The Case for the Sixth Domain of War: Psychological Warfare in the Age of Advanced Technology

Bethany Vailliant and Media Ajir

Abstract

Wills win wars. A country at war must have and maintain the support of its people to achieve victory. Targeting will, using advanced information technology (IT), presents a new vulnerability for the United States. Literature in this field has largely ignored the psychological effects of new, cyber-enabled tools; therefore, the concept of information warfare has tended to favor primarily technical infrastructure. This oversight has caused state mismanagement of what was once carefully managed disruption by the United States. Tools and techniques have been refined to transcend effects beyond material goods, entering our minds and manipulating our behavior. The weaponization of these tools urges us to consider the sufficiency of our current framework for warfare—the five domains. This research argues that due to the disruptive change in the delivery method of information, a sixth, psychological domain should be established to properly assess and operationalize effects going forward.

Keywords: cyberspace, psychological domain, psychological warfare, information warfare, fifth domain, sixth domain

El caso del sexto dominio de la guerra: guerra psicológica en la era de la tecnología avanzada

Resumen

Las voluntades ganan guerras. Un país en guerra debe tener y mantener el apoyo de su gente para lograr la victoria. La focalización, utilizando tecnología de información avanzada, presenta una nueva vulnerabilidad para los Estados Unidos. La literatura en este campo ha ignorado en gran medida los efectos psicológicos de las nuevas herramientas cibernéticas; por lo tanto, el concepto de guerra de información ha tendido a favorecer principalmente la infraestructura

 doi: 10.18278/gsis.5.1.2

técnica. Este descuido ha provocado una mala gestión estatal de lo que antes era una interrupción cuidadosamente manejada por Estados Unidos. Las herramientas y técnicas se han refinado para trascender los efectos más allá de los bienes materiales, entrar en nuestras mentes y manipular nuestro comportamiento. El armamento de estas herramientas nos insta a considerar la suficiencia de nuestro marco actual para la guerra: los cinco dominios. Esta investigación argumenta que, debido al cambio disruptivo en el método de entrega de información, se debe establecer un sexto dominio psicológico para evaluar y operacionalizar adecuadamente los efectos en el futuro.

Palabras clave: Ciberespacio, dominio psicológico, guerra psicológica, guerra de información, quinto dominio, sexto dominio

第六战争领域案例：先进科技时代下的心理战

摘要

意志赢得战争。战争中的国家必须拥有人民支持，并保持这种支持以获得胜利。使用先进信息技术对意志发起攻击，为美国增添了一个新的弱点。该领域文献在很大程度上忽视了新型网络工具带来的心理效果；因此，信息战概念往往主要偏好技术基础设施。这一疏忽已导致各州在信息中断方面管理不善，后者曾一度由美国仔细管控。工具和技术经过改良，产生的影响已超越有形物品，进入我们的思维并操纵我们的行为。这些工具的武器化敦促我们衡量当前对五个战争领域所提出的框架的充足性。本研究主张，鉴于信息交付方式中的破坏性变化，应建立第六领域，即心理领域，以对未来产生的效果进行正确评估和操作化。

关键词：网络空间，心理领域，心理战，信息战，第五领域，第六领域

Introduction

As warfare has modernized, its disruptive nature continues to take advantage of advanced technologies, especially those within the information sphere. According to the Department of Defense (DoD), "Information is a powerful tool to influence, disrupt, corrupt, or usurp an adversary's ability to make and share decisions" (Joint Chiefs of Staff 2014).

Such disruptions began with the invention of mass printing in the fifteenth century, when books became available to large swaths of people, arguably igniting civilization's leap forward into the current era, "including but not limited to the Reformation, the Enlightenment, the steam engine, journalism, modern literature, modern medicine, and modern democracy" (Marantz 2019).

While the chains that shackled the free flow of information were coming undone, so too did misinformation break free as its opposite. The gatekeepers of knowledge started to shift from princes and priests, to new entrepreneurs who had the financial means to access and purchase the powerful new technology of the printing press.

In the twentieth century, with the advent of the internet, new liberators of information have emerged. The dawn of this new era was described with the same excitement as that of the printing press. Unlike the print media however, where gatekeepers—and the law in many places—had final say on what was published and what was not, this new means of information sharing was unregulated/under-regulated and full of advocates for an internet based on the liberation of knowledge and power. However, while stakeholders in this era have debated the antiquities of free speech and its nuances, what has been ignored almost entirely is the potential for a new kind of warfare targeting the human mind, amplified by new technology and tools of communication.

Over the years, while the United States has been building up its unmatched and largely physical military strength, its adversaries have been busy searching out and filling whatever asymmetric power gaps they are able. As we argued in our previous article, *Russian Information Warfare: Implications for Deterrence Theory*, a common development of state actors with fewer defense resources has led to the development of tools of power that are low cost and high impact (Ajir and Vailliant 2018). The United States (and many other Western states for that matter) is still unprepared to deal with this new reality.

The Joint Chiefs of Staff (2014) clearly call out the problem:

> The instruments of national power (diplomatic, informational, military, and economic) provide leaders in the United States with the means and ways of dealing with crises around the world. Employing these means in the information environment requires the ability to securely transmit, receive, store, and process information in near real time. The nation's state and non-state adversaries are equally aware of the significance of this new technology, and will use information-related capabilities (IRCs) to gain advantages in the information environment, just as they would use more traditional military technologies to gain advantages in other operational environments. These realities have transformed the information environment into a battlefield,

which poses both a threat to the Department of Defense (DOD), combatant commands (CCMDs), and Service components and serves as a force multiplier when leveraged effectively.

This paper argues for the recognition of a new, psychological domain in order to create the framework to understand the target effects of such new tools. The **delivery method** for information is rapidly changing, making its potential **effects** more detrimental and/or lethal, especially in a world of reemerging great power competition. Therefore, the establishment of a sixth domain of warfare is necessary as we move forward into the twenty-first century. In order to make the case for its recognition, we will define the necessary components of a domain, identify where the cyber domain ends and where the psychological domain begins, and illustrate the implications of advanced technology on warfare in the new domain. At its core, this research seeks to explore why a psychological domain has not yet been recognized, and to argue that the time to do so is now.

Information Operations in the Age of Advanced Technology

The United States' military superiority has largely been defined by its unique ability to navigate and dominate its enemies in the classical domains of warfare. Military operations have fundamentally changed throughout the twentieth century to adapt to new technologies. Historically, operations were dominated by the two domains of land and sea. The advent of powered flight in 1904 resulted in the creation of the third domain, air, and fifty years after the first powered flight, the US Air Force was born. The space domain was acknowledged not long after, with the advent of Ronald Reagan's Strategic Defense Initiative in the 1980s (Allen and Gilbert 2018). Finally, the Pentagon's declaration of cyberspace as the fifth domain of warfare came after a massive DoD network compromise in 2008 (Horning 2011).

Despite the importance of domains to war, a clear and concise definition does not seem to have been put forth in military doctrine. We recognize that the very concept of "domain" may be problematic to some, as they all cannot be compared equally. The conventional domains of air, land, and sea are certainly more physical in nature than the cyber domain and, while space may also be physical, it has so far proven to be most useful for virtual enabling effects, such as communication, surveillance, and navigation (Heftye 2017). However, "domain" has become such an embedded concept in military thinking that we do not wish to debate its value as a construct. Therefore, we put forward the definition by Patrick Allen and Dennis Gilbert of Johns Hopkins University for consideration:

1) It is a sphere of interest

2) It is a sphere of influence in that activities, functions, and operations can be undertaken in that sphere to accomplish missions

3) It is a sphere that may include the presence of an opponent

4) It is a sphere in which control can be exercised over that opponent.

All of the war domains are nested within the larger information environment. The use of information during wartime or in peacetime operations is not unique to any of the domains. The objective when conducting information operations in any of the domains is to deny, corrupt, or destroy an adversary's information and systems, to defend our own, and to exploit available information to enhance the decision cycle and achieve information superiority (Kovacich and Jones 2006). The Joint Chiefs of Staff (2019) define "information environment" as:

> The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.

Furthermore, it defines "information operations" as:

> The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.

More broadly, "information warfare" generally comprises three functional areas:

- electronic warfare (e.g., jamming communications links, eavesdropping of signals)
- network warfare (where computer networks are the weapons and targets)
- psychological operations (which aims at altering the perceptions of the target audience to be favorable to one's objective) (Brazzoli 2007)

Where the Cyber Domain Begins and Ends

Mapping out cyberspace can assist in visualizing the fifth domain (see Appendix 1). Cyberspace is generally viewed as three layers: physical, logical, and social. Within these three layers are five components: geographic, the physical network, the logical network, cyber persona, and persona. The geographic component refers to the physical location of network elements. The physical network components include all of the hardware and infrastructure required for network operability. The logical layer is technical in nature and consists of the logical connections that exist between devices. The social layer consists of cyber personas, referring to identification on a network, such as email addresses or computer IP addresses, and personas, meaning the actual person behind the network. This top social layer is obviously required, as the fifth domain cannot be navigated without end-to-end users. However, operations conducted with targets in the cyber domain allow only for the effects of the two functional areas of electronic and network warfare, excluding the effects of psychological operations.

The Joint Chiefs of Staff (2019) define "cyberspace" as:

> A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

The tendency to artificially view acts that occur in cyberspace as automatically constituting network and electronic warfare excludes the impacts of virtual connectivity that extend far beyond the underlying infrastructure that makes its existence possible. This, we believe is the first mistake—nowhere in the definition of cyberspace are the human-related tools and effects included. In order to begin untangling the cyber domain from the others, it is first important to understand exactly what the larger objectives of cyber warfare by itself are, and consequently what they are not.

RAND defines "cyber warfare" as follows:

> The actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

Cyberwar and its effects, as defined by the DoD, occur exclusively within the cyber domain, and are by their very nature inseparable from the information systems that magnify the impacts of war in the information environment. Attacks on critical infrastructure (such as railways, hospitals, stock exchanges, airlines, financial systems, oil pipelines, water distribution systems, electric grids, etc.), distributed denial of service (DDoS) attacks (online banking, digital news media, government websites, etc.), malware, ransomware, and data deletion are some of the most prominent examples of methods used to conduct an attack in the cyber domain (Greenberg 2019). The objective of an attack in the cyber domain is to directly target the information itself or the systems on which the information resides.

According to the Geneva Centre for Security Sector Governance, Computer Network Operations (CNO) are comprised of three forms: 1) computer network attacks, which are operations designed to disrupt, deny, degrade, or destroy information on computers or computer networks or the computers or networks themselves, 2) computer network exploitation, which is the retrieving of intelligence-grade data and information from enemy computers by ICT means, and 3) computer network defense, which consists of all measures necessary to protect one's own ICT means and infrastructures. All three CNO forms of activity can take place within cyberspace in a manner that does not rise to the level of impact necessary to constitute an attack or warfare.

While the impacts from cyber warfare are potentially many, the underlying threat that ultimately emanates

from war in the cyber domain is our ever-increasing dependence on the electromagnetic spectrum (EMS), which is the foundation upon which entrance into the virtual space and the storage of information is possible (Schreier 2015). It is the targeting and exploitation of this underlying technological infrastructure that makes the cyber domain distinct from the other domains. The modern world has become so reliant upon cyberspace for all aspects of life that the loss of the ability to operate in cyberspace is potentially crippling in all domains. Indeed, cyberspace enables faster and more efficient transmission of information within and across all of the other domains. Networks, information technology (IT) systems, and computer databases enable national leadership and the military to create a higher level of shared situational awareness, to better synchronize command, control, and intelligence, and to translate information superiority into combat power (Schreier 2015). All types of national-level operations are increasingly reliant on the use of data and information, and virtual transmission through cyberspace allows its ingestion and analysis, sometimes almost instantaneously.

Therefore, we believe that the definition of "cyberspace" offered by the DoD needs to be expanded. While it does correctly state that cyberspace is a part of the broader information environment, its second mistake is that it does not recognize its role as a force multiplier that enhances the effectiveness of the information environment as a whole. For this reason, we offer the following to accurately reflect the true nature of the role of cyberspace:

> A global domain that operates within, **and as an enabler of**, the information environment through the use of the information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

As a result of cyberspace's role in enhancing the effectiveness of the information environment, subsequent cyber-enabled delivery methods of information will continue to evolve. This means effects for psychological operations will require their own domain and the definition of cyberspace will not need to include human-related tools and effects. This is precisely where the cyber domain ends, and where the psychological domain begins. Because while the distinguishing feature of war in the cyber domain is its targeting of the structures that enable cyberspace to function, war in the cyber domain does not include the influence operations that seek to, for example, spread disinformation and propaganda or hurt adversaries by leaking damaging information about them (Greenberg 2019).

Where the Psychological Domain Begins

The human dimensions of information have always existed within the information environment. Often called by another name, "psychological operations" (or PSYOPS) have

often been recognized as one of the core components of information warfare. If psychological operations occur within the human mind and have always existed, why has it not been officially recognized as a domain of war? The answer is that historically, as an instrument of war, influencing public opinion within an enemy state was expensive, slow, data-poor, and attributable (Hwang and Rosen 2017). This is no longer true, and the reason admittedly has everything to do with cyberspace and its underlying foundation of advanced technology.

The combined use of technology with these human-related dimensions exponentially amplifies the influence that a message has on decision-making. If cyber-enabled psychological operations are undertaken with the objective of achieving information superiority, the effects will not be found within cyberspace—they will be found in the sixth, and currently unrecognized psychological domain. While the ultimate target in the cyber domain is the underlying EMS that makes up our virtual world and everything that depends on it to work, it is within the psychological domain that the human mind is targeted through constantly evolving methods of cyber-enabled psychological warfare.

It is important to note that the sixth domain should be called the psychological domain, rather than the cognitive domain. Cognition is "the mental action or process of acquiring knowledge and understanding through thought, experience, and the senses" (*Oxford Online Dictionary*, s.v. "cognition," https://www.lexico.com/en/definition/cognition). This involves the biological and neurological processes linked to attention, executive function, memory, visuospatial function, and language. In contrast, psychological refers to "of, affecting, or arising in the mind; related to the mental and emotional state of a person" (*Oxford Online Dictionary,* s.v. "psychological," https://www.lexico.com/en/definition/psychological). Cognition can be viewed as a faculty of being human that is one aspect of psychology studies. This distinction is important because cyber-enabled information warfare does not attack *only* the underlying cognition of the human brain, but the broader psychology of an individual, including their mental state; perception; cognitive, emotional, and social processes; and behavior. Furthermore, there is a body of research that illustrates how the growing use of technology can affect human cognitive abilities (Wilmer, Sherman, and Chein 2017), such as attention span and memory. Therefore, our cognition is being targeted as an indirect result of peoples' increasing reliance on technology, making us more vulnerable to future targeted cyber-enabled psychological operations.

Using Allen and Gilbert's proposed definition and subsequent components of a domain, the psychological domain has all the required characteristics to be formally recognized. First, the human mind is a sphere of interest for those inclined to manipulate its decision-making processes, behaviors, and emotions. Second, within this sphere, activities, functions, and operations

can be undertaken to accomplish missions—these actions have existed since the beginning of humanity and have exponentially increased along with the expansion of technology. Third, it is a sphere that may include the presence of an opponent—adversaries are increasingly using information operations to gain an advantage within the human mind. Lastly, it is a sphere in which control can be exercised over an opponent, as information warfare tactics aim to deceive, manipulate, and control an opponent's decisions or lack thereof.

In the second component, the psychological and cyber domains are intertwined, making their distinction difficult. This is because the activities, functions, and operations undertaken to influence the human mind in the psychological domain are occurring through cyberspace in the modern information environment (refer to the social layer of cyberspace in Appendix 1). This may be difficult to understand in the traditional sense, since the classical domains of warfare tend to lend themselves to easy delineation. For example, tanks conduct ground warfare, ships belong in the ocean, and planes fly in the air; however, even these relatively straightforward examples demand some scrutiny. All domains have entry and exit points into other domains at some point. Aircraft land on the ground or at sea, and ships dock at land-based ports. Warheads enter space before making their reentry to hit their land-based targets. This differentiation becomes more important as we move away from traditional warfare and towards the more convoluted, virtual spheres of influence. The sphere of influence where the effects actually take place and the end objective are always more important when assigning an operation to a domain of war than whatever activities are necessary to achieve it.

Information can be defined in two ways: facts provided or learned about something or someone and what is conveyed or represented by a particular arrangement or sequence of things (in computing, this is data as processed, stored, or transmitted by a computer). In fact, in Late Middle English, information was known as the "formation of the mind" (*Oxford Online Dictionary*, s.v. "information," https://www.lexico.com/en/definition/information). As stated previously, the information environment is a sphere in which all domains operate. Figure 1 illustrates our proposed model of how information, whether delivered through virtual or non-virtual methods, can be transported and have psychological effects. This manner of visualizing our theory is two-fold. First, it allows cyber-enabled psychological operations to be carried out within its own domain and its effects to have a home. Second, it demonstrates that without a human to cognitively observe and infer what is happening (a cognitive maneuver), none of the other domains matter, and arguably, without people writ large applying their cognition, those domains arguably do not exist. This illustrates that targeting the psychological domain can impact all actions in the other domains downstream.

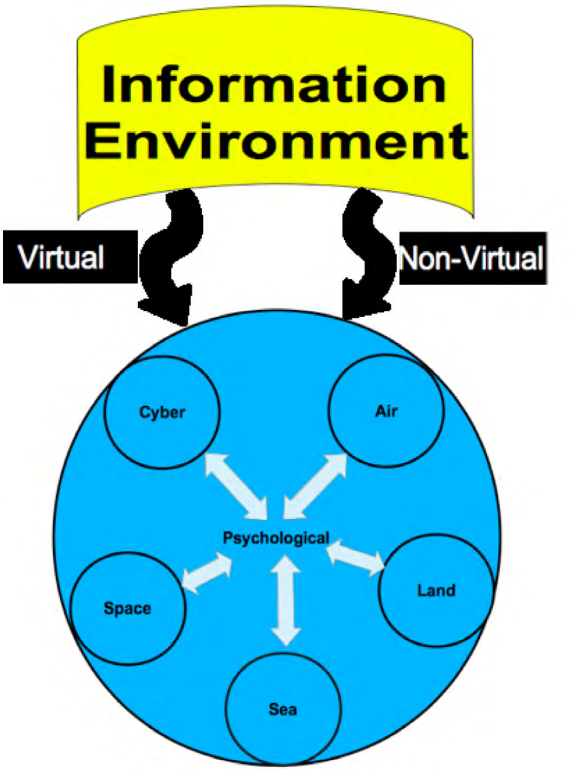


Figure 1. The information environment spans across all war domains, enhanced by the use of cyber-enabled (virtual) delivery methods.

Cyberspace gives states and independent groups a **direct pathway into the hearts and minds of individual citizens through the internet.** For this reason, "cyber-enabled" psychological war in the psychological domain shares many characteristics of the cyber domain, such as low cost of entry, the ability to be endlessly replicated, the difficulty of attribution, and the odds currently being in favor of the offense over the defense. Within the larger information environment, activities undertaken in cyberspace are a pathway into the human mind, enhancing, but not solely enabling, the activities, functions, and operations that an adversary undertakes to achieve its objectives. Just as an intercontinental ballistic missile allows nuclear warheads to be guided to their targets thousands of miles away, the internet allows messages to be carried across oceans right into our pockets. This analogy, although oversimplified, is no less powerful—methods of delivery that minimize the time it takes and the distance a message has to travel can create catastrophic outcomes for those on the receiving end. Regardless of the way that information travels, however, the most important consideration should always be what end-state the adversary intends to create to achieve its overall mission.

Methods of Cyber-Enabled Psychological Warfare

In his book *Thinking, Fast and Slow*, Daniel Kahneman argues that the way the human mind deals with information is broken down into two systems: "System 1" and "System 2." System 1 operates automatically and quickly, with little or no effort and no sense of voluntary control; System 2 allocates attention to the mental activities that demand it, including complex computations. System 1, while useful to people as a way to deal with the chaos of the world around them, is often overrun with subconscious biases. Ideally, that is when System 2 steps in to correct the mistakes of System 1; however, according to Kahneman (2011), "constantly questioning our own thinking would be impossibly tedious, and System 2 is much too slow and inefficient to serve as a substitute for System 1 in making routine decisions."

Applying Kahneman's two systems theory to the psychological domain illustrates how cyber-enabled information warfare tactics can take advantage of the inherent weaknesses of the human mind to further agendas and influence the perceptions and actions of individuals in the real world. There are four main types of cyber-enabled methods that can influence the human mind in a way that makes it rely on the quick and impulsive tendencies of System 1 rather than System 2.

1) Disinformation dissemination via the internet

As previously noted, the concept of disinformation is not a new phenomenon. It is also important to note that "online disinformation specifically and narrowly refers to information that is demonstrably false and deliberately spread on the internet with the intention of shaping public opinion. This separates it from 'misinformation' which is false information, but that may not be deliberately so" (Raderstorf and Camilleri 2019). Previous tactics of dissemination of false information included newspapers, broadcasting, leaflets, etc. Twenty-first century information warfare now includes the internet, in particular social media—cyberspace's premier host for social interaction. With its existence comes a number of distinct characteristics that can be categorized as both benefits and vulnerabilities, depending on which side you are on.

- The **speed**_by which the rate of disinformation delivery has exponentially increased via cyberspace, especially through social media. Algorithms have been designed to increase views and shares, quickly making stories go viral (Nemr and Gangware 2019), and automated bot armies can deliver volume and repetition at high speeds to amplify messages (Adams 2018).

- The **ease of this delivery method** has exponentially increased. One post can reach millions of targets because as an online post is not scalable; it takes the same amount

of effort to reach one person as it does five million (Shallcross 2017). Conversely, the simplicity by which information is shared has led to **increased accessibility** by those on the receiving end.

- **Attribution** in this arena is increasingly difficult. Social personas can create profiles that appear to be legitimate, but in reality are fake. Websites can also be created by unknown sources to relay disinformation. Furthermore, the narratives do not necessarily have to be untrue. For example, they can be attached to already-established movements within a democratic society. The impact of this is twofold: first, it gives artificial credibility and visibility to otherwise illegitimate groups. Second, if the deception is detected, it can have the opposite effect of discrediting legitimate groups by tainting them with foreign interference.

- There is an **ever-growing information environment**. Information overload can lead to mass confusion and the subsequent disengagement of society, making information manipulation by the aggressor easier and more normalized. The "velocity of human interaction and the velocity of information is at an all-time high," leading to somewhat of a truth crisis (Banach 2018). Even if there is an overall awareness of deception by the public and the individuals that comprise it, the limitations of System 2 to handle so much information means that corrections and fact checking almost never fully undo the damage done (Kagan, Bugayova, and Cafarella 2019).

2) Cyber Espionage

While there is no agreed upon definition at the moment, the 2013 Tallinn manual defines cyber espionage as "an act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather (or attempt to gather) information with the intention of communicating it to the opposing party" (Schmitt). These hacking operations are typically carried out by nation states, but are increasingly taken up by non-state actors. Conversely, "hacktivism" blends hacking and activism for a political or social cause, and state and local governments are increasingly finding themselves targets (Bergal 2017). This form of digital disobedience, however altruistic the intent, is highly disruptive and regarded as harassment.

While there are a variety of ways hacked information can be used to influence targets, one tactic is hack and leak operations. This involves two stages: the first "focuses on intrusion (unauthorized access to networks), while the second concentrates on influence (the use of digital technologies to shift public debate) (Shires 2019). The intrusion into specific digital systems and networks constitutes cyber espionage—the theft of information in cyberspace, usually classified as compromising material. On the other hand, the leak of said stolen information into the public arena has intended psychological effects. This is perhaps especially so when the

release of documents is promulgated in a meticulous fashion, to achieve heightened effects and reactions. James Shires (2019) argues that hack and leak operations are *mechanisms of delegitimization*, based on their technical characteristics, social and political context, and target audiences. This conceptualized framework advances our argument for a sixth domain: the effects of a cyber-operation such as cyber espionage can reach far beyond the intrusion itself and into the realm of public consciousness.

3) Technical Disruptions

Technical disruptions typically involve the hindrance and/or suspense of activities in cyberspace in order to degrade operational effectiveness, which inevitably leads to emotional frustration. This activity includes causing glitches in IT to influence emotions, motives, and objective reasoning. Ultimately, the behavior of an operative becomes less efficient and effective in performing their own cyber missions in a manner favorable to their objectives. Much of this effort focuses on "creating an endless series of technology annoyances and time-wasting interruptions that degrade and disrupt the workflow of network operators significantly" (Lin 2020). These methods involve the usage of cyberspace to affect the brain and, by extension, behavior.

4) Precision Target identification through use of data and predictive analytics

This tactic refers to acquiring data that exhibits user habits online to precisely target victims more likely to be impacted by actions to drive and manipulate behavior. It allows for building insight from analysis of data collected through online interactions and engagements to form predictions about future behavior. Artificial intelligence trained with data from users' social media accounts, economic media interactions (Uber, Apple Pay, etc.), and their devices' geolocation can infer predictive knowledge of its targets (Telley 2018). A commercial example to illustrate this technique is the new phenomenon of using consumer data habits to drive real time automated bidding on personalized advertising—otherwise known as "programmatic advertising." It is only a matter of time before nation states begin to weaponize this technique, particularly in elections and civic engagement (Patterson 2019).

Why Recognition of the Psychological Domain Matters

The distinguishing feature of war in the psychological domain is the targeting of human decision-making. Information often empowers people and enriches their lives, and the internet enhances it by providing ever-greater access to new knowledge, business, and services; however, there is a downside to virtual space as well. Many topics in the social sciences are approached with the assumption that people are "rational actors," but our adversaries approach war in the cognitive domain knowing full well that the opposite is often much closer to the truth. People are not simply rational processors of information, and

cyber-enabled psychological warfare takes advantage of the vulnerabilities created by the limitations of the human mind. These same individuals are what constitute the core of democratic societies, making this issue fundamental to the United States. However, defending democracy is not just a job that falls to individuals or to businesses—it is a national security issue that demands the attention and resources of our defense infrastructure.

First, the establishment of the psychological domain will undoubtedly encourage investment in further research, discussion, and resources, including personnel and appropriate infrastructure. In conflict, there is always an advantage to the side that understands and operates within a domain better than the opponent (Allen and Gilbert 2018). Distinguishing effects carried out within domains in the information environment allows for the proper framework to carry out and assess operations, while sharing best practices. Planners and decision-makers can strengthen the effectiveness and efficiency of these operations, using common language, methods, and capabilities. The US government needs to devote substantially more effort to understanding the science and practice of psychological operations, as they are not synonymous with cyber operations. Cyber operations are intended to hack silicon-based processors and technology, while psychological operations are intended to hack carbon-based processors—that is, human brains. If an organization's expertise is primarily with the former, how can it execute operations intended to optimize the outcomes of the latter (Lin 2020)? What is required is expertise on social cognition and behavioral economics—the fundamental psychological science underlying influence campaigns—along with social network analysis, decision analysis, and the human aspects of command and control.

By recognizing the psychological domain, it gives credibility to the idea and will lead to the further development of a body of literature on the subject and, ultimately, a deeper understanding of the problem. This is not just exclusive to the United States, but could be an international effort as well. When the United States recognized cyber as a domain, NATO soon followed suit, and a vast amount of research naturally followed thereafter. This does not necessarily mean there will be an immediate consensus, but in the case of the cyber domain, it created a legitimate space to begin the development of a broader conversation. In many ways, this conversation has already begun; however, as we have argued throughout this paper, the conversation is not being framed effectively. The way that the government frames national security issues often has a substantial impact on how organizations that are trying to offer their support or on how academics trying to add to the literature put forth their own contributions. The fact that the United States, and many other Western states, draw upon the public's knowledge as input to the larger policy discussion is a strength that many of our adversaries do not take advantage of. There is incredible potential in en-

gaging with the broader community to find ways of combating this new and unique threat.

Second, the establishment of the psychological domain is critical because democratic governance relies on reliable and trustworthy information for people to make rational and calculated decisions. Yet, cyber-enabled war in the psychological domain allows for the spread of falsehoods and the sowing of chaos that distorts reality and degrades trust. As it stands, foreign influence and interference pose a significant threat to democracy. Whether it be through pure cyber-attacks on a state's infrastructure or disinformation campaigns, adversaries are seeking to divide our societies and degrade confidence not only in elections, but also in the overall credibility of our institutions. Adversaries will continue to adopt and look for ways to weaken the United States and its allies, strengthening their own strategic position on the world stage. This will be an ongoing intrusion that knows no borders, infringing on the functioning of democracies worldwide.

Third, the establishment of the psychological domain will send a signal to our adversaries, initiating digital deterrence. As we argued in our previous article, the weaponization of information changes the application of deterrence, both within the cyber domain and the psychological domain (Ajir and Vailliant 2018). Elements of deterrence will be applied to each domain differently, hence changing its applicability. In an era of great power competition, US strategic deterrence will need to evolve to encompass warfare in all domains, including the psychological domain. However, we must take a few steps back and understand that we cannot meaningfully deter our adversaries unless they are aware of our capabilities; these capabilities will not be fully developed unless the sixth domain is established.

Conclusion

In her 1979 book *The Printing Press as an Agent of Change,* Elizabeth Eisenstein acknowledges the profit motive that drove many early printers and the fact that disinformation and propaganda was still rife. However, she argues that despite the downsides, such as heightened ethnic tensions, the spread of medical disinformation, and about a century's worth of European religious wars, the long game was more important. In other words, "even when early printing technology ought to be described as a weapon, Eisenstein treats it more like a light bulb" (Marantz 2019). But what happens when modern technology completely changes information dissemination? Will the light bulb continue to illuminate, or will it be dropped and burn everything to the ground? Or perhaps, if not guided, it will shine a glaring light on the ugliness beneath the social cohesion of contemporary society. This is why establishing a sixth domain is necessary—it will lead to a more comprehensive understanding of the effects of cyber-enabled psychological attacks on the human psyche, subsequently leading to policies in de-

fense of our nation. It means taking the downside risks of the light bulb more seriously, and with a bit more caution, as the long game is more important.

It may seem paradoxical, as some may argue that acting in this sixth domain will make us no better than Russia or China—two anti-democratic regimes, competing to be great powers. We counter that the United States exemplifies the democratization of information—upholding liberal values of democracy including free speech and the free flow of information, something Russia and China and many other authoritarian regimes do not allow. Both states use information operations domestically to suppress dissent and control what people think, whether through manipulation or censorship, all while exporting a particular model of digital authoritarianism globally. Russia and China illustrate the unintended consequences of the digital information age—the new paradigm scholars once thought would give more power to the people is instead being used to silence and control them. Our adversaries have weaponized information to control behavior both at home and abroad, as a method of normal politics, while Western democracies tend to limit it to wartime activity.

As we move forward with the new realities of a digital world, information will not only be critical to, but also the key to, success in all domains. Furthermore, the exponential growth of technology and its widespread use has ensured that those who take part in information war are individuals, and not just armed forces. Advanced technology such as deep fakes, artificial intelligence, and 5G network speed will further refine cyber-enabled psychological operations, having profound effects on information warfare in particular and allowing us to recognize its new role in offensive and defensive operations. Yet the speed by which we act is not yet sufficient, and is instead reactive and inductive. Certainly, this is not to downplay the complexity of dealing with new types of warfare. In the real world, resources are often stretched and responses to adversarial behavior will probably always err on the side of being reactive rather than proactive. What matters most is that when we see these developments unfolding, we create the proper frameworks for addressing each individual problem area. Doing so will ensure the continuation of proper attention and resources being dedicated to combating new threats as they arise.

Disclaimer

The views presented in this article are those of the authors and do not necessarily represent the views of USSTRATCOM, the US Air Force, the DoD, or the US Government.

Acknowledgements

Thanks to Brian Burke and Tommy Nimrod, for their thoughtful expertise in regards to the information environment and psychology, respectively, in guiding this research.

Bethany Vailliant is an Analyst at the United States Department of Defense. She is also an Adjunct Professor teaching International Relations at the University of Nebraska at Omaha, where she earned her M.S. in Political Science with a certification in Intelligence and National Security.

bethanyrvailliant@gmail.com

Media Ajir is an Analyst at the United States Department of Defense. She is also an Adjunct Professor at the University of Nebraska at Omaha and Bellevue University, where she teaches International Relations and Political Science. She holds an M.S. in Political Science with a certificate in Intelligence and National Security.

majir@unomaha.edu

References

Adams, Tim. 2018. "The Charge of the Chadbots: How Do You Tell Who' Human Online?" *The Guardian,* November 18, 2018.

Ajir, Media and Bethany Vailliant. 2018. "Russian Information Warfare: Implications for Deterrence Theory." *Strategic Studies Quarterly* 12 (3): 70–89.

Allen, Patrick and Dennis Gilbert. 2018. "The Information Sphere Domain Increasing Understanding and Cooperation." NATO CCDCOE.

Banach, Stephan J. 2018. "Virtual War – A revolution in Human Affairs." *Small Wars Journal*

Bergal, Jenni. 2017. "Hacktivists Launch more Cyberattacks against Local, State Governments." *PBS.*

Brazzoli, M.S. 2007. "Future Prospects of Information Warfare and Particularly Psychological Operation: South African Army Vision 2020." *Institute for Security Studies, Pretoria*, 217–32.

Greenberg, Andy. 2019. "The WIRED Guide to Cyberwar." WIRED. August 23, 2019.

Heftye, Erik. 2017. "Multi-Domain Confusion: All Domains Are Not Created Equal." The Strategy Bridge. May 26, 2017.

Horning, Donna. 2011. "Cyberwar: The Fifth Domain of Warfare." The Politic. December 19, 2011.

Hwang, Tim, and Lea Rosen. 2017. "Harder, Better, Faster, Stronger: International Law and the Future of Online PsyOps."

Joint Chiefs of Staff. 2014. "Joint Publication 3-13. Information Operations."

Joint Chiefs of Staff. 2019. "Joint Publication 6-0: Joint Communications System."

Kagan, Frederick, Nataliya Bugayova, and Jennifer Cafarella. 2019. "Confronting the Russian Challenge: A New Approach for the U.S." Institute for the Study of War.

Kahneman, Daniel. 2011. *Thinking, Fast and Slow*. Farrar, Straus and Giroux.

Kovacich, Gerald, and Andy Jones. 2006. "High-Technology Crime Miscreants: Profiles, Motives, and Philosophies." In *High-Technology Crime Investigator's Handbook: Establishing and Managing a High-Technology Crime Prevention Program*, 2nd ed., 23–48. Elsevier.

Lin, Herb. 2020. "On the Integration of Psychological Operations with Cyber Operations." *Lawfare*. January 9, 2020.

Lin, Herbert. 2019. "The Existential Threat from Cyber-Enabled Information Warfare." *Bulletin of the Atomic Scientists* 75 (4): 187–96.

Marantz, Andrew. 2019. "The Dark Side of Techno-Utopianism." *The New Yorker*, September 23, 2019.

Patterson, Dan. 2018. "How Campaigns Use Big Data Tools to Micro-Target Voters." *CBS News,* November 6, 2018.

Raderstorf, Ben and Michael Camilleri. 2019. "Online Disinformation in the United States: Implications for Latin America." *The Dialogue.*

RAND. n.d. "Cyber Warfare." https://www.rand.org/topics/cyber-warfare.html.

Schmitt, Michael N., ed..2009. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence.* Tallinn, Estonia: International Group of Experts.

Schreier, Fred. 2015. "On Cyber Warfare." Geneva Centre for Security Sector Governance.

Shallcross, N.J. 2017. "Social Media and Information Operations in the 21st Century." *Journal of Information Warfare* 16 (1): 1–10.

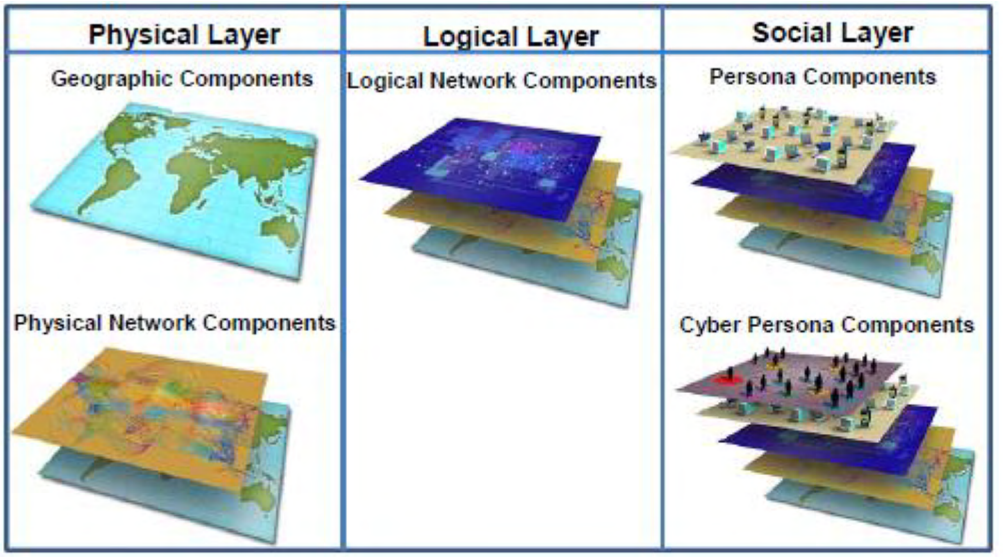
Shires, James. 2018. "Hack-and-Leak Operations: Intrusion and Influence in the Gulf." *Journal of Cyber Policy* 4 (2): 235–56.

Telley, Chris. 2018. "Influence at Machine Speed: The Coming of AI-Powered Propaganda." *Mad Scientist Laboratory*, May 24, 2018.

US Army. 2010. "Cyberspace Operations Concept Capability Plan 2016-2028." *The US Training and Doctrine Command, Fort Eustis*.

Wilmer, H.H., L.E. Sherman, and J.M. Chein. 2017. "Smartphones and Cognition: A Review of Research Exploring the Links Between Mobile Technology Habits and Cognitive Functioning." *Frontiers in Psychology* 8: 605.

Appendix 1



US Army, Cyberspace Operations Concept Capability Plan 2016-2028.