support Active and Healthy Ageing: An Exploration of Past, Present, and Future," *Journal of Biomedical Informatics* 84 (2018): 17–30, https://doi.org/10.1016/j.jbi.2018.06.010; Anthony Nadler, Matthew Crain, and Joan Donovan, *Weaponizing the Digital Influence Machine: The Political Perils of Online Ad Tech* (New York: Data and Society Research Institute, 2018), https://www.datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf.

21. Spitaletta, "Human Factors Considerations of Undergrounds in Cyber Resistance."

22. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus, and Giroux, 2020); Jan Goldman, "Influence Operations and the Role of Intelligence," in *Routledge Handbook of Disinformation and*

National Security, ed. Rubén Arcos, Irena Chiru, and Cristina Ivan (New York: Routledge, 2024), 84–94.

23. Nathan Bos et al., *Human Factors Considerations of Undergrounds in Insurgencies*, 2nd ed. (Fort Liberty, NC: U.S. Army Special Operations Command, 2013), https://www.soc.mil/ARIS/books/pdf/HumanFactorsS.pdf; McClintock, *Instruments of Statecraft*; Lennart Maschmeyer, "A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict," *Journal of Strategic Studies* 46, no. 3 (2023): 570–94, https://doi.org/10.1080/01402390.2022.2104253.

24. Shawn J. Parry-Giles, "The Eisenhower Administration's Conceptualization of the USIA: The Development of Overt and Covert Propaganda Strategies," *Presidential Studies Quarterly* 24, no. 2 (1994): 263–76, https://www.jstor.org/stable/27551240; Moritz Poellath, "Agents, Fascists and Provocateurs: Disinformation as an Instrument to Delegitimize Uprisings in Eastern Europe (1953, 1956, 1968) and Its Impact on the Politics of Memory," *Journal of Intelligence History* 22, no. 2 (2023): 234–56, https://doi.org/10.1080/16161262.2021.1918940; Mikkel Thorup, "The Anarchist and the Partisan—Two Types of Terror in the History of Irregular Warfare," *Terrorism and Political Violence* 20, no. 3 (2008): 333–55, https://doi.org/10.1080/09546550802073300; Kastner and Wohlforth, "A Measure Short of War."

25. McClintock, *Instruments of Statecraft*; Kastner and Wohlforth, "A Measure Short of War"; Spitaletta, "Human Factors Considerations of Undergrounds in Cyber Resistance."

26. Lennart Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations," *International Security* 46, no. 2 (2021): 51–90, https://doi.org/10.1162/isec_a_00418.

27. Tate Ryan-Mosley, "The World Is Moving Closer to a New Cold War Fought with Authoritarian Tech," MIT Technology Review, 22 September 2022, https://www.technologyreview.com/2022/09/22/1059823/cold-war-authoritarian-tech-china-iran-sco/.

28. Matthew D. Cebul and Jonathan C. Pinckney, *Digital Authoritarianism and Nonviolent Action: Challenging the Digital Counterrevolution* (Washington, DC: United States Institute of Peace, 2021), https://www.usip.org/publications/2021/07/digital-authoritarianism-and-nonviolent-action-challenging-digital; Thomas V. Maher and Jennifer Pan, "The Digital Repression of Social Movements, Protest, and Activism: A Synthetic Review," *Science Advances* 8, no. 10 (2022): eabl8198, https://doi.org/10.1126/sciadv.abl8198.

29. Inga K. Trauthig, Zelly C. Martin, and Samuel C. Woolley, "Messaging Apps: A Rising Tool for Informational Autocrats," *Political Research Quarterly* 77, no. 1 (2024): 17–29, https://doi.org/10.1177/10659129231190932; Erol Yayboke and Samuel Brannen, "Promote and Build: A Strategic Approach to Digital Authoritarianism," Center for Strategic and International Studies, accessed 21 October 2024, https://www.csis.org/analysis/promote-and-build-strategic-approach-digital-authoritarianism; Ryan-Mosley, "The World Is Moving Closer to a New Cold War Fought with Authoritarian Tech."

30. John S. McCain, "National History and Universal Values: Prioritizing Human Rights in US Foreign Policy," *Brown Journal of World Affairs* 16, no. 2 (2010): 9–14, https://bjwa.brown.edu/16-2/national-history-and-universal-values/; Paul J. Thompkins Jr., "The Special Forces Profession," *Special Warfare* 32, no. 2 (June 2019): 6–7, https://www.swcs.mil/Portals/111/32-2_APR_JUN_2019.pdf.

31. *Oxford Research Encyclopedia of International Studies*, s.v. "The Politics of Digital (Human) Rights," by Ben Wagner et al., 13 December 2023, https://doi.org/10.1093/acrefore/9780190846626.013.694; The White House, *National Security Strategy* (Washington, DC: The White House, October 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

32. World Economic Forum, *The Global Risks Report 2024*, 19th ed. (Geneva: World Economic Forum, 2024), https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf.

33. Huajie Shao et al., "Misinformation Detection and Adversarial Attack Cost Analysis in Directional Social Networks," in *2020 29th International Conference on Computer Communications and Networks (ICCCN)* (New York: IEEE, August 2020), 1–11, https://doi.org/10.1109/ICCCN49398.2020.9209609; Massimo Stella, Emilio Ferrara, and Manlio De Domenico, "Bots Increase Exposure to Negative and Inflammatory Content in Online Social Systems," *Proceedings of the National Academy of Sciences* 115, no. 49 (2018): 12435–40; https://doi.org/10.1073/pnas.1803470115; William Reno and Jahara Matisek, "A New Era of Insurgent Recruitment: Have 'New' Civil Wars Changed the Dynamic?," *Civil Wars* 20, no. 3 (2018): 358–78, https://doi.org/10.1080/13698249.2018.1497314.

34. Clare L. Foster, "Truth as Social Practice in a Digital Era: Iteration as Persuasion," *AI & Society* 38, no. 5 (2023): 2009–23, https://doi.org/10.1007/s00146-021-01306-w.

35. David Omand, "The Threats from Modern Digital Subversion and Sedition," *Journal of Cyber Policy* 3, no. 1 (2018): 5–23, https://doi.org/10.1080/23738871.2018.1448097.

36. Richard Ashby Wilson, "Digital Authoritarianism and the Global Assault on Human Rights," *Human Rights Quarterly* 44, no. 4 (2022): 704–39, https://doi.org/10.1353/hrq.2022.0043; Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models" (Washington, DC: Brookings Institution, 2019), 1–22, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf; Eda Keremoğlu and Nils B. Weidmann, "Authoritarianism and Digital Communication," in *Research Handbook on Authoritarianism*, ed. Natasha Lindstaedt and Jeroen J. J. Van den Bosch (Cheltenham, UK: Edward Elgar Publishing, 2024), 128–38.

37. Peter Schrijver and Paul Ducheine, "Cyber-Enabled Influence Operations," *Militaire Spectator* 192, no. 6 (2023): 284–95, https://militairespectator.nl/sites/default/files/bestanden/uitgaven/inhoudsopgaven/militaire_spectator_6_2023_schrijver.pdf; Ann Väljataga, "Cyber Vigilantism in Support of Ukraine: A Legal Analysis" (Tallinn, EE: NATO Cooperative Cyber Defence Centre of Excellence, March 2022), https://www.ccdcoe.org/uploads/2022/04/Cyber-vigilantism-in-support-of-Ukraine-a-legal-analysis.pdf; Miron Lakomy, "Let's Play a Video Game: Jihadi Propaganda in the World of Electronic Entertainment," *Studies in Conflict & Terrorism* 42, no. 4 (2017): 383–406, http://dx.doi.org/10.1080/1057610X.2017.1385903; Iria Puyosa, "Asymmetrical Information Warfare in the Venezuelan Contested Media Spaces," in *When Media Succumbs to Rising Authoritarianism*, ed. Ezequiel Korin and Paromita Pain (New York: Routledge, 2021), 32–45; Nicholas A. Bredenkamp and Mark Grzegorzewski, "Supporting Resistance Movements in Cyberspace," *Special Operations Journal* 7, no. 1 (2021): 17–28, https://doi.org/10.1080/23296151.2021.1904570.

38. Rid, *Active Measures*.

39. Gabriele Giacomini, *The Arduous Road to Revolution: Resisting Authoritarian Regimes in the Digital Communication Age*

(San Giovanni, IT: Mimesis International, 2022); Christian Fuchs, "The Internet as a Self-Organizing Socio-Technological System," *Cybernetics & Human Knowing* 12, no. 3 (2003): 37–81, https://dx.doi.org/10.2139/ssrn.458680.

40. Spitaletta, "Human Factors Considerations of Undergrounds in Cyber Resistance."

41. Ibid.

42. Randy Burkett, "An Alternative Framework for Agent Recruitment: From MICE to RASCLS," *Studies in Intelligence* 57, no. 1 (2013): 7–17, https://www.cia.gov/resources/csi/studies-in-intelligence/volume-57-no-1/an-alternative-framework-for-agent-recruitment-from-mice-to-rascls/.

43. Matz, Appel, and Kosinski, "Privacy in the Age of Psychological Targeting."

44. Harry Oinas-Kukkonen and Marja Harjumaa, "Persuasive Systems Design: Key Issues, Process Model, and System Features," *Communications of the Association for Information Systems* 24, no. 1 (2009): 28, https://aisel.aisnet.org/cais/vol24/iss1/28/.

45. Mona Alhasani et al., "A Systematic Review of Persuasive Strategies in Stress Management Apps," in *BCSS@ PERSUASIVE* (2020): 1–13, https://ceur-ws.org/Vol-2662/BCSS2020_paper4.pdf; Thales Teixeira, Michel Wedel, and Rik Pieters, "Emotion-Induced Engagement in Internet Video Advertisements," *Journal of Marketing Research* 49, no. 2 (2012): 144–59, https://doi.org/10.1509/jmr.10.0207; Tuka AlHanai and Mohammad Ghassemi, "Predicting Latent Narrative Mood Using Audio and Physiologic Data," *Proceedings of the AAAI Conference on Artificial Intelligence* 31, no. 1 (2017), https://doi.org/10.1609/aaai.v31i1.10625; Robert LiKamWa et al., "Moodscope: Building a Mood Sensor from Smartphone Usage Patterns," in *MobiSys '13: Proceedings of the 11th Annual International Conference on Mobile Systems, Applications, and Services* (New York: Association for Computing Machinery, June 2013), 389–402, https://doi.org/10.1145/2462456.2464449; Bokai Cao et al., "DeepMood: Modeling Mobile Phone Typing Dynamics for Mood Detection," in *KDD '17: Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (New York: Association for Computing Machinery, 2017), 747–55, https://doi.org/10.1145/3097983.3098086; Gregory Park et al., "Automatic Personality Assessment Through Social Media Language," *Journal of Personality and Social Psychology* 108, no. 6 (2015): 934–52, https://doi.org/10.1037/pspp0000020.

46. Bernd Marcus, Franz Machilek, and Astrid Schütz, "Personality in Cyberspace: Personal Web Sites as Media for Personality Expressions and Impressions," *Journal of Personality and Social Psychology* 90, no. 6 (2006): 1014–31, https://doi.org/10.1037/0022-3514.90.6.1014; Michal Kosinski, David Stillwell, and Thore Graepel, "Private Traits and Attributes Are Predictable from Digital Records of Human Behavior," *Proceedings of the National Academy of Sciences* 110, no. 15 (2013): 5802–5, https://doi.org/10.1073/pnas.12187721; Wu Youyou, Michal Kosinski, and David Stillwell, "Computer-Based Personality Judgments Are More Accurate Than Those Made by Humans," *Proceedings of the National Academy of Sciences* 112, no. 4 (2015): 1036–40, https://doi.org/10.1073/pnas.1418680112; Daniele Quercia et al., "Our Twitter Profiles, Our Selves: Predicting Personality with Twitter," in *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing* (New York: IEEE, 2011), 180–85, https://doi.org/10.1109/PASSAT/SocialCom.2011.26; Michal Kosinski et al., "Mining Big Data to Extract Patterns and Predict Real-Life Outcomes," *Psychological Methods* 21, no. 4 (2016): 493–506, https://doi.org/10.1037/met0000105; Tal Yarkoni, "Personality in 100,000 Words: A Large-Scale Analysis of Personality and Word Use Among Bloggers," *Journal of Research in Personality* 44, no. 3 (2010): 363–73, https://doi.org/10.1016%2Fj.jrp.2010.04.001; Alhasani et al., "A Systematic Review of Persuasive Strategies in Stress Management Apps"; Andrew Schwartz et al., "Personality, Gender, and Age in the Language of Social Media: The Open-Vocabulary Approach," *PloS ONE* 8, no. 9 (2013): e73791, https://doi.org/10.1371/journal.pone.0073791; Joe J. Gladstone, Sandra C. Matz, and Alain Lemaire, "Can Psychological Traits Be Inferred From Spending? Evidence from Transaction Data," *Psychological Science* 30, no. 7 (2019): 1087–96; Crisitina Segalin et al., "The Pictures We Like Are Our Image: Continuous Mapping of Favorite Pictures into Self-Assessed and Attributed Personality Traits," *IEEE Transactions on Affective Computing* 8, no. 2 (April-June 2017): 268–85, https://doi.org/10.1109/TAFFC.2016.2516994.

47. Marengo and Montag, "Digital Phenotyping of Big Five Personality"; Appel and Matz, "Psychological Targeting in the Age of Big Data."

48. Appel and Matz, "Psychological Targeting in the Age of Big Data"; Maschmeyer, "A New and Better Quiet Option?"

49. David Evans et al., "Facebook's 8 Fundamental Hooks and 6 Basic User Types: A Psychographic Segmentation," *Four Peaks Review* 2 (2012): 36–54, https://digital.lib.washington.edu/researchworks/bitstream/handle/1773/47843/2-3.pdf; Christopher Wylie, *Mindf*ck: Inside Cambridge Analytica's Plot to Break the World* (London: Profile Books, 2019).

50. Bakir, "Psychological Operations in Digital Political Campaigns."

51. Wylie, *Mindf*ck*.

52. Bakir, "Psychological Operations in Digital Political Campaigns."

53. Kathleen Hall Jamieson, *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't, and Do Know* (New York: Oxford University Press, 2020); Nahal Kazemi, "Spies, Trolls, and Bots: Combating Foreign Election Interference in the Marketplace of Ideas," *Voting Rights and Democracy Forum* 2, no. 2 (2024): 227, https://ir.lawnet.fordham.edu/vrdf/vol2/iss2/3/.

54. Jason A. Spitaletta, "Sabotage, Subversion, and Nonviolent Resistance: A Nuanced Approach to Special Warfare in Great Power Competition," chap. 3 in *SOF Paradigm in Great Power Competition*, ed. Spencer Meredith III (Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense, 2019), https://nsiteam.com/social/wp-content/uploads/2019/11/SOF-Paradigm_Invited-Perspective_FINAL3.pdf.

55. "Unified Combatant Command for Special Operations Forces," 10 U.S.C. § 167 (2016), https://www.law.cornell.edu/uscode/text/10/167; Jason A. Spitaletta, "Neuropsychological Operations: A Concept for Counter-Radicalization," in *Topics for Operational Considerations: Insights from Neurobiology & Neuropsychology on Influence and Extremism—An Operational Perspective*, ed. Marty Reynolds and David Lyle (Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense, 2013), 71–83, https://apps.dtic.mil/sti/citations/AD1093605.

56. Burkett, "An Alternative Framework for Agent Recruitment: From MICE to RASCLS."

57. Spitaletta, "Human Factors Considerations of Undergrounds in Cyber Resistance"; Maschmeyer, *Subversion*.

58. Maschmeyer, *Subversion*.

59. Yarkoni, "Psychoinformatics"; Christian Montag, Éilish Duke, and Alexander Markowetz, "Toward Psychoinformatics: Computer Science Meets Psychology," *Computational and Mathematical Methods in Medicine* (2016), https://doi.org/10.1155/2016/2983685.

60. Thomas R. Insel, "Digital Phenotyping: A Global Tool for Psychiatry," *World Psychiatry* 17, no. 3 (October 2018): 276–77, https://doi.org/10.1002%2Fwps.20550; Luke Stark, "Algorithmic Psychometrics and the Scalable Subject," *Social Studies of Science* 48, no. 2 (2018): 204–31, https://doi.org/10.1177/0306312718772094; Ramus H. Birk and Gabrielle Samuel, "Can Digital Data Diagnose Mental Health Problems? A Sociological Exploration of 'Digital Phenotyping,'" *Sociology of Health and Illness* 42, no. 8 (November 2020): 1873–87, https://doi.org/10.1111/1467-9566.13175.

61. Yunji Liang, Xiaolong Zheng, and Daniel D. Zeng, "A Survey on Big Data-Driven Digital Phenotyping of Mental Health," *Information Fusion* 52 (December 2019): 290–307, https://doi.org/10.1016/j.inffus.2019.04.001.

62. Ibid.

63. Ibid.

64. Ibid.

65. Ibid.

66. Henry A. Murray and Donald W. MacKinnon, "Assessment of OSS Personnel," *Journal of Consulting Psychology* 10, no. 2 (1946): 76, https://doi.org/10.1037/h0057480.

67. Bram M. Fridhandler, "Conceptual Note on State, Trait, and the State–Trait Distinction," *Journal of Personality and Social Psychology* 50, no. 1 (1986): 169, https://doi.org/10.1037/0022-3514.50.1.169.

68. Joanne Hinds and Adam N. Joinson, "Digital Data and Personality: A Systematic Review and Meta-Analysis of Human Perception and Computer Prediction," *Psychological Bulletin* 150, no. 6 (2024): 727–66, https://psycnet.apa.org/fulltext/2024-82524-001.pdf.

69. Esther Hanssen et al., "An Ecological Momentary Intervention Incorporating Personalised Feedback to Improve Symptoms and Social Functioning in Schizophrenia Spectrum Disorders," *Psychiatry Research* 284 (February 2020): 112695, https://doi.org/10.1016/j.psychres.2019.112695.

70. Shlomo Berkovsky, Jill Freyne, and Harri Oinas-Kukkonen, "Influencing Individually: Fusing Personalization and Persuasion," *ACM Transactions on Interactive Intelligent Systems* 2, no. 2 (2012): 9, https://doi.org/10.1145/2209310.2209312; Fogg, *Persuasive Technology*; Matz, Appel, and Kosinski, "Privacy in the Age of Psychological Targeting"; Rita Orji et al., "Personalizing Persuasive Technologies Workshop 2020," *Persuasive 2020 Adjunct Proceedings* 2629 (2020), http://ceur-ws.org/Vol-2629/1_workshop_orji.pdf.

71. Robert C. Jones, "Deterring 'Competition Short of War': Are Gray Zones the Ardennes of Our Modern Maginot Line of Traditional Deterrence?," Small Wars Journal, 14 May 2019, https://smallwarsjournal.com/jrnl/art/deterring-competition-short-war-are-gray-zones-ardennes-our-modern-maginot-line; Erica D. Lonergan and Jacqelyn Schneider, "The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation," *Journal of Cybersecurity* 9, no. 1 (2023): tyad006, https://doi.org/10.1093/cybsec/tyad006; Emma Schroeder, Stewart Scott, and Trey Herr, "Victory Reimagined: Toward a More Cohesive US Cyber Strategy" (Washington, DC: Atlantic Council, June 2022), https://www.atlanticcouncil.org/wp-content/uploads/2022/06/Victory-reimagined-Toward-a-more-cohesive-US-cyber-strategy.pdf.

72. Herbert Lin, "Doctrinal Confusion and Cultural Dysfunction in DoD," *Cyber Defense Review* 5, no. 2 (Summer 2020): 89–108, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2288578/doctrinal-confusion-and-cultural-dysfunction-in-dod/.

73. Antonia Chayes, "Rethinking Warfare: The Ambiguity of Cyber Attacks," *Harvard National Security Journal* 6 (2015), 474–519, https://harvardnsj.org/wp-content/uploads/2015/06/Chayes.pdf.

74. IEEE Standards Association, *Guide for IEEE Standards for Policy Makers* (New York: IEEE Standards Association, 11 May 2020), https://standards.ieee.org/wp-content/uploads/import/documents/other/policymakers-guide-to-standards.pdf.

75. Jason Spitaletta, ed., *White Paper on Bio-Psycho-Social Applications to Cognitive Engagement* (Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense, October 2016), https://apps.dtic.mil/sti/pdfs/AD1092269.pdf; Mica R. Endsley, "Final Reflections: Situation Awareness Models and Measures," *Journal of Cognitive Engineering and Decision Making* 9, no. 1 (2015): 101–11, https://doi.org/10.1177/1555343415573911.

76. The term "human factors" has a rather broad set of interpretations depending on the context in which the phrase is used. Robert W. Proctor and Trisha van Zandt define the field as "the scientific discipline concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance." Robert W. Proctor and Trisha van Zandt, *Human Factors in Simple and Complex Systems*, 2nd ed. (Boca Raton, FL: CRC Press, 2008). This definition, while comprehensive, is not necessarily congruent with how "human factors" has historically been used in information operations, now operations in the information environment doctrine, policy, and practice. Instead, the intelligence community definition seems more appropriate for the purposes of this article. The intelligence community defines human factors analysis as "the psychological, cultural, behavioral, and other human attributes that influence decision-making, the flow of information, and the interpretation of information by individuals and groups at any level in any state or organization." Director of Central Intelligence Directive 7/3, *Information Operations and Intelligence Community Related Activities* (Washington, DC: CIA, 1 July 1999), 10, https://www.cia.gov/readingroom/docs/DIRECTOR%20OF%20CENTRAL%20INTEL%5B15812646%5D.pdf.

77. Alessandro Pollini et al., "Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach," *Cognition, Technology & Work* 24, no. 2 (2022): 371–90, https://doi.org/10.1007/s10111-021-00683-y; Kathleen M. Carley, "Social Cybersecurity: An Emerging Science," *Computational and Mathematical Organization Theory* 26, no. 4 (2020): 365–81, https://doi.org/10.1007/s10588-020-09322-9.

78. Stoney Trent et al., "Cyberspace Operations and the People Who Perform Them," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 60, no. 1 (2016): 216–17, https://doi.org/10.1177/1541931213601048; Cebo Daniel and Jason R. Sipper, "Hacking Humans: The Art of Exploiting Psychology in the Digital Age," *Journal of Research and Development* 10, no. 2 (2023): 224, https://www.longdom.org/open-access/hacking-humans-the-art-of-exploiting-psychology-in-the-digital-age-101458.html; Phillip Arceneaux and Moriah Harman, "Social Cybersecurity," *Journal of Information Warfare* 20, no. 3 (2021): 24–43, https://

www.jinfowar.com/journal/volume-20-issue-3/social-cybersecurity-policy-framework-addressing-computational-propaganda.

79. Matthew J. Flynn, "Cyber Rollback: Popular Resistance in the Cyber Age," *Journal of Strategic Security* 16, no. 4 (2023): 8, https://doi.org/10.5038/1944-0472.16.4.2128.

80. Fuchs, "The Internet as a Self-Organizing Socio-Technological System."

81. Youyou, Kosinski, and Stillwell, "Computer-Based Personality Judgments Are More Accurate Than Those Made by Humans"; Marengo and Montag, "Digital Phenotyping of Big Five Personality."

82. Milton Mueller and Karl Grindal, "Information as Power: Evolving US Military Information Operations," *Cyber Defense Review* 7, no. 2 (Spring 2022): 79–98, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/3034105/information-as-power-evolving-us-military-information-operations/; John Whiteaker and Sami Valkonen, "Cognitive Warfare: Complexity and Simplicity," chap. 11 in *Cognitive Warfare: The Future of Cognitive Dominance*, ed. Bernard Claverie et al. (Neuilly-sur-Seine, FR: NATO Collaboration Support Office, 2022), https://hal.science/hal-03635948/document.

83. Stefan Varga et al., "Automated Text Analysis for Intelligence Purposes: A Psychological Operations Case Study," in *Open-Source Intelligence and Cyber Crime: Social Media Analytics*, ed. Mohammad A. Tayebi et al. (Cham, SU: Springer 2020), 221–51, https://doi.org/10.1007/978-3-030-41251-7_9; Chaveso Cook, "PSYOP, CYBER, and Internet Influence," *Journal of Information Warfare* 21, no. 2 (2022): 95–104, https://www.jinfowar.com/journal/volume-21-issue-2/psyop-cyber-internet-influence-firing-digital-bullets.

84. Jonathan Z. Bakdash, Diego Pizzocaro, and Alun Preece, "Human Factors in Intelligence, Surveillance, and Reconnaissance: Gaps for Soldiers and Technology Recommendations," in *2013 IEEE Military Communications Conference* (New York: IEEE, 2013), https://users.cs.cf.ac.uk/A.D.Preece/publications/download/milcom2013.pdf.

85. Kota Numada et al., "Perceiving Human Psychological Consistency: Attack Detection Against Advanced Persistent Social Engineering," in *International Conference on Emerging Internet, Data & Web Technologies* (Cham, SU: Springer Nature Switzerland, February 2024), 152–62, https://doi.org/10.1007/978-3-031-53555-0_15.

86. Stephen G. Fogarty and Jamie O. Nasi, "Special Operations Forces Truths—Cyber Truths," *Cyber Defense Review* 1, no. 2 (Fall 2016): 19–28, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR-FALL2016.pdf?ver=2017-03-27-130219-357.

87. Fuchs, "The Internet as a Self-Organizing Socio-Technological System."

88. Richard J. Aldrich, "From SIGINT to Cyber: A Hundred Years of Britain's Biggest Intelligence Agency," *Intelligence and National Security* 36, no. 6 (2021): 910–17, https://doi.org/10.1080/02684527.2021.1899636.

89. Brian Hamel, "Reframing the Special Operations Forces-Cyber-Space Triad: Special Operations' Contributions to Space Warfare," *Military Review* 104-SE (March 2024): 121–29, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/March-2024/Cyber-Space-Triad/SOF-Contributions-to-Space-UA.pdf.

90. U.S. Army John F. Kennedy Special Warfare Center and School (website), accessed 13 September 2024, https://www.swcs.mil; Guillaume Beaurpere, Jeremy Mushtare, and Bradley Bloom, "PSYWAR School for the Range of Military Operations," *Special Warfare* 36, no. 2 (January 2024): 24–27, https://media.defense.gov/2024/Jan/10/2003373826/-1/-1/1/SWM_JAN%2024_VOL%2036%20ISSUE%202.PDF.

91. Beaurpere, Mushtare, and Bloom, "PSYWAR School for the Range of Military Operations."

92. "SOF Truths," U.S. Special Operations Command, accessed 21 October 2024, https://www.socom.mil/about/sof-truths. The fifth SOF truth states that "most special operations require non-SOF support." The operational effectiveness of our deployed forces cannot be, and never has been, achieved without being enabled by our joint service partners. The support Air Force, Army, Marine, and Navy engineers, technicians, intelligence analysts, and the numerous other professions that contribute to SOF, have substantially increased our capabilities and effectiveness throughout the world.

93. Joint Special Operations University (JSOU) (website), accessed 13 September 2024, https://jsou.edu.

94. "National Resistance Course," JSOU, accessed 13 September 2024, https://jsou.edu/Courses/Index/334; "Joint Unconventional Warfare Operations Course," JSOU, accessed 13 September 2024, https://jsou.edu/Courses/Index/338; "SOF Sensitive Activities Foundations," JSOU, accessed 13 September 2024, https://jsou.edu/Courses/Index/8; "Special Operations Forces – Influence and Operations in the Information Environment," JSOU, accessed 13 September 2024, https://jsou.edu/Courses/Index/652.

95. "Cyberspace and Special Operations Forces," JSOU, accessed 13 September 2024, https://jsou.edu/Courses/Index/274; "TSOC Cyber Planner Course," JSOU, accessed 13 September 2024, https://jsou.edu/Courses/Index/381.

96. "Anthony G. Oettinger School of Science and Technology Intelligence," National Intelligence University, accessed 13 September 2024, https://www.ni-u.edu/school-of-science-and-technology-intelligence/.

97. BinHui Tang et al. "Advanced Persistent Threat Intelligent Profiling Technique: A Survey," *Computers and Electrical Engineering* 103 (October 2022): 108261, https://doi.org/10.1016/j.compeleceng.2022.108261.

98. Martti Lehto, "APT Cyber-Attack Modelling: Building a General Model," *17th International Conference on Cyber Warfare and Security* 17, no. 1 (March 2022): 121–29, https://doi.org/10.34190/iccws.17.1.36.

99. Fridman, *Russian "Hybrid Warfare"*; Sven Herpig and Thomas Reinhold, "Spotting the Bear: Credible Attribution and Russian Operations in Cyberspace," in *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, ed. Nicu Popescu and Stanislov Secrieru, Chaillot Paper No. 148 (October 2018), 33–42; Lev R. Klebanov and Svetlana V. Polubinskaya, "Computer Technologies for Committing Sabotage and Terrorism," *RUDN Journal of Law* 24, no. 3 (2020): 717–34, http://journals.rudn.ru/law/article/viewFile/24569/18587; Adam Klus, "Myatezh Voina: The Russian Grandfather of Western Hybrid Warfare," Small Wars Journal, 10 July 2016, https://smallwarsjournal.com/jrnl/art/myatezh-voina-the-russian-grandfather-of-western-hybrid-warfare.

100. Sandworm is an advanced persistent threat that has been attributed to Russia's General Staff Main Intelligence Directorate Main Center for Special Technologies military unit 74455. For additional information, see "Sandworm Team," MITRE, accessed 13 September 2024, https://attack.mitre.org/groups/G0034/; Martti Lehto, "Cyber Warfare and War in Ukraine," *Journal of Information Warfare* 22, no. 1 (2023): 61–75, https://www.jinfowar.com/journal/volume-22-issue-1/cyber-warfare-war-ukraine; Rod

Thornton and Marina Miron, "Winning Future Wars: Russian Offensive Cyber and Its Vital Importance," *Cyber Defense Review* 7, no. 3 (2022), 117–35, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/3129508/winning-future-wars-russian-offensive-cyber-and-its-vital-importance/.

101. J. E. J. Buckman et al., "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 (August 2018): 13–38, https://doi.org/10.1016/j.cpr.2018.07.005; Alec Buchanan, "Risk and Dangerousness," *Psychological Medicine* 29, no. 2 (March 1999): 465–73, https://doi.org/10.1017/S0033291798008101; Insel, "Digital Phenotyping"; Bader Al-Sada, Alireza Sadighian, Gabriele Oligeri, "Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database," *IEEE Access* 12 (December 2023): 1217–34, https://doi.org/10.1109/ACCESS.2023.3344680.

102. Liang, Zheng, and Zeng, "A Survey on Big Data-Driven Digital Phenotyping of Mental Health."

103. Beth B. Tigges et al., "Measuring Quality and Outcomes of Research Collaborations: An Integrative Review," *Journal of Clinical and Translational Science* 3, no. 5 (2019): 261–89, https://doi.org/10.1017/cts.2019.402.

104. Lin, "Doctrinal Confusion and Cultural Dysfunction in DoD"; Christopher Whyte and Brian Mazanec, *Understanding Cyber-Warfare: Politics, Policy and Strategy* (New York: Routledge, 2023); Jean-Loup Samaan, "Cyber Command: The Rift in US Military Cyber-Strategy," *RUSI Journal* 155, no. 6 (2010): 16–21, https://doi.org/10.1080/03071847.2010.542664; Cook, "PSYOP, CYBER, and Internet Influence"; Arceneaux and Harman, "Social Cybersecurity"; Otto Fiala, Kirk Smith, and Anders Löfberg, *Resistance Operating Concept* (MacDill Air Force Base, FL: JSOU Press, 2020), https://jsou.edu/Press/PublicationDashboard/25.

105. Nur Ilzam Che Mat et al., "A Systematic Literature Review on Advanced Persistent Threat Behaviors and Its Detection Strategy," *Journal of Cybersecurity* 10, no. 1 (2024): tyad023, https://doi.org/10.1093/cybsec/tyad023.

106. "Our Mission and Vision," U.S. Cyber Command, accessed 13 September 2024, https://www.cybercom.mil/About/Mission-and-Vision/.

107. Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41, no. 3 (2017): 72–109, https://doi.org/10.1162/ISEC_a_00267; Jennifer Leigh Phillips, "Tactical Maneuver in the Cyber Domain," *Joint Force Quarterly* 93, no. 2 (2019): 14–20, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1841055/tactical-maneuver-in-the-cyber-domain-dominating-the-enemy/.

108. Maschmeyer, Subversion; Gary D. Brown, "The Cyber Longbow & Other Information Strategies: U.S. National Security and Cyberspace," *Journal of Law and International Affairs* 5, no. 1 (April 2017): 1–28, https://elibrary.law.psu.edu/jlia/vol5/iss1/3.

109. U.S. Department of Defense, *Summary of 2023 Cyber Strategy of the Department of Defense* (Washington, DC: U.S. Department of Defense, 2023), https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF; Cyber National Mission Force Public Affairs, "About the Cyber National Mission Forces," U.S. Cyber Command, 6 December 2023, https://www.cybercom.mil/Media/News/Article/3610711/about-the-cyber-national-mission-forces/.

110. Ryan Shandler, Michael L. Gross, and Daphna Canetti, "Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis," *Journal of Global Security Studies* 8, no. 1 (March 2023): ogac042, https://doi.org/10.1093/jogss/ogac042; Cook, "PSYOP, CYBER, and Internet Influence."

111. Christopher Whyte, "Cyber Conflict or Democracy 'Hacked'? How Cyber Operations Enhance Information Warfare," *Journal of Cybersecurity* 6, no. 1 (2020): tyaa013, https://doi.org/10.1093/cybsec/tyaa013; Maschmeyer, *Subversion*.

112. Fiala, Smith, and Löfberg, *Resistance Operating Concept*; Robert S. Burrell and John Collison, "A Guide for Measuring Resiliency and Resistance," *Small Wars & Insurgencies* 35, no. 1 (2024): 147–72, https://doi.org/10.1080/09592318.2023.2292942.

113. Nicholas H. Vidal, "Enemy at the Gates: A Strategic Cultural Analysis of Russian Approaches to Conflict in the Information Domain," *Journal of Advanced Military Studies* 14, no. 2 (Fall 2023): 49–76, https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JAMS-vol-14-no-2/Enemy-at-the-Gates/; Andrew S. Bowen, "Russia and Breakaway Republics," chap. 29 in *Routledge Handbook of Proxy Wars*, ed. Assaf Moghadam, Vladimir Rauta, and Michel Wyss (New York: Routledge, 2023).

114. Elspeth Van Veeren, Clare Stevens, and Amaha Senu, "Secrecy Games, Power, and Resistance in Global Politics," *Review of International Studies* (2024): 1–18, https://doi.org/10.1017/S0260210524000275.

115. Jordan Richard Schoenherr, "The First Total War and the Sociotechnical Systems of Warfare," *IEEE Technology and Society Magazine* 42, no. 3 (September 2023): 42–56, https://doi.org/10.1109/MTS.2023.3299315.

116. Pascal Brangetto and Matthijs A. Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations," in *2016 8th International Conference on Cyber Conflict (CyCon)* (New York: IEEE, May 2016), 113–26, https://doi.org/10.1109/CYCON.2016.7529430.

117. Paulo Shakarian, Jana Shakarian, and Andrew Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (New York: Elsevier Science, 2013).

118. Bredenkamp and Grzegorzewski, "Supporting Resistance Movements in Cyberspace."

119. Maschmeyer, *Subversion*.

120. Margaret W. Smith and Thomas Dean, "The Irregulars: Third-Party Cyber Actors and Digital Resistance Movements in the Ukraine Conflict," in *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (New York: IEEE, May 2023), 103–19, https://doi.org/10.23919/CyCon58705.2023.10182061; Oren Barak, Amit Sheniak, and Assaf Shapira, "The Shift to Defence in Israel's Hybrid Military Strategy," *Journal of Strategic Studies* 46, no. 2 (2023): 345–77, https://doi.org/10.1080/01402390.2020.1770090.

121. Hamel, "Reframing the Special Operations Forces-Cyber-Space Triad."

122. Jelena Vićić and Erik Gartzke, "Cyber-Enabled Influence Operations as a 'Center of Gravity' in Cyberconflict: The Example of Russian Foreign Interference in the 2016 US Federal Election," *Journal of Peace Research* 61, no. 1 (2024): 10–27, https://doi.org/10.1177/00223433231225814.

123. R. David Edelman, *Rethinking Cyber Warfare: The International Relations of Digital Disruption* (New York: Oxford University Press, 2024).

124. Duggan, "Strategic Development of Special Warfare in Cyberspace"; Charon and Vilmer, *Chinese Influence Operations*.

125. Klus, "Myatezh Voina"; Ian J. Courter, "Russian Preinvasion Influence Activities in the War with Ukraine," *Military Review* 102,

no. 5 (September-October 2022): 16–37, https://www.armyupress.army.mil/Portals/7/PDF-UA-docs/Courter-2022-UA.pdf.

126. Vidal, "Enemy at the Gates"; Bowen, "Russia and Breakaway Republics."

127. Fridman, *Russian "Hybrid Warfare."*

128. U.S. Cyber Command PAO, "CYBER 101–Defend Forward and Persistent Engagement," U.S. Cyber Command, 25 October 2022, https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/; Maschmeyer, Subversion.

129. Appel and Matz, "Psychological Targeting in the Age of Big Data"; Spitaletta, "Remote Behavioral Assessment: Political Psychology Methods," in *What Do Others Think and How Do We Know What They Are Thinking?*, ed. Mariah Yager (Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense, March 2018), 57–60, https://nsiteam.com/social/wp-content/uploads/2018/03/White-Paper_What-Do-Others-Think_March2018_FINAL.pdf.

130. Jason Spitaletta, *Operational Cyberpsychology: Adapting a Special Operations Model for Cyber Operations* (Washington, DC: Strategic Multilayer Assessment Office, Office of the Secretary of Defense, June 2021), https://apps.dtic.mil/sti/pdfs/AD1142095.pdf.

131. Spitaletta, "Neuropsychological Operations."

132. Robert C. Jones, "Strategic Influence: Applying the Principles of Unconventional Warfare in Peace," Small Wars Journal, 15 July 2021, https://smallwarsjournal.com/blog/strategic-influence-applying-principles-unconventional-warfare-peace-robert-c-jones; Thompkins, "Special Forces Profession."