# Neurocognitive hacking
## A new capability in cyber conflict?

**John J. Heslen**, *Augusta University*

Abstract. **This article presents a discussion of neurocognitive hacking and its potential for use at the strategic, operational, and tactical levels of cyber conflict. Neurocognitive hacking refers to the ability to activate specific neural areas of the brain, via subliminal or supraliminal stimuli, to shape the behavioral outcomes of an adversary. Research suggests that awareness of mortality-related stimuli has neural correlates in the right amygdala and left anterior cingulate cortex and mediates negative behavior toward out-group members, including unconscious discriminatory behavior. Given its in-group/out-group dynamic, the phenomenon could be exploited for use in information operations toward target populations, specifically ones that are multiethnic, multicultural, or multireligious. Although development of the theoretical framework behind neurocognitive hacking is ongoing, mortality-related stimuli are proposed to activate one's unconscious vigilance system to further evaluate the locus and viability of the suspect stimuli. Research suggests that the subsequent discriminatory affective reactions directed toward out-group members are representative of automatic heuristics evolved to protect the organism in the event a stimulus represents a more serious threat to survival. Therefore, presenting mortality-related stimuli over computer networks to targeted audiences may facilitate the ingestion of tailored propaganda or shaping of specific behavioral outcomes within a population, including sowing division in a target community or weakening support for a specific political regime.**

Key words: Subliminal stimuli, terror management theory, psychological operations, information operations, persuasion, cyberwar, propaganda, mortality bias

The use of propaganda in war likely dates to the dawn of civilization. Its methods are constantly being updated and improved to match current advancements in communications technology. As propaganda (considered a type of information operation) has been inextricably linked with war, employment of these capabilities by major world powers will likely increase in what are referred to as "gray zones" as the dawning of the nuclear age has made kinetic warfare between them far too risky. Philip M. Taylor, in his important work *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day* (2003), noted that with the advent of nuclear weapons, war between nuclear-armed adversaries increasingly is prosecuted within the information space. The use of propaganda in information wars between great powers has now become "part of the struggle for perceptions in which words attempt to speak as loud as actions, and sometimes even replace the need for action" (Taylor, 2003, p. 8). In fact, one has to look no further than the 2016 U.S. presidential election to get a glimpse of the new world of great-power information conflict. For example, the U.S. Intelligence Community report assessing Russian hacking activities during the presidential election noted that one of Russia's primary goals was to "undermine the US-led liberal democratic order" (Office of the Director of National Intelligence, 2017, p. ii).

More recently, a European Commission report outlined the "sustained" disinformation campaign by the Russian government to depress voter turnout and influence voter preferences during the 2019 European parliamentary elections (European Commission, 2019). As a result, many in the West are now well acquainted with the dangers of propaganda, sometimes colloquially referred to as "fake news." And there is worry among cyberwarfare analysts that in the future, political conflict utilizing information operations may become ubiquitous

**doi:** 10.1017/pls.2020.3
Correspondence: John J. Heslen, Augusta, Department of Social Sciences, Political Science, 1120 15th Street, Augusta, Georgia, 30904-4562. Email: *jheslen@augusta.edu*

as it offers nation-states the ability to act covertly while cyber deterrence measures remain dangerously underdeveloped (Valeriano & Jensen, 2019). In fact, many nation-state militaries increasingly are developing and utilizing a suite of cognitive tools to influence and persuade target populations referred to as CAMO, or "cognitive aspects of military operations" (Astorino-Courtois, 2017).

## Definitions and conceptual issues

The *Oxford English Dictionary* defines propaganda as "the systematic dissemination of information, especially in a biased or misleading way in order to promote a political cause or point of view." However, because the concept was not sufficiently comprehensive to describe the full range of influences involved in persuasive activities (in addition to the negative connotations the word acquired from its use by the Nazi and Soviet regimes), it fell out of favor in much of the West in favor of "persuasion," considered a more comprehensive and less polarizing term (Markova, 2008). Still, the two words have a tendency to be used interchangeably, but scholars have proposed an interesting dichotomy to differentiate between them. Propaganda is conceptualized as a one-way "monologic" communication from a "source" to a "receiver," with the goal of "transform[ing] the heterogeneous thought of individuals into those of a homogenous 'collective mind' of masses, and to lead those masses to a specific action" (Markova, 2008, p. 41). In other words, propaganda can be thought of as a unidirectional communication in which the source of the message holds the predominance of power with regard to the ability to create, change, or normalize the social reality of the receiver (Markova, 2008).

In contrast, persuasion is conceptualized as a two-way "dialogic" communication in which the power between the source of the message and the receiver is more broadly shared, but it is also conceptualized to include one's internal dialogue and unconscious aspects of thought. However, unlike propaganda, in which the more powerful source seeks to "fuse" its reality with that of the receiver, in persuasion, the source's aim is to "convince the other party of one's own case and of the superiority of one's own idea or belief over that of the [receiver]" (Markova, 2008, p. 45). With this in mind, neurocognitive hacking is proposed to support the role of propaganda by making its ingestion more likely and facilitating persuasion by cultivating a neural environment in the receiver more accommodating to the source's narrative, especially when it involves in-group/out-group dynamics.

For the same reasons discussed earlier, "psychological operations" and "information operations" are terms requiring clear distinctions. Both words are typically used in relation to nation-state-sponsored military or civilian intelligence operations, but they have different operational scopes. The U.S. Department of Defense defines psychological operations (PSYOPs) as "planned operations that convey selected information and indicators to foreign target audiences to influence their emotions, motives, objective reasoning, and ultimately, the behavior of foreign governments, groups and individuals" (U.S. Department of the Army, 2003, p. GL-8).

In modern military operations, propaganda is conceptualized as a tool of PSYOPs. However, because of innovations and advancements in technologies complementary to PSYOPs, along with the efficiencies gained by employing them in concert with other supporting capabilities, Western militaries increasingly refer to information operations as

> the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities to influence, disrupt, corrupt or usurp human and automated decision making while protecting our own.
>
> *(Larson et al., 2009, p. xiii).*

Additionally, although brain science is considered by many to be in its infancy, thanks to recent developments in brain imaging technology, the field is advancing rapidly and gaining insights into once-invisible processes (Jorgenson et al., 2015). As artificial intelligence tools are incorporated into these research efforts, the rate of discovery will likely only increase; however, there are many ongoing foundational debates regarding brain function that have yet to be resolved, such as the relationship between one's evaluation (i.e., attitude) of an object or concept and subsequent behavior toward it (Ajzen & Cote, 2008). As neurocognitive hacking proposes the ability to utilize specific stimuli to activate neural structures (e.g., amygdala and anterior cingulate correlate) for the purposes of exploiting affective reactions and shaping targeted *behavioral* outcomes, a quick treatment of the mood/attitude–behavior linkage is offered.

Conceptually, regarding the reactions to mortality-related stimuli, the author agrees with the logic of Tritt

and colleagues (2012) and their use of the term "affect" versus "moods" or "emotions," as it avoids unnecessary theoretical and sematic "baggage." For example, there are ongoing debates regarding the extent to which (conscious) cognitive processes are involved in emotion (Winkielman & Berridge, 2004) and attitude formation (Devos, 2008). However, by using the construct of "affect" to describe moods or emotions that are inclusive of behavioral phenomenon occurring below conscious awareness (e.g., mortality-related stimuli) and thus opaque to self-reported measures, these controversies are largely avoided.

In fact, research by Winkielman and colleagues (2004) suggests that affective responses intense enough to influence one's behavior can remain below awareness. Therefore, reactions to mortality-related stimuli (M-rS) will not be conceptualized in terms of an attitude-mediated behavioral construct (e.g., MODE model, theory of planned behavior) but as a biologically construed "mortality bias" composed of unconscious affective reactions (Winkielman et al., 2005), activated by an energized threat detection system (Tritt et al., 2012) for the purposes of reducing false negative (Type II) errors (Haselton & Buss, 2000) and "psychological uncertainty" (Tritt et al., 2012). A more in-depth discussion of this topic will be presented later in the article.

## Psychological operations in conflict

Taylor (2003) highlights many fascinating uses of propaganda throughout history, covering operations from ancient Greece to the post–Cold War era. His well-regarded book highlights the evolution of propaganda and explicates how its methods generally mirror the overall advancement of technology in a society. In ancient Greece, for example, architectural marvels like the Acropolis were used to persuade citizens and noncitizens alike of the superiority of Greek culture. More than two millennia later during the Cold War, Americans utilized radio (e.g., Voice of America) in their propaganda efforts against the Soviet bloc. As communications technology in the information age continues to advance, its technologies will provide increasingly rich support for disseminating propaganda in new digital formats to match the current crop of polarizing memes, "fake news" on social media, and "deepfake" manipulations of video clips.

Regardless of the polarizing nature of the concept, Taylor suggests that readers approach propaganda as a morally neutral concept best looked upon as a "process for the sowing, germination, and cultivation of ideas" (2003, p. 2). He notes that the Vatican operationalized this process during the Protestant Revolution in Europe to defend itself against heretics with such success that even today, Catholics and Protestants can still be distrustful of one another. This example alone could attest to the incredible power of propaganda; however, Taylor is quick to note that it alone is not enough to win conflicts but is most effective when integrated with other levers of power, such as diplomatic, military, or economic.

Contemporary history is replete with examples of political and military leaders using propaganda and other broader forms of PSYOPs to their benefit—or their peril, if they failed to incorporate it into their repertoire of operational capabilities. For example, John Nagl's *Learning to Eat Soup with a Knife* (2002) highlights the positive role PSYOPs played during the 1940s–1950s British fight against the communist insurgency in Malaysia. Nagl points out the British Army after World War II was more of a "learning organization" compared with their American counterparts and more willing to experiment with unconventional tactics, including the use of PSYOPs to win "hearts and minds." To a large extent, this resulted from the British Army's experience fighting many "small wars" in remote locations over the previous two centuries and being forced to adapt to myriad enemies and operating environments. However, because the British did not have inexhaustible resources to bring to bear on these limited wars, they focused heavily on understanding (and exploiting) the motivations of their enemies, an effort often made easier by partnering with indigenous civil authorities.

This approach prompted experimentation with various tools of persuasion and influence to help the British exploit and ultimately break the will of their enemies. In Malaysia, for example, British field commanders were given flexibility to employ various PSYOP tactics (including blasting propaganda from loudspeakers mounted on airplanes, placing bounties on the heads of insurgent leaders, and dropping leaflets over enemy territory), an effort that by 1960 largely proved successful (Nagl, 2002).

Nagl highlights how the U.S. Army, in contrast with the British, was less apt to incorporate PSYOPs into military operations as the Americans relied on (and could afford to use) a policy of fielding much larger units, intent on using overwhelming force to exact total destruction on the enemy. He notes that when General William Westmoreland took command in Vietnam, his army

was sorely lacking in its understanding of PSYOPs and thus its preparation was "inappropriate to the demands of counterinsurgency warfare in South Vietnam" (Nagl, 2002, p. 174). American deficiencies were compounded by the strength of PSYOPs conducted by their National Liberation Front foes, who, as the scholar Francis Fitzgerald pointed out, were geared toward inculcating the "systematic encouragement of hatred" of the United States. Similarly, having recognized the motivational benefit of generating hatred within the Vietnamese people toward their French occupiers a generation prior, Ho Chi Minh purportedly said, "I have no army, I have no finances, I have no education system, I only have my hatred" (Fitzgerald, 1972, p. 169). Hate is a powerful motivator and the rise of the internet, in combination with other information communication technologies and platforms, has made it easier for both separatists and terrorist groups to generate and exploit it for specific purposes.

One of the more recent and concerning innovations of terrorist organizations is their ability to utilize social media for radicalization and recruitment. Communications scholar Gabriel Weimann (2015) notes that social media has given terrorists groups an enormous advantage because of the "effectively limitless" audience it creates for recruitment and the ease with which propaganda videos can be uploaded in response to dynamic operating environments. Two cases from nearly a decade ago highlight the speed and effectiveness with which PSYOPs can be used in the cyber domain to support the terrorist radicalization process.

In 2011, Arid Uka, an Albanian Muslim immigrant to Germany, admitted to becoming self-radicalized as a result of consuming online jihadist propaganda. In roughly six months, after watching numerous propaganda videos, including one doctored by the Islamic Movement of Uzbekistan falsely depicting U.S. soldiers sexually assaulting Iraqi and Afghan women, Uka drove to nearby Frankfurt Airport and shot and killed two U.S. military personnel transiting from a base in the United Kingdom (Bohleber & Bohleber, 2012).

Similarly, the case of British citizen Roshonara Choudhry (Pearson, 2015) highlights a rare instance of a female terrorist attacker being radicalized to action online. In early 2010, Choudhry, a fairly typical university student working toward completing her degree at King's College, London, admitted to becoming radicalized as a result of spending several months viewing hours of propaganda videos. Many of these videos featured the well-known jihadist Sheikh Abdullah Azzam and the American radical propagandist Anwar al-Awlaki. By the end of the academic year, Choudhry had dropped out of university, become estranged from most of her friends and family, and attempted to stab to death a British member of Parliament. Her case was highly unusual in that most jihadist attacks are committed by men, with the vast majority of Islamic propagandist urging women to participate in support actions only. However, during questioning after her arrest, she noted that she overcame these gender and ideological barriers to action after viewing videos of Sheikh Abdullah Azzam, who decreed "even women" had a duty to engage in jihadist attacks (Windsor, 2018).

## Information operations in the digital era

Although the capabilities of terrorist groups to conduct PSYOPs for purposes of recruitment and radicalization present a formidable challenge to global security, they generally lack the resources needed to conduct full-spectrum information operations. The science of information operations in the digital era is advancing rapidly, and it is increasingly characterized by 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 [one's] own" (U.S. Department of Defense, 2014, p. ix). Modern information operations apply theories developed from the study of persuasion and motivation, and the capability is becoming increasingly sophisticated as it parallels advances in those fields (Jowett & O'Donnell, 1986). These advances are supported by new imaging tools such as functional magnetic resonance imaging (fMRI) and co-registration techniques that combine old and new technologies to produce more comprehensive scans. These new imaging tools have illuminated previously unknown neural processes in the brain responsible for interpreting the social world, including highlighting the importance of neural structures such as the amygdala in evaluating stimuli with emotional value. As many of these processes are known to occur below the level of consciousness (Adolphs et al., 1995) they underscore the susceptibility of neural components like the amygdala to manipulation as their activation may be exploited to shape targeted behavioral outcomes.

In fact, research suggests that *subliminal* mortality-related stimuli (e.g., an image of a dead body) can

activate the amygdala and other neural components associated with the processing of threat stimuli (Quirin et al., 2011). Therefore, exploiting these unconscious processes, combined with the ability to commandeer communication networks supporting smartphones and other electronic media devices, is proposed to offer a powerful tool for increasing the ingestion of propaganda and subsequent shaping of perception and behavior of adversaries. It should be noted that although the effects on behavior from neurocognitive hacking are conceptualized to be small, the ability to "nudge" a small group of people in one direction can have enormous strategic consequences, as highlighted by the fact that the 2016 U.S. presidential election was determined by fewer than 80,000 votes in three states (Bump, 2016).

To highlight the growing strategic relevance of information operations in interstate conflict, consider the indictments by the U.S. Office of Special Counsel. It charged Russian agents with interfering in the 2016 presidential election by seeking to "sow discord" within the U.S. political system (U.S. Department of Justice, 2018). As part of their efforts, Russian operatives were accused of creating numerous social media handles geared toward increasing public polarization over several highly contested social issues. According to the indictment, these social media accounts sought to inflame attitudes over issues such as African American and Muslim civil rights, using provocative names, including "Woke Blacks" and "United Muslims of America." Although it is difficult to calculate the extent to which this propaganda influenced the public, consider if the targeted audiences had first been primed with mortality-related stimuli that prompted the activation of neural correlates related to threat perception and response. It is proposed that such a targeted neurological attack on these neural structures would have increased the rate of propaganda ingestion by the targeted audience and subsequent level of societal discord within the United States. The ability to influence or "hack" the perception of adversaries to shape behavioral outcomes is of increasing interest to national security stakeholders in the United States, many of whom assess the United States' current capability in this area to be critically underdeveloped (Astorino-Courtois, 2017).

## Why mortality-related stimuli?

Research utilizing priming stimuli is controversial; however, a meta-analysis by Weingarten et al. (2016) and research by Winkielman et al. (2005) suggest they can have a significant effect on behavior. These effects appear even greater when primes incorporate the use of words with negative valence (Nasrallah et al., 2009). In fact, robust research exists suggesting that priming with mortality-related stimuli mediates prejudicial behavior toward out-groups and their respective cultural symbols (Greenberg et al., 1990). After perceiving mortality-related stimuli, individuals have been shown to unconsciously exhibit negative biases toward out-groups, including increased hostility and willingness to engage in avoidance behavior, as well as a greater willingness to actively denigrate out-group cultures (Burke et al., 2010; Greenberg et al., 1990). The preponderance of research utilizing mortality-related primes has traditionally been subsumed under a theoretical construct referred to as terror management theory (TMT).

Motivated by the writings of Ernst Becker, TMT's theoretical framework is controversial, as it asserts that during the course of evolution, humans reached a level of cognitive sophistication enabling an awareness of the inevitability of death (Greenberg et al., 1986). According to TMT, the inexorable nature of death created such maladaptive terror in humans that it prompted the species to generate a suite of psychological coping mechanisms referred to as "cultural anxiety buffers" (Rosenblatt et al., 1989). When mortality-related stimuli are salient in the environment, the buffers are theorized to work by managing the paralyzing effects of death awareness. Therefore, they are purported to facilitate a deeper fusion with one's cultural worldview to give symbolic immortality and mitigate the finality of biological death (Solomon et al., 2004). To test these assertions, TMT researchers utilize a priming manipulation referred to as "mortality salience."

The effects of mortality salience (i.e., awareness of mortality-related stimuli) are explored in research settings by asking subjects to consider the ramifications of their physical death and examining their subsequent behaviors. In general, TMT researchers have found that priming with mortality-related themes tends to facilitate "worldview defense" (a worldview comprising the foundational beliefs one holds to help understand and interpret the world). A worldview defense, therefore, is roughly defined as actions involving the defense of one's culturally based belief system. Examples include exhibiting negative discriminatory behavior toward out-groups (i.e., those holding different worldviews) or positive discrimination toward one's in-groups (Greenberg et al., 1990).

Although experiments using mortality salience manipulations to induce prejudiced reactions are numerous (Greenberg et al., 1990; Rosenblatt et al., 1989), the framework suggested by TMT has been criticized on several theoretical grounds (Fessler & Navarrete, 2005; Holbrook et al., 2011; Kirkpatrick & Navarrete, 2006). For instance, researchers in the field of coalitional psychology assert that reactions to mortality salience (i.e., mortality-related stimuli) result from a series of prosocial behaviors that evolved in humans to better coordinate social interactions within in-groups, especially behaviors that would be adaptive when reacting to crises or threatening situations (Kirkpatrick & Navarrete, 2006). Coalitional psychology offers a cogent explanation for why mortality-related stimuli affect social relations, and it, along with other complimentary theories (Haselton and Buss, 2000; Tritt et al., 2012), provides a well-grounded explanation for the biological foundations of the phenomenon.

Error management theory, an evolutionary perspective on the development of cognitive biases, proposes that under conditions of uncertainly, reactions to adaptively relevant stimuli (e.g., dead animals, potential threats from out-groups, or sexual opportunities) are biased toward false positive (Type I) errors. For example, men have been shown to overestimate the extent to which women have sexual interest in them, as this bias would likely facilitate greater reproductive success over the long term. Similarly, when primed with fear, individuals presented with neutral faces have been shown to attribute more anger to them (Haselton et al., 2009), a bias that is likely to have proved protective during the environment of evolutionary adaptiveness. Given that mortality-related stimuli could resolve into actual existential threats (e.g., finding a dead body in one's immediate environment could represent the presence of a lethal attacker or a lethal disease), response heuristics encoded to avoid making false negative (Type II) errors would likely have been adaptive.

Regarding the biological mechanics of reactions to mortality-related stimuli, Tritt et al. (2012) propose the existence of a "biological anxiety system" activated by states of "psychological uncertainty." When psychological uncertainty results from a "mismatch" between one's actual and expected reality, a component of this biological anxiety system, referred to as the behavioral inhibition system (BIS), is triggered. As Tritt and colleagues (2012) note, the BIS is thought to be integral to both the function of anxiety and approach-avoidance dynamics, as it activates inhibitory neural components located in the right hemisphere of the brain. This explanation comports with findings by Quirin et al. (2011) showing activation of the right amygdala and left anterior cingulate cortex (ACC) subsequent to priming with mortality-related stimuli.

Research suggests that subliminal stimuli can trigger affective reactions without conscious awareness (Winkielman & Berridge, 2004); however, there is controversy over this issue. Addressing this, Custers (2009) notes that most models of human goal pursuit conceptualize a *conscious* mechanism for determining whether a goal will be pursued based on the "expected value" of the goal. However, because reactions to subliminal goal primes can occur outside of conscious awareness, Custers asserts that the most logical mechanism for determining the expected value of a goal outside of conscious awareness "would be one that relies on affective [not conscious] processes" (2009, p. 179). Additionally, based on research suggesting that there are differentials in the amplitude of affective reactions to valenced stimuli (Holbrook et al., 2011), there are likely only a few affective reactions that are as impactful on behavior as those induced by mortality-relevant stimuli.

With the foregoing theoretical framework in mind, the author proposes the term "mortality bias" (Heslen, 2016) to capture the suite of automatic processes related to reactions to mortality-related stimuli.

## Role of the amygdala in shaping perception and behavior

Although several neural structures are thought to influence social cognition and human decision-making in concert with the amygdala (Adolphs, 2003, 2009), the structure is of particular interest to the conceptualization of neurocognitive hacking given growing evidence of its involvement in the processing and encoding of emotion, fear, and ambiguity within social contexts (Whalen, 1998).

The amygdala is an almond-shaped structure located deep within the temporal lobes of the brain. Traditionally, it was thought to function solely for evaluating threat-related information; however, it is now assessed to be part of an early vigilance system that works with other neural structures to process the emotional value of stimuli. As such, researchers have surmised that the amygdala may act as a complex area for processing the "social, homeostatic, and survival-related meaning of a class of complex stimuli, such as facial expressions of some emotions" (Adolphs et al., 1995, p. 5889). This view of the

amygdala's role in facilitating emotional evaluations is supported by other research suggesting that it is more sensitive to negative *animate* versus negative *inanimate* stimuli in human social contexts. For example, subjects presented with subliminal images of both threatening animals and threatening inanimate objects, such as pointed guns, experience greater amygdala activation in response to the threatening animals (Fang et al., 2016). Again, this finding suggests that the amygdala plays an important role with other neural components in linking emotional valence to specific objects.

Combining evidence suggesting that unconscious perception of mortality-related stimuli activates the right amygdala and the left rostral ACC with findings suggesting that an activated amygdala is correlated with the propagation of unconscious racial stereotypes (Phelps et al., 2000), a logical leap has been made suggesting that the discriminatory behaviors induced by mortality-related stimuli are mediated by the activation of these neural structures. Therefore, by integrating research suggesting that individuals continuously (and automatically) update their social evaluations of others (Wheeler & Fiske, 2005) with evidence suggesting that the amygdala plays a significant role in facilitating these automatic evaluations (Adolphs et al., 1995), neurocognitive hacking proposes the ability to exploit this interplay to shape perceptual and behavioral outcomes of targeted audiences.

Additionally, scholarship suggests that subliminal exposure to mortality-related stimuli mediates behavior in a similar manner as conscious (supraliminal) exposures. For example, in one experiment, American participants subliminally primed with the word "death" were more critical of anti-American essays than participants who were subliminally primed with the word "field." Interestingly, terror management theory researchers have found that reactions (e.g., discrimination toward out-groups) occurring subsequent to *conscious* mortality primes do not manifest until after a short distraction exercise is given. This is not the case with subliminal mortality-related primes, the effects of which can be immediately observed without a distraction (Arndt et al., 1997).

The need for a distraction exercise has been proposed by Heslen (2016) to involve the "System 1" and "System 2" dual-processing cognitive construct suggested by Stanovich and West (2000) and popularized by Daniel Kahneman in his book *Thinking, Fast and Slow* (2011). In general, while both systems are believed to work in a complimentary fashion, System 1 is thought to comprise the suite of automatic mechanisms that constantly evaluate and respond to environmental stimuli, whereas System 2 facilitates more conscious, deliberative functions. As such, the distraction exercise following conscious awareness of mortality-related stimuli likely interrupts the conscious appraisals of System 2, thus giving primacy to System 1 dynamics, where automatic behavioral heuristics are generated.

## Cognitive aspects of military operations (CAMO)

Several of the United States' strategic adversaries, including Russia, have been involved in researching the cognitive and psychological aspects of information warfare for decades (Thomas, 2004). However, within the U.S. defense establishment, there is growing recognition that the armed forces are behind in this area of research and lack the ability to incorporate knowledge of the "human/cognitive domain" into military operational planning. As opposed to the physical/kinetic domain (e.g., weapons systems and personnel training), where the United States is considered dominant, its utilization of the human-cognitive domain (i.e., the ability to influence "attitudes and behaviors of populations or opponent forces by manipulating information and otherwise preying on human perceptual vulnerabilities"; Astorino-Courtois, 2017, p. 6) is proposed to be lacking. It is a space, however, in which United States' major adversaries are assessed to have invested heavily. Increasingly, this suite of cognitive tools is conceptualized as the cognitive aspects of military operations (CAMO) and incorporates techniques to exploit three key psychological functions: cognition, affect, and conation (Astorino-Courtois, 2017).

In 2016, the Strategic Multilayer Assessment Office of the U.S. Department of Defense published a white paper titled "A Cognitive Capabilities Agenda: A Multi-Step Approach for Closing DoD's Cognitive Capability Gap" (Astorino-Courtois, 2017). The paper made several recommendations for how the United States could close the cognitive capabilities gap proposed to exist with its strategic adversaries, including Russia, China, Iran, and North Korea. In addition to recommending updates to doctrine, it called for the Defense Department to increase funding for "actionable cognitive research" and the development of "analytic tools" to integrate cognitive capabilities with the physical/kinetic aspects of warfighting (Astorino-Courtois, 2017). The ability to operationalize these cognitive capabilities in "gray zones" (characterized as intense areas of military competition that fall short of conventional war; see Votel et al., 2016)

is an area in which Western allies, given adequate investment, can significantly increase their effectiveness, in light of recent scientific advancements.

Among the West's strategic competitors, Russia is assessed to be the most advanced with regard to their research efforts and ability to execute cognitive operations. In fact, during the 1960s and 1970s, Russia developed a theory of information warfare referred to as "reflexive control" to maximize advantages in both cognitive and computer-based decision-making processes. Reflexive control has been defined as a method of deception to relay "specially prepared information to incline [adversaries] to voluntarily make [a] predetermined decision desired by the initiator of the action" (Thomas, 2004, p. 237). Russian military theorists assert that during a conflict, the combatant with the greatest understanding of enemies' moral, cognitive, and psychological underpinnings, including those of senior decision makers, tend to be most successful because they are better prepared to induce the enemy into making adverse decisions (Thomas, 2004).

The need to increase understanding of the cognitive tools used to manipulate perception was well illustrated by the 2016 U.S. Intelligence Community report on Russian hacking and the subsequent indictment filed by the U.S. Office of Special Counsel in February 2018. The 2016 report, "Background to 'Assessing Russian Activities and Intentions in Recent U.S. Elections'" claimed that Russia tried to influence the 2016 election to "undermine the U.S.-led liberal democratic order" and "public faith in the U.S. democratic process" (Office of the Director of National Intelligence, 2017, p. ii). The later indictment filed by the Office of Special Counsel highlighted both the organizations involved and the tactics used by Russian operatives to accomplish these goals. For instance, the special counsel charged the Russian Internet Research Agency with election interference in part for its role in creating highly polarized fake social media accounts.

These accounts were geared toward spreading inflammatory and derogatory information for the purposes of creating strife in the U.S. political system. Fake social media profiles such as "Woke Blacks," "Blacktivist," and "United Muslims of America" were established in an attempt to suppress the minority vote during the election. Examples of messages on these sites included memes such as, "Hillary Clinton Doesn't Deserve the Black Vote," "Hillary is a Satan…," and "Donald wants to defeat terrorism…Hillary wants to sponsor it" (U.S. Department of Justice, 2018). Given the strong reinforcing dynamics that group membership can exact on individual behavior (Glassner, 1985; Jost et al., 2016), the efficacy of these messages, when engineered to exploit central characteristics of group identity, should not be underestimated (Hogg et al., 1995).

To understand how a constant stream of socially engineered messages can influence one's emotional state, consider a study conducted by Facebook several years ago. In early 2012, the social media giant initiated an extraordinary experiment aimed at manipulating the emotional states of 700,000 of its newest members. For one week, the site changed these users' newsfeeds to display a preponderance of either happy/positive or sad/negative news stories for the purposes of assessing any effects on their emotional states. At the end of the week, depending on their respective treatment, users did show a propensity to post either positive or negative words, providing evidence of an "emotional contagion" effect (Meyer, 2014).

Consistent with this research, in 2016, the chief executive officer of Cambridge Analytica—the data analytics firm that assisted multiple African elections as well as, later, the Trump presidential campaign—stated, "If you know the personality of the people you're targeting, you can nuance your messaging to resonate more effectively with those key audience groups" (Nyabola, 2019, p. 1). A former employee of Cambridge Analytica turned whistle-blower offered a more succinct and colloquial analysis of his company's mission, noting that the company had succeeded in developing a "psychological warfare mind-fuck tool" (Halpern, 2018).

In fact, during testimony to the U.K. Parliament, the employee accused Cambridge Analytica of specifically developing software tools, known as psychometrics, to target voters in the 2016 U.S. presidential campaign (National Public Radio, 2018). The use of these psychometrics to identify individuals or populations susceptible to socially engineered propaganda, in concert with the ability to manipulate neural areas of the brain to unconsciously shape behavior and disrupt decision-making abilities (i.e., neurocognitive hacking), foreshadows the sophisticated and potentially dangerous future of information operations in cyber conflict.

## Neurocognitive hacking

The potential to secretly exploit adversary computer networks to prompt users with stimuli for the express purpose of manipulating neural structures and

influencing political behavior is sobering. This capability is even more concerning as it can likely be accomplished using subliminal imagery of which a target audience is unaware. Because of its focus on manipulating actual neural structures in the brain, it goes beyond what has been conceptualized as "cognitive hacking," a phenomenon more concerned with manipulating perception through the use of deception. For example, a common illustration of cognitive hacking involves the case of Mark Jakob, who created a series of false media releases to lower the cost of a specific stock and subsequently realized a significant profit (Cybenko et al., 2002). Although cognitive hacking can be covert and include the manipulation of perceptions, the concept does not address shaping behavior through the targeted activation of neural structures.

A simple way to conceptualize neurocognitive hacking is through the lens of a Russian propaganda sample used prior to the 2016 U.S. presidential election. Below is a highly inflammatory anti–Hillary Clinton advertisement that surfaced in the months leading up to the election. Although there is no way to quantify the amount of influence this or other ads may have had on the undecided electorate, it is possible that enough voters were swayed in critical states to have influenced the outcome of the election. Consider if, prior to viewing such an ad (Figure 2), subliminal, mortality-related images (Figure 1) were presented to activate the amygdalae and its associated neural components (i.e., threat response activation) of potential voters. Based on knowledge of the effects of mortality-related stimuli on in-group/out-group behavior, it is possible the images would have generated even greater emotion resonance and anti-Clinton sentiment on behalf of undecided voters.

PSYOPs personnel have been known to utilize disinformation campaigns (e.g., spreading rumors) to exacerbate underlying levels of societal conflict. And, with the advent of social media platforms, disinformation can spread more quickly and even generate lethal violence against perceived out-groups. For example, in early 2018, at least nine people were killed in India as a result of a rumor being spread in rural communities regarding the existence of a child abduction ring (Dwoskin & Gowen, 2018). Using WhatsApp, tens of thousands of unsuspecting citizens spread video images of a faked child abduction, resulting in enraged local mobs attacking and killing innocent strangers suspected of involvement. Therefore, it is likely that the use of neurocognitive hacking techniques to activate threat-related neural structures of a targeted audience, prior to initiating a disinformation/rumor campaign, would increase both effectiveness and the rate of dissemination.

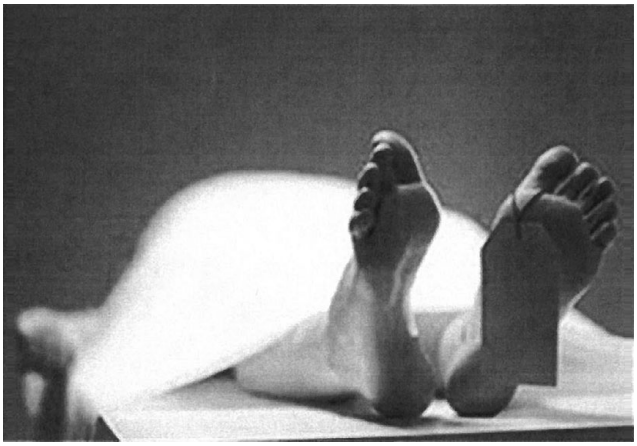

**Figure 1.** A dead body on a gurney is an example of a mortality-related stimulus. Shutterstock.com, royalty-free photo.


**Figure 2.** An example of a Russian-produced propaganda meme found on Facebook prior to the 2016 U.S. Presidential election (Singer & Brooking, 2018).

Additionally, strategically targeting specific members of a community who are more likely to believe conspiracy theories could increase both the rate and success at which the disinformation is spread. For instance, research suggests that political conservatives and less

educated individuals are more likely to believe in conspiracies (Douglas et al., 2015; Fessler et al., 2017). Furthermore, there is research suggesting that individuals who are 65 or older are seven times more likely to share disinformation on social media than younger individuals (Guess et al., 2019). Thus, initially targeting older, less educated, and conservative members of a community with neurocognitive hacking attacks, followed by socially engineered, culturally appropriate disinformation, may increase the probability that the disinformation is ingested and disseminated throughout the community.

In remote tactical operations, in which military personnel need access to adversaries' computer systems to disrupt command and control capabilities, neurocognitive hacking techniques could also be operationally useful. For example, subliminally prompting enemy forces with mortality-related stimuli may increase their propensity to open socially engineered emails containing malicious payloads, especially if the subject lines contain culturally resonant references.

In addition to utilizing subliminal mortality-related imagery, the use of subliminal sounds to induce or compound an effect is also a theoretical possibility. Research suggests that aversive sounds at specific acoustic frequencies can activate the human amygdala (Kumar et al., 2012). Although this research did not investigate the effects of sounds in subliminal frequencies, exploring any possible compounding effects on behavior when combining subliminal visual and auditory prompts would be of interest, as the observed effects from visual prompts tend to last longer when given multiple times (Levy et al., 2014). Examples of effective mortality-related auditory prompts may include hissing sounds from venomous snakes or linguistic threats such as the words "death" and "kill."

## Future research

In light of revelations regarding Russian interference into U.S. and European Union elections, the ultimate aim of this line of inquiry is to better understand the extent to which behavior can be manipulated in response to subliminal prompts of mortality-related stimuli (M-rS) and explore means by which the effects can be mitigated (i.e., neurocognitive cybersecurity). These opportunities include investigating the effects of M-rS on hostile attribution, voting behavior, and group polarization. Given prior evidence suggesting M-rS produces effects similar to state anxiety (Gauthier, 2011) along with evidence suggesting state anxiety can be compounded (Pederson & Larson, 2016), exploring the relationship between priming frequency and behavior would be of interest (e.g., would prompting with 20 subliminal M-rS prompts every minute be more effective in eliciting targeted behavioral outputs than one every 10 minutes?).

Also, given that state anxiety is known to disrupt cognitive functioning (Eysenk et al., 2007), exploring for decrements in reaction time, attention, and memory resulting from M-rS would be of interest. If negative effects were found, and given susceptibility to email phishing has been attributed to limitations in cognitive ability (Goel et al., 2017), it follows that neurocognitive attacks could disrupt the speed and efficiency with which adversary military coders are able to efficiently respond to malware attacks during time-critical military operations.

Additionally, given previous research suggesting a correlation between the small ballistic eye movements referred to as micro-saccades and threat salience (Laretzaki et al., 2011), along with the strong association between the human visual system and the amygdala (Burra et al., 2013), further exploration of this connection would be of interest. A strong correlation may allow for the development of neurocognitive cybersecurity protocols for cyber operations personnel (i.e., detection of subliminal attacks using M-rS) as well as a biometric for use in medical diagnostics (e.g., Parkinson's or Alzheimer's disease) or security operations (e.g., detecting individuals with lethal ruminations/intent before boarding airplanes or entering military installations or entertainment venues).

An additional research avenue involves exploring the effects of repeated subliminal activations on the amygdala and ACC. In other words, much like the hippocampus of London taxi drivers has been shown to change after years of memory training (Maguire et al., 2006), it is logical to assume the amygdala and other neural components are similarly malleable. If so, determining whether amygdala growth moderates negative emotional reactivity (e.g., hostile attribution and ego threat) would be of interest.

Similarly, there is much research indicating the existence of neural correlates to common emotional experiences such as empathy, beauty, and romantic love (Lane & Nadel, 2002). Therefore, determining any repeated exposure effects to subliminal images known to activate these areas would be of interest and could extend the scope of neurocognitive hacking. For instance, would pairing subliminal images associated with positive emotional states with images of a cultural out-group help generate positive affect toward them? If so, how many subliminal exposures

would be required to manipulate the specific neural structures and produce an effect? Hundreds an hour? Thousands a day? Millions over a period of weeks or months?

Finally, as evidence suggests that "mere exposure" to subliminal images of neutral objects can subsequently increase positive affiliation for them (Zajonc, 2001), extending this line of research to neurocognitive hacking techniques may prove useful in civil-military operations. For example, consider a situation whereby the United Nations deployed a peacekeeping force composed of soldiers ethnicity different from the combatants they were ordered to separate. Theoretically, exposing the combatants to subliminal images of the ethnically different peacekeeping troops before the deployment may decrease the amount of suspicion or resistance the indigenous populations initially generate.

## Conclusion

In February 2013, Valery Gerasimov, a retired Russian general, published a short essay on the use of information in modern warfare that came to be known as the "Gerasimov Doctrine" (Duncan, 2018). Among other things, the doctrine highlighted the need for Russia to possess the capability to execute sustained information operations for purposes of creating chaos and unrest against adversaries. Russia is assessed to have used the tactics outlined in the Gerasimov Doctrine during its 2014 Ukrainian operations and prior to its annexation of Crimea (Duncan, 2018). Judging by the information in the U.S. Intelligence Community report on Russian social media hacking and the Office of Special Counsel's February 2018 indictment, Russia has now turned its sights on Western liberal democracies. In fact, the director of the U.S. Federal Bureau of Investigation recently warned of the ongoing interference and "significant counterintelligence threat" posed by Russians actors to the 2020 U.S. presidential election (Barnes & Goldman, 2019).

Information warfare theorists predict these types of information operations will be ubiquitous in the future (Polyakova & Boyer, 2018), so further exploration of cognitive tools like those discussed here should be undertaken to give democratic countries defensive as well as offensive leverage. Supporting the development of mitigating strategies against adversaries who may employ these tactics against democratic elections should be a priority. These mitigating strategies would best be conceptualized in terms of providing *neurocognitive cybersecurity* and prioritized for those with important military or national security-related responsibilities.

## References


Adolphs, R. (2003). Cognitive neuroscience of human social behaviour. *Nature Reviews Neuroscience*, 4(3), 165–178. https://doi.org/10.1038/nrn1056

Adolphs, R. (2009). The social brain: Neural basis of social knowledge. *Annual Review of Psychology*, 60, 693–716. https://doi.org/10.1146/annurev.psych.60.110707.163514

Adolphs, R., Tranel, D., Damasio, H., & Damasio, A. R. (1995). Fear and the human amygdala. *Journal of Neuroscience*, 15(9): 5879–5891.

Ajzen, I., & Cote, N. G. (2008). Attitudes and the prediction of behavior. In W. D. Crano & R. Prislin (Eds.), *Frontiers of social psychology*: *Attitudes and attitude change* (pp. 289–311). Psychology Press.

Arndt, J., Greenberg, J., Pyszczynski, T., & Solomon, S. (1997). Subliminal exposure to death-related stimuli increases defense of the cultural worldview. *Psychological Science*, 8(5), 379–385. https://doi.org/10.1111/j.1467-9280.1997.tb00429.x

Astorino-Courtois, A. (2017). *A cognitive capabilities agenda: A multi-step approach for closing DoD's cognitive capability gap*. Strategic Multilayer Assessment Office, U.S. Department of Defense. https://nsiteam.com/a-cognitive-capabilities-agenda-a-multi-step-approach-for-closing-dods-cognitive-capability-gap/

Barnes, J., & Goldman, A. (2019, April 26). FBI warns of Russian interference in 2020 race and boosts counterintelligence operations. *New York Times*. https://www.nytimes.com/2019/04/26/us/politics/fbi-russian-election-interference.html

Bohleber, W., & Bohleber, M. (2012). *Processes of political and terrorist radicalization in late adolescences—Some case examples* [Paper presentation]. Annual Freud Conference, Melbourne, Australia. http://www.freudconference.com/downloads/BohleberLeuzinger-BohleberRadicalizationinadolescence1-2.pdf

Bump, P. (2016, December 1). Donald Trump will be president thanks to 80,000 people in three states. *Washington Post*. https://www.washingtonpost.com/news/the-fix/wp/2016/12/01/donald-trump-will-be-president-thanks-to-80000-people-in-three-states/

Burke, B., Martens, A., & Faucher, E. (2010). Two decades of terror management theory: A meta-analysis of mortality salience research. *Personality and Social Psychology Review*, 14(2), 155–195.

Burra, N., Hervais-Adelman, A., Kerzel, D., Tamietto, M., Gelder, B. D., & Pegna, A. J. (2013). Amygdala activation for eye contact despite complete cortical blindness. *Journal of Neuroscience*, 33(25), 10483–10489. https://doi.org/10.1523/jneurosci.3994-12.2013

Custers, R. (2009). How does our unconscious know what we want? The role of affect in goal representations. In G. B.

Moskowitz & H. Grant (Eds.), *The psychology of goals* (pp. 179–202). Guilford Press.

Cybenko, G., Giani, A., & Thompson, P. (2002). Cognitive hacking: A battle for the mind. *Computer*, 35(8), 50–56. https://doi.org/10.1109/mc.2002.1023788

Devos, T. (2008). Implicit attitudes 101: Theoretical and empirical insights. In W. D. Crano & R. Prislin (Eds.), *Attitudes and persuasion* (pp. 61–94). Psychology Press.

Douglas, K. M., Sutton, R. M., Callan, M. J., Dawtry, R. J., & Harvey, A. J. (2015). Someone is pulling the strings: Hypersensitive agency detection and belief in conspiracy theories. *Thinking & Reasoning*, 22(1), 57–77. https://doi.org/10.1080/13546783.2015.1051586

Duncan, A. J. (2018). New hybrid war or old dirty tricks? The Gerasimov debate and Russia's response to the contemporary operating environment. *Canadian Military Journal*, 17(3), 6–16.

Dwoskin, E., & Gowen, A. (2018, July 23). On WhatsApp, fake news is fast and can be fatal. *Washington Post*. https://www.washingtonpost.com/business/economy/on-whatsapp-fake-news-is-fast–and-can-be-fatal/2018/07/23/a2dd7112-8ebf-11e8-bcd5-9d911c784c38_story.html

European Commission. (2019). *Report on the implementation of the action plan against disinformation*. https://eeas.europa.eu/sites/eeas/files/joint_report_on_disinformation.pdf

Eysenk, M., Derakshan, N., Sanos, R., & Calvo, M. (2007). Anxiety and cognitive performance: Attentional control theory. *Emotion*, 7(2), 336–353.

Fang, Z., Li, H., Chen, G., & Yang, J. (2016). Unconscious processing of negative animals and objects: Role of the amygdala revealed by fMRI. *Frontiers in Human Neuroscience*, 10. https://doi.org/10.3389/fnhum.2016.00146

Fessler, D. M., & Navarrete, C. D. (2005). The effect of age on death disgust: Challenges to terror management perspectives. *Evolutionary Psychology*, 3(1), 147470490500300. https://doi.org/10.1177/147470490500300120

Fessler, D. M., Pisor, A. C., & Holbrook, C. (2017). Political orientation predicts credulity regarding putative hazards. *Psychological Science*, 28(5), 651–660. https://doi.org/10.1177/0956797617692108

Fitzgerald, F. F. (1972). *Fire in the lake*. Atlantic Monthly Press.

Gauthier, C. (2011). *Are we afraid or anxious about death? Clarifying the meaning of "terror" in terror management theory* [Doctoral dissertation]. New School for Social Research.

Glassner, B. (1985). Review of *Social identity and intergroup relations*, by H. Tajfel. *Contemporary Sociology*, 14(4), 520–521. https://doi.org/10.2307/2069233.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, 18(1), 22–44. https://doi.org/10.17705/1jais.00447

Greenberg, J., Pyszczynski, T., & Solomon, S. (1986). The causes and consequences of a need for self-esteem: A terror management theory. In R. F. Baumeister (Ed.), *Public and private self* (pp. 189–212). Springer-Verlag. https://doi.org/10.1007/978-1-4613-9564-5_10

Greenberg, J., Pyszczynski, T., Solomon, S., Rosenblatt, A., Veeder, M., Kirkland, S., & Lyon, D. (1990). Evidence for terror management theory II: The effects of mortality salience on reactions to those who threaten or bolster the cultural worldview. *Journal of Personality and Social Psychology*, 58 (2), 308–318. https://doi.org/10.1037//0022-3514.58.2.308

Guess, A., Nagler, J., & Tucker, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*, 5(1). https://doi.org/10.1126/sciadv.aau4586

Halpern, S. (2018, March 30). Cambridge Analytica and the perils of psychographics. *The New Yorker*. https://www.newyorker.com/news/news-desk/cambridge-analytica-and-the-perils-of-psychographics

Haselton, M. G., Bryant, G. A., Wilke, A., Frederick, D. A., Galperin, A., Frankenhuis, W. E., & Moore, T. (2009). Adaptive rationality: An evolutionary perspective on cognitive bias. *Social Cognition*, 27(5), 733–763. https://doi.org/10.1521/soco.2009.27.5.733

Haselton, M. G., & Buss, D. M. (2000). Error management theory: A new perspective on biases in cross-sex mind reading. *Journal of Personality and Social Psychology*, 78(1), 81–91. https://doi.org/10.1037//0022-3514.78.1.81

Heslen, J. (2016). *Leading a more effective intelligence community: Understanding and managing the cognitive challenges of human intelligence collection in lethal environments* [Doctoral dissertation]. University of Oklahoma.

Hogg, M. A., Terry, D. J., & White, K. M. (1995). A tale of two theories: A critical comparison of identity theory with social identity theory. *Social Psychology Quarterly*, 58(4), 255–269. https://doi.org/10.2307/2787127

Holbrook, C., Sousa, P., & Hahn-Holbrook, J. (2011). Unconscious vigilance: Worldview defense without adaptations for terror, coalition, or uncertainty management. *Journal of Personality and Social Psychology*, 101(3), 451–466. https://doi.org/10.1037/a0024033

Jorgenson, L. A., Newsome, W. T., Anderson, D. J., Bargmann, C. I., Brown, E. N., Deisseroth, K., … Wingfield, J. C. (2015).

The brain initiative: Developing technology to catalyse neuroscience discovery. *Philosophical Transactions of the Royal Society B: Biological Sciences*, 370(1668), 20140164. https://doi.org/10.1098/rstb.2014.0164

Jost, J., Banaji, M., & Nosek, B. (2016). A decade of system justification theory: Accumulated evidence of conscious and unconscious bolstering of the status quo. *Political Psychology*, 25(6), 881–919. https://doi.org/10.31234/osf.io/6ue35

Jowett, G. S., & O'Donnell, V. (1986). *Propaganda and persuasion*. Sage Publications.

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Kirkpatrick, L., & Navarrete, C. (2006). Reports of my death anxiety have been greatly exaggerated: A critique of terror management theory from an evolutionary perspective. *Psychological Inquiry*, 17(4), 288–298. https://doi.org/10.1080/10478400701366969

Kumar, S., Kriegstein, K. V., Friston, K., & Griffiths, T. D. (2012). Features versus feelings: Dissociable representations of the acoustic features and valence of aversive sounds. *Journal of Neuroscience*, 32(41), 14184–14192. https://doi.org/10.1523/jneurosci.1759-12.2012

Lane, R. D., & Nadel, L. (2002). *Cognitive neuroscience of emotion*. Oxford University Press.

Laretzaki, G., Plainis, S., Vrettos, I., Chrisoulakis, A., Pallikaris, I., & Bitsios, P. (2011). Threat and trait anxiety affect stability of gaze fixation. *Biological Psychology*, 86(3), 330–336. https://doi.org/10.1016/j.biopsycho.2011.01.005

Larson, E., Darilek, R., Kaye, D., Morgan, F., Nichiporuk, B., Durham-Scott, D., Thurston, C., & Leuschner, K. (2009). *Understanding commanders' information needs for influence operations* (Report No W74V8H-06-C-0001). RAND Corporation. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG656.pdf

Levy, B. R., Pilver, C., Chung, P. H., & Slade, M. D. (2014). Subliminal strengthening. *Psychological Science*, 25(12), 2127–2135. https://doi.org/10.1177/0956797614551970

Maguire, E. A., Woollett, K., & Spiers, H. J. (2006). London taxi drivers and bus drivers: A structural MRI and neuropsychological analysis. *Hippocampus*, 16(12), 1091–1101. https://doi.org/10.1002/hipo.20233

Markova, I. (2008). Persuasion and propaganda. *Diogenes*, 55 (1), 37–51. https://doi.org/10.1177/0392192107087916

Meyer, R. (2014, June 28). Everything we know about Facebook's secret mood manipulation experiment. *The Atlantic*. https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/

Nagl, J. A. (2002). *Learning to eat soup with a knife: Counterinsurgency lessons from Malaya and Vietnam*. University of Chicago Press.

Nasrallah, M., Carmel, D., & Lavie, N. (2009). Murder, she wrote: Enhanced sensitivity to negative word valence. *Emotion*, 9(5), 609–618. https://doi.org/10.1037/a0016305

National Public Radio. (2018, March 27). *They don't care: Whistleblower says Cambridge Analytica aims to undermine democracy*. https://www.npr.org/sections/thetwo-way/2018/03/27/597279596/they-don-t-care-whistleblower-says-cambridge-analytica-seeks-to-undermine-democr

Nyabola, N. (2019, February 15). *The spectre of Cambridge Analytica still haunts African elections*. Al Jazeera. https://www.aljazeera.com/indepth/opinion/nigerian-elections-money-190215080009476.html

Office of the Director of National Intelligence. (2017, January 6). *Background to 'Assessing Russian activities and intentions in recent US elections': The analytic process and cyber incident attribution*. https://www.dni.gov/files/documents/ICA_2017_01.pdf

Pearson, E. (2015). The Case of Roshonara Choudhry: Implications for theory on online radicalization, ISIS women, and the gendered jihad. *Policy & Internet*, 8(1), 5–33. https://doi.org/10.1002/poi3.101

Pedersen, W. S., & Larson, C. L. (2016). State anxiety carried over from prior threat increases late positive potential amplitude during an instructed emotion regulation task. *Emotion*, 16(5), 719–729. https://doi.org/10.1037/emo0000154

Phelps, E. A., Oconnor, K. J., Cunningham, W. A., Funayama, E. S., Gatenby, J. C., Gore, J. C., & Banaji, M. R. (2000). Performance on indirect measures of race evaluation predicts amygdala activation. *Journal of Cognitive Neuroscience*, 12 (5), 729–738. https://doi.org/10.1162/089892900562552

Polyakova, A., & Boyer, S. P. (2018). *The Future of political warfare: Russia, the West, and the coming age of global digital competition*. Brookings Institution. https://www.brookings.edu/wp-content/uploads/2018/03/the-future-of-political-warfare.pdf

Quirin, M., Loktyushin, A., Arndt, J., Küstermann, E., Lo, Y.-Y., Kuhl, J., & Eggert, L. (2011). Existential neuroscience: A functional magnetic resonance imaging investigation of neural responses to reminders of one's mortality. *Social Cognitive and Affective Neuroscience*, 7(2), 193–198. https://doi.org/10.1093/scan/nsq106

Rosenblatt, A., Greenberg J., Solomon, S., Pyszczynski, T., & Lyon, D. (1989). Evidence for terror management theory I: The effects of mortality salience on reactions to those who violate or uphold cultural values. *Journal of Personality and Social Psychology*, 57(4), 681–690. https://doi.org/10.1037//0022-3514.57.4.681

Singer, P.W., Emerson, B.T. (2018). *Like War: The Weaponization of Social Media*. Houghton-Mifflin Harcourt Publishing.

Solomon, S., Greenberg, J., & Pyszczynski, T. (2004). The cultural animal: Twenty years of terror management theory and research. In J. Greenberg, S. L. Koole, & T. Pyszczynski (Eds.), *Handbook of experimental existential psychology* (pp. 13–34). Guilford Press.

Stanovich, K., & West, R. (2000). Individual differences in reasoning: Implications for the rationality debate. *Behavioral and Brain Sciences*, 23(5), 645–726. https://doi.org/10.1017/s0140525x00003435

Taylor, P. M. (2003). *Munitions of the mind: A history of propaganda from the ancient world to the present day*. Manchester University Press.

Thomas, T. (2004). Russia's reflexive control theory and the military. *Journal of Slavic Military Studies*, 17(2), 237–256. https://doi.org/10.1080/13518040490450529

Tritt, S. M., Inzlicht, M., & Harmon-Jones, E. (2012). Toward a biological understanding of mortality salience (and other threat compensation processes). *Social Cognition*, 30(6), 715–733. https://doi.org/10.1521/soco.2012.30.6.715

U.S. Department of the Army. (2003). *Psychological operations tactics, techniques, and procedures* (FM 33-1-1). https://fas.org/irp/doddir/army/fm3-05-301.pdf

U.S. Department of Justice. (2018). *United States of America v. Internet Research Agency LLC.* https://www.justice.gov/file/1035477/download

U.S. Department of Defense (2014). JP-3-13, Information Operations (JP 3-13). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

Valeriano, B., & Jensen, B. (2019). *The myth of the cyber defense: The case for restraint* (Policy Analysis No. 862). CATO Institute. https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint

Votel, J., Clevland, C., Connett, C., & Irwin, W. (2016). Unconventional warfare in the gray zone. *Joint Forces Quarterly*, 80, 101–109.

Weimann, G. (2015). Terrorist migration to social media. *Georgetown Journal of International Affairs*, 16(1), 180–187.

Weingarten, E., Chen, Q., Mcadams, M., Yi, J., Hepler, J., & Albarracin, D. (2016). On priming action: Conclusions from a meta-analysis of the behavioral effects of incidentally-presented words. *Current Opinion in Psychology*, 12, 53–57. https://doi.org/10.1016/j.copsyc.2016.04.015

Whalen, P. J. (1998). Fear, vigilance, and ambiguity: Initial neuroimaging studies of the human amygdala. *Current Directions in Psychological Science*, 7(6), 177–188. https://doi.org/10.1111/1467-8721.ep10836912

Wheeler, M. E., & Fiske, S. T. (2005). Controlling racial prejudice. *Psychological Science*, 16(1), 56–63. https://doi.org/10.1111/j.0956-7976.2005.00780.x.

Windsor, L. (2018). The language of radicalization: Female internet recruitment to participation in ISIS activities. *Terrorism and Political Violence. Advance online publication.* https://doi.org/10.1080/09546553.2017.1385457

Winkielman, P., & Berridge, K. C. (2004). Unconscious emotion. *Current Directions in Psychology*, 13(3), 120–123.

Winkielman, P., Berridge, K. C., & Wilbarger, J. L. (2005). Unconscious affective reactions to masked happy versus angry faces influence consumption behavior and judgments of value. *Personality and Social Psychology Bulletin*, 31(1), 121–135. https://doi.org/10.1177/0146167204271309

Zajonc, R. (2001). Mere exposure: A gateway to the subliminal. *Current Directions in Psychological Science*, 10(6), 224–228. https://doi.org/10.1111/1467-8721.00154