

**REPORT DOCUMENTATION PAGE**

Form Approved  
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.  
**PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

<b>1. REPORT DATE (DD-MM-YYYY)</b> 04/22/2019		<b>2. REPORT TYPE</b> Master's of Operational Studies		<b>3. DATES COVERED (From - To)</b> JUN 2018 - JUN 2019	
<b>4. TITLE AND SUBTITLE</b> Operation FORTITUDE 2035: The Role of Deception in Future War				<b>5a. CONTRACT NUMBER</b> N/A	
				<b>5b. GRANT NUMBER</b> N/A	
				<b>5c. PROGRAM ELEMENT NUMBER</b> N/A	
<b>6. AUTHOR(S)</b> Richardson, Daniel, R., Major, USAF				<b>5d. PROJECT NUMBER</b> N/A	
				<b>5e. TASK NUMBER</b> N/A	
				<b>5f. WORK UNIT NUMBER</b> N/A	
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> USMC School of Advanced Warfighting Marine Corps University 2044 South Street Quantico, VA 22134				<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b> N/A	
<b>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b>				<b>10. SPONSOR/MONITOR'S ACRONYM(S)</b>	
				<b>11. SPONSOR/MONITOR'S REPORT NUMBER(S)</b> N/A	
<b>12. DISTRIBUTION/AVAILABILITY STATEMENT</b> Approved for public release, distribution unlimited.					
<b>13. SUPPLEMENTARY NOTES</b>					
<b>14. ABSTRACT</b> This paper argues that in light of great power competition, operational deception offers a proven path toward mitigating risk associated with the erosion of US technological superiority through 2035. To support this argument, the paper analyzes three historical operational deceptions from the 20th century using a framework developed by the Central Intelligence Agency to illuminate common deception characteristics. The feasibility of targeting these characteristics in the future operating environment is then analyzed, concluding that it will be possible. Five recommendations then follow for improving the joint force's ability to create operational deceptions during great power competition and conflict.					
<b>15. SUBJECT TERMS</b> Deception; operational deception; large-scale deception; self-deception; National Defense Strategy; great power competition; Operation FORTITUDE; 1973 Arab-Israeli War; the 1973 Yom Kippur War; the Ramadan War; the First and Second Offensives of the Korean War; sensors; artificial intelligence; human cognition; cognition biases					
<b>16. SECURITY CLASSIFICATION OF:</b>			<b>17. LIMITATION OF ABSTRACT</b>	<b>18. NUMBER OF PAGES</b>	<b>19a. NAME OF RESPONSIBLE PERSON</b>
<b>a. REPORT</b>	<b>b. ABSTRACT</b>	<b>c. THIS PAGE</b>			<b>19b. TELEPHONE NUMBER (Include area code)</b>
Unclass	Unclass	Unclass	UU	28	USMC School of Advanced Warfighting (703) 432-5420 (Admin Office)

*United States Marine Corps  
School of Advanced Warfighting  
Marine Corps University  
3070 Moreell Avenue  
Marine Corps Combat Development Command  
Quantico VA 22134*

## **FUTURE WAR PAPER**

### ***Operation FORTITUDE 2035: The Role of Deception in Future War***

SUBMITTED IN PARTIAL FULFILLMENT  
OF THE REQUIREMENTS FOR THE DEGREE OF  
MASTER OF OPERATIONAL STUDIES

***Major Daniel R. Richardson***

AY 2018-19

Mentor: Dr. Lauren Mackenzie

Approved: \_\_\_\_\_

Date: \_\_\_\_\_

*28 May 19*

## DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE SCHOOL OF ADVANCED WARFIGHTING OF ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

## **INTRODUCTION**

The historical record is unequivocal in its support for deception as an effective weapon of war. A landmark study conducted by Dr. Barton Whaley, who investigated 138 military engagements between 1914 and 1967, showed that when deception achieved surprise the attacker caused 14.5 enemy casualties for every one of his own, whereas without surprise the casualty ratio fell to parity.<sup>1</sup> The quantitative evidence is clear: in warfighting, surprise offers a marked advantage, and deception is its most effective agent.<sup>2</sup>

This truth is especially important for the US to consider in future war because the nation has recently exited a prolonged period of preeminence as the world's sole superpower following the collapse of the Soviet Union in 1991. In the years that followed, technological superiority and a focus on violent extremism changed the organization, training, and equipment of the US military, including an atrophy of large-scale deception skills tailored to the unique challenges of great power competition. However, two changes in the global security environment have combined to threaten US national interests in a way that hasn't been seen for over 25 years, and operational deception offers a proven path toward mitigating this risk.

The first change is an imposing, assertive China and a revisionist Russia, identified as the long-term strategic competitors in the 2018 National Defense Strategy (NDS), and returning the US to an era of great power competition against nation states.<sup>3</sup> The threat posed by great power competition's reemergence is exacerbated by the second change, the erosion of the US military's technological superiority. Factors contributing to this erosion include a declining manufacturing base, instability in the defense industrial base due to budgeting uncertainty, the theft of intellectual property by foreign nations, and the decline of military research powering commercial innovation.<sup>4</sup>

While this combination of peer competitors and the loss of technological superiority should compel a renewed interest in the use of deception, forecasts of the future operating environment (FOE) envision advances in technology that significantly change the character of war and bring into question whether the US military could still successfully conduct a large-scale deception. Forecast technologies involve an increased ability to collect intelligence, a corresponding decrease in the ability to conceal the signatures of people and equipment, and revolutionary advances in computer-aided decision-making. Yet despite the implications these developments suggest, it is argued that deception at the operational level of war will still be possible in 2035.

A two-step analysis will support this thesis. First, three historical operational deceptions from the 20th century will be examined using a framework developed by the Central Intelligence Agency (CIA) to illuminate each example's deception characteristics. The CIA framework was the product of a Deception Research Program effort in 1981 that reviewed historical deception case studies, including the work of Dr. Whaley, and synthesized 10 maxims that underpin the creation of successful deceptions (see Figure 1).<sup>5</sup> Second, deception characteristics common to all three historical examples will be evaluated against the 2035 FOE to discern whether they will still be feasible. Only then will recommendations for enhancing the US military's ability to employ large-scale deception be offered.

## **“Deception Maxims: Fact and Folklore” – June 1981**

### **Central Intelligence Agency, Deception Research Program**

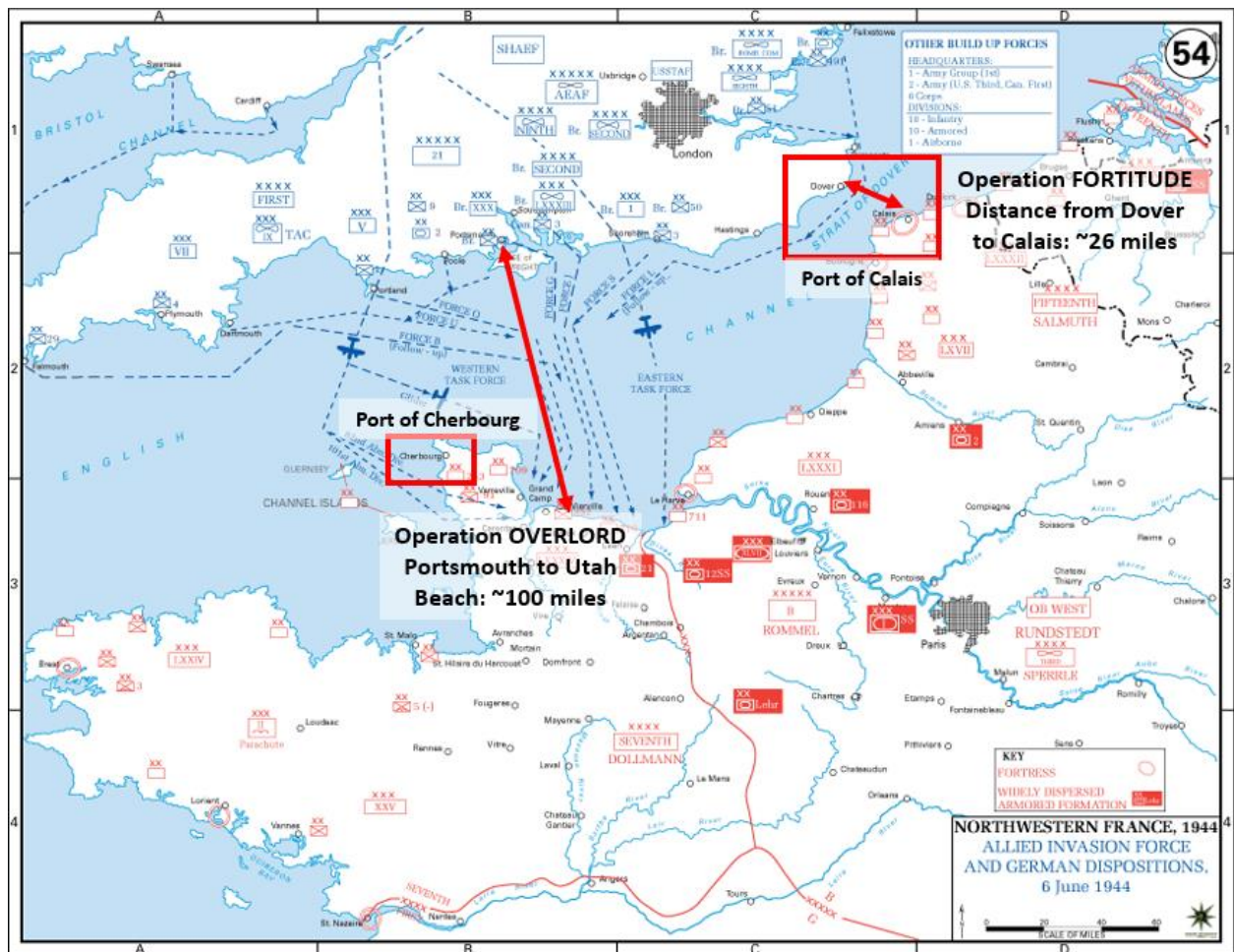
1. **Magruder’s Principle—the Exploitation of Preconceptions:** It is generally easier to induce an opponent to maintain a preexisting belief than to present notional evidence to change that belief. Thus, it may be more fruitful to examine how an opponent’s existing beliefs can be turned to advantage than to attempt to alter these views.
2. **Limitations to Human Information Processing:** There are several limitations to human information processing that are exploitable in the design of deception schemes—among these, the law of small numbers and susceptibility to conditioning.
3. **The Multiple Forms of Surprise:** Surprise can be achieved in many forms. In military engagements, these forms include location, strength, intention, style, and timing. Should it not prove attractive or feasible to achieve surprise in all dimensions, it may still be possible to achieve surprise in at least one of these. Thus, for example, if intentions cannot be concealed, it may still be possible to conceal timing (cry-wolf syndrome), place, strength, or style.
4. **Jones’ Lemma:** Deception becomes more difficult as the number of channels of information available to the victim increases. However, within limits, the greater the number of controlled channels the greater the likelihood of the deception being believed.
5. **A Choice Among Types of Deception:** Where possible the objective of the deception planner should be to reduce the ambiguity in the mind of the victim, to force him to seize upon a notional world view as being correct—not making him less certain of the truth, but more certain of a particular falsehood. However, increasing the range of alternatives and/or the evidence to support any of many incorrect alternatives—in the jargon ‘increasing the noise’—may have particular use when the victim already has several elements of truth in his possession.
6. **Axelrod’s Contribution: The Husbanding of Assets:** There are circumstances where deception assets should be husbanded despite the costs of maintenance and risk of waste, awaiting a more fruitful use. Such decisions are often susceptible to rational analysis.
7. **A Sequencing Rule:** Deception activities should be sequenced so as to maximize the persistence of the incorrect hypothesis(es) for as long as possible. In other words, “Red-handed” activities should be deferred to the last possible instant.
8. **The Importance of Feedback:** A scheme to ensure accurate feedback increases the chance of success in deception.
9. **“The Monkey’s Paw”:** Deception efforts may produce subtle and unwanted side effects. Planners should be sensitive to such possibilities and, where prudent, take steps to minimize these counter-productive aspects.
10. **Care in the Design of Planned Placement of Deceptive Material:** Great care must be exercised in the design of schemes to leak notional plans. Apparent “windfalls” are subject to close scrutiny and often disbelieved. Genuine leaks often occur under circumstances thought improbable.

**Figure 1:** Presents the 10 deception “maxims” developed by the CIA’s exploratory Deception Research Program in an effort to “aid intelligence analysts in thinking about the problem of deception and in detecting, analyzing and evaluating foreign deception schemes relevant to current intelligence problems.”<sup>6</sup>

## **HISTORICAL EXAMPLES**

### **WWII: OPERATION FORTITUDE**

The first historical deception example is Operation FORTITUDE, the combined US and British deception plan supporting the Allied invasion of northern France during World War II. Deception was essential to the Allied landing to prevent the Germans from deploying forces in sufficient strength to repulse the seizing of a lodgment. The Germans considered the coastline near the Port of Calais to be the most likely site for an Allied landing in Western Europe and had stationed the formidable Fifteenth Army nearby to repel any attempted invasion (see Map 1).



**Map 1:** Depicts location of the Allied deception code named Operation FORTITUDE near the Port of Calais, versus the actual landing site at Normandy east of the Port of Cherbourg. Note: overlays have been added to the original map to highlight aspects of the deception.<sup>7</sup>

Aware of this German preconception thanks to ULTRA, the code breaking program that allowed the Allies to decrypt German message traffic, the Allied deception plan aimed to reinforce this belief. Plans were drawn up for a fake amphibious assault at Calais with the goal of fixing the German Fifteenth Army 170 miles from the actual landing beaches.<sup>8</sup> Additionally, a fake army group was created with decoy infrastructure and rubberized versions of equipment near the Strait of Dover. Allied double-agents, false radio traffic, and the select passage of German surveillance aircraft became conduits for passing false intelligence.<sup>9</sup> Furthermore, the Allied bombing campaign preceding the invasion explicitly required that for every bomb

dropped on defenses in the real landing area, two had to be dropped in the deception landing area at Calais.<sup>10</sup>

The deception was a complete success. When the invasion at Normandy occurred, the Germans believed it was a diversion and the Fifteenth Army was not moved in time to oppose the Allied landing.<sup>11</sup>

Using the CIA deception framework, Operation FORTITUDE relied on at least five maxims:

1. Maxim 1: Magruder's Principle—the Exploitation of Preconceptions, which states that “it is generally easier to induce an opponent to maintain a preexisting belief than to present notional evidence to change that belief.”<sup>12</sup> The Allied deception plan was meant to reinforce the German preconception that the most likely location for an invasion would be near the port of Calais.
2. Maxim 2: Limitations to Human Information Processing, which states that “there are several limitations to human information processing...[including] susceptibility to conditioning.”<sup>13</sup> By creating a fake invasion plan with supporting infrastructure, German intelligence was conditioned by signals that reinforced their belief that the landing would occur near Calais.
3. Maxim 5: A Choice Among Types of Deception, which states that “where possible the objective of the deception planner should be to reduce the ambiguity in the mind of the victim...not making him less certain of the truth, but more certain of a particular falsehood.”<sup>14</sup> Operation FORTITUDE was primarily an ambiguity-decreasing deception meant to convince Germany that a landing would occur at Calais in the late summer of 1944.

4. Maxim 6: Axelrod's Contribution: The Husbanding of Assets, which states that "there are circumstances where deception assets should be husbanded despite the costs...awaiting a more fruitful use."<sup>15</sup> This maxim was employed in the judicious use of ULTRA intercepts to support other operations in order to ensure ULTRA was not compromised before the larger payoff of Operation FORTITUDE.
5. Maxim 8: The Importance of Feedback, which states that "a scheme to ensure accurate feedback increases the chance of success in deception."<sup>16</sup> The CIA framework uses ULTRA to illustrate this point, citing it as one of the best examples of the role of feedback in modern warfare.

## **EGYPT AND THE 1973 RAMADAN WAR**

The second historical deception is the Egyptian offensive that began the 1973 Ramadan War, the fourth Arab-Israeli war rooted in "competing claims to religious and cultural homelands between Jews and Muslims."<sup>17</sup> During the previous war, Israel had seized Egyptian territory including the Sinai Peninsula to the east bank of the Suez Canal, and Egyptian plans to retake its lost territory were hatched shortly thereafter.<sup>18</sup>

After the war, Israel assumed their ability to project air power and their nearly 100-mile earthen defensive barrier along the Suez Canal would deter Egypt from going to war. This preconception colored Israeli interpretations of intelligence suggesting an impending Egyptian invasion in October 1973, causing multiple warning signals to be dismissed.<sup>19</sup>

Though it is unclear whether Egyptian President Sadat knew of this Israeli preconception, he nonetheless embarked on a comprehensive political and military deception scheme to reinforce the belief that Egypt's military was weak. Politically, Sadat's deception relied on two efforts: misleading leaks to news outlets suggesting the Egyptian army was ill-equipped and ill-

trained, and a change in rhetoric by Sadat in public speeches.<sup>20</sup> Militarily, Sadat secretly acquired modern Soviet surface-to-air missiles and anti-tank weapons that Israeli Defense Forces had not yet encountered.<sup>21</sup> Moreover, Sadat conducted three large scale troop mobilizations in 1973 to condition Israeli leaders to the presence of troop concentrations near the Suez Canal. The first two of these resulted in counter mobilizations by Israel at significant cost.<sup>22</sup> Egyptian forces used these mobilizations to position equipment that would rapidly penetrate the earthen defensive wall (see Photos 1 and 2).



**Photo 1:** The 70' high earthen defensive wall is shown, along with a passage blasted through the sand by Egyptian combat engineers using high pressure water. Israeli defense plans assumed it would take a minimum of 12 hours to blast through the sand wall using explosives, giving Israel adequate time to mobilize reserve forces. High pressure water broke through in 3 hours.<sup>23</sup>



**Photo 2:** Shows one of several bridge crossings constructed by the Egyptians. It spanned the width of the Suez Canal, which varies between 590 to 720 feet. It was built in a matter of hours following the blasting of passages through the earthen defensive wall.<sup>24</sup>

When war began on 6 October 1973, Egyptian forces achieved complete surprise.

Bridgeheads were established far earlier than Israel thought possible and the use of advanced surface-to-air and anti-tank missiles defeated initial Israeli counterattacks.

Analyzing the Ramadan War using the CIA framework, there are at least four maxims unpinning the Egyptian deception and one that Israeli self-deception capitalized on:

1. Maxim 1: Magruder's Principle. Israeli senior leaders were deceived by their own preconceptions about the conditions required before Egypt would attack. At the strategic level, Egyptian deception plans reinforced this preconception by projecting an image of military weakness. At the tactical level, the innovative use of high pressure water hoses to blast through the Israeli defensive wall in three hours exploited the Israeli assumption that its defenses afforded at least 12 hours of protection while it mobilized reinforcements, creating an operational level opportunity.

2. Maxim 2: Limitations to Human Information Processing. The three Egyptian army mobilizations conditioned Israeli leaders to the presence of Egyptian forces along the Suez Canal. This is supported by the fact that Israel counter-mobilized for the first two, but not for the third.
3. Maxim 5: A Choice Among Types of Deception. Egypt's deception efforts were solely aimed at convincing the Israelis that another war would not occur. From information operations (IO) to multiple mobilizations to secretly acquiring new weapons, Sadat's actions reinforced the idea that Egypt was not an immediate threat.
4. Maxim 6: Axelrod's Contribution: The Husbanding of Assets. In today's vernacular, the terms "reveal" and "conceal" illuminate this maxim. Egypt secretly acquired new surface-to-air missiles and anti-tank missiles. This enabled Egyptian forces to defeat the first air and ground counterattacks launched by Israel and reach their planned military objectives.

### **CHINESE ENTRANCE INTO THE KOREAN WAR**

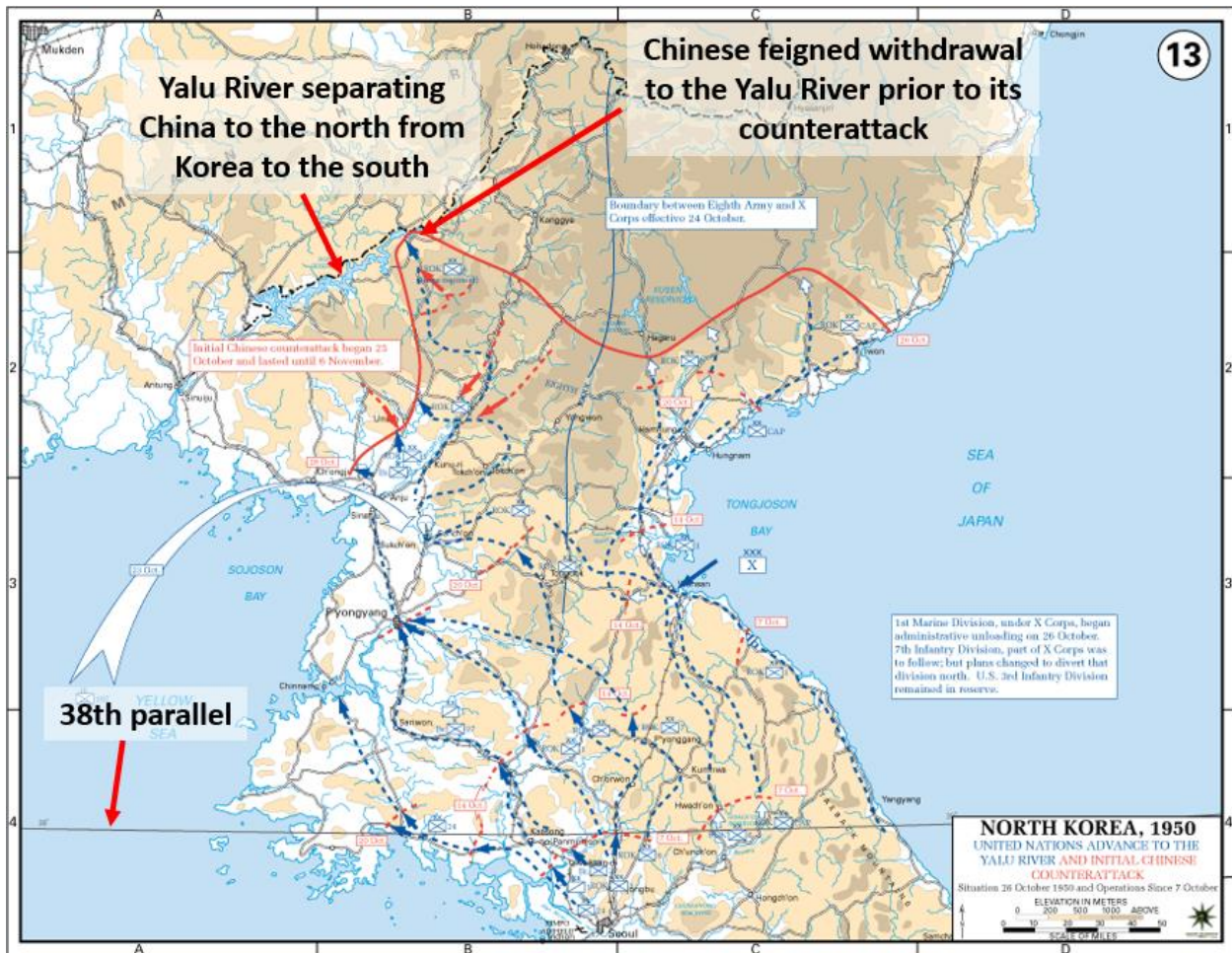
The final historical deception is the Chinese entrance into the Korean War, which effectively surprised United Nations Command (UNC) forces approaching the Yalu River.

In October 1950, General MacArthur had just achieved a stunning reversal against the North Korean People's Army (NKPA) following his amphibious end run at Inchon, and was pursuing the remnants of the NKPA toward the Yalu River despite a warning from the Chinese not to cross north of the 38th parallel.<sup>25</sup> MacArthur, aware that the Chinese Communist Party had just finished a brutal civil war and was technologically inferior, concluded this was an idle threat.

In reality, after UNC forces crossed the 38th parallel, Marshal Peng Dehau, the commander of the Chinese People's Volunteers (CPV), was ordered to enter Korea and fight. Knowing he faced an adversary with air superiority and a tremendous firepower advantage, Peng moved his 300,000 soldiers in secret across hundreds of miles to conceal the true size of his force. MacArthur and his staff, convinced that the Chinese would not fight in strength this late in the war against a far superior adversary, minimized the emerging intelligence picture of CPV forces.

After conducting probing attacks designed to arrest the UNC advance without revealing the true size of his force, Peng broke contact and began a feigned withdrawal back to the Yalu, further reinforcing MacArthur's preconception. In Marshal Peng's own words, "we employed the tactic of purposely showing ourselves to be weak, increasing the arrogance of the enemy...and luring him deep into our areas."<sup>26</sup>

MacArthur bought this ruse and when Peng's full-strength counteroffensive began, it caught UNC forces completely by surprise (see Map 2). The subsequent fighting forced a UNC withdrawal south of the 38th parallel, and Peng's deception was key to the eventual outcome of the war.



**Map 2:** Depicts Chinese deception during the First and Second Offensives as a feigned withdrawal to the Yalu River in order to lure United Nations Command forces into a surprise counteroffensive. Note: overlays have been added to the original map to highlight the deception.<sup>27</sup>

Using the CIA framework to analyze Peng’s Offensives, there are three maxims the Chinese deception capitalized on:

1. Maxim 1: Magruder’s Principle. MacArthur was convinced the Chinese would not attack UNC forces in strength. The CPV’s secret movement and limited initial probing attacks reinforced this preconception by masking the true size of CPV forces.
2. Maxim 2: Limitations to Human Information Processing. In addition to the tendency to become conditioned to a pattern of behavior, this maxim includes the tendency “to dismiss unlikely events as impossible events.”<sup>28</sup> Having deemed an army-level CPV

attack as highly unlikely, MacArthur and the UNC staff's minimized the emerging intelligence picture of the size of CPV forces, even after the probing attacks caused significant casualties to a Republic of Korea division.

3. Maxim 5: A Choice Among Types of Deception. Peng's deception efforts were designed to decrease ambiguity in MacArthur's mind regarding the likelihood of a CPV attack in force. Peng's covert movement of forces and seemingly abrupt withdrawal northward further convinced MacArthur that the CPV would not fight.

### **THE KEY TO UNDERSTANDING DECEPTION IN FUTURE WAR**

Having identified deception maxims unique to each historical example, three emerge as common to all: Maxim 1: Magruder's Principle; Maxim 2: Limitations to Human Information Processing; and Maxim 5: A Choice Among Types of Deception. Note that all three of these maxims seek to exploit human cognition biases. In the case of Maxim 1, it preys on the primacy of existing beliefs in decision making. Maxim 2 encompasses a host of cognition issues, but targets the innate human tendency to simplify complex phenomenon. Finally, Maxim 5 complements the previous two, as ambiguity-increasing and ambiguity-decreasing deception often plays off preconceptions and the limited ability of the human mind to process large amounts of information. Since the exploitation of human cognition biases is not true of all 10 maxims, this linkage provides a useful key for focusing the analysis of the FOE. Instead of examining all projected FOE changes, this analysis will focus on only those changes that directly affect human cognition and decision making.

With that in mind, the Joint Operating Environment (JOE) 2035 offers a useful framework for categorizing projected changes to the FOE into three main areas: World Order; Human Geography; and Science, Technology, and Engineering (ST&E).<sup>29</sup> The first two areas, World Order and Human Geography, focus on projected changes to the distribution of power across states and international organizations and trends like asymmetric population growth, migration, urbanization, and resource scarcity.<sup>30</sup> Using the previously identified key of exploiting human cognition, this analysis posits that while these changes may evolve the selection of military deception targets or the means used to signal a deception, it won't make human decision makers impervious to targeting nor will it change human cognition and decision making. As such, these changes will not impact the viability of successfully employing deception in future war.

Even in the last JOE area of ST&E, several projected changes can be eliminated from the analysis because they don't directly affect human cognition and decision making. Advances in areas like energy production and storage, additive manufacturing, improved precision fires, and robotics promise changes to the character of deception without bringing into question the validity of exploiting human cognition.<sup>31</sup>

Advances in genomic science can also be eliminated despite the field's potential for enhancing human cognition. This is because scientists have made very little progress in determining what genes influence human intelligence.<sup>32</sup> The largest study of its kind in 2014 revealed three genetic variants related to intelligence, but their total contribution was "maddeningly small."<sup>33</sup> Unlike genomic science targeting physical health, the science of human intelligence is unlikely to make significant strides by 2035 because of the enormous complexity associated with understanding human reasoning.<sup>34</sup>

However, there are two projected changes in ST&E that will directly affect human cognition and decision making, and both are related to information. Broadly speaking, two interrelated changes—the proliferation of connected sensors and the advancement of artificial intelligence (AI)—will change the volume and velocity of data used to derive intelligence estimates as well as the level of predictive analysis supporting decision makers by 2035. This is supported by two independent projections of the FOE, one by the US Army and the other by the British Ministry of Defence, as well as by the 2016 Marine Corps Operating Concept, all of which stress the centrality of information as it relates to future war.<sup>35</sup>

Technologies such as micro satellites, persistent Intelligence Surveillance and Reconnaissance (ISR) platforms, new electromagnetic spectrum sensors, nanosensors, and the embedding of sensors into more existing technologies will exponentially increase the types and quantity of data collected, making it increasingly difficult to hide human and equipment signatures.<sup>36</sup> When combined with the projected improvements in AI, these advances will offer a more complete understanding of the battlespace, allowing commanders to make more informed—and therefore arguably better—decisions about warfighting.

These advancements will radically enhance the capability and effectiveness of two technologies that are already robust. Regarding networked sensors, one source estimates there will be over 75 billion Internet of Things connected devices—virtually all of which will possess sensors—by 2025, up from 23 billion in 2018.<sup>37</sup> The likely increase by 2035 will be staggering. Regarding AI, consider that in April 2018, Chinese police, augmented by AI-powered glasses conducting real-time facial recognition, were able to accurately identify a wanted criminal in a crowd of 60,000 at a concert.<sup>38</sup>

Potential breakthroughs in quantum computing would radically enhance these two capabilities, providing revolutionary advances in sensor capabilities and AI processing power.<sup>39</sup> For example, quantum computing would allow AI to break existing encryption algorithms, potentially offering ULTRA-like insights into adversary decision making and feedback regarding how well a deception operation is working.<sup>40</sup> However, it is also important to note that any increased reliance on sensors and AI brings with it a corresponding vulnerability, a point that will be revisited later.

Though the forecasts for how advanced these technologies will become varies by source, even the most conservative estimates raise two issues regarding the effectiveness of deception in future war: the inability to hide forces and equipment, and the ability of AI to offset or overcome human cognition biases. With respect to the former, additional and more capable sensors will increase transparency. However, when considering the historical deception examples provided earlier, concealment was only a meaningful consideration for Chinese deception and, to a lesser extent, Egypt's deception against Israel, and arguably both would have been successful without it.

For Marshal Peng, moving 300,000 CPV troops to Korea in secret prevented MacArthur from accurately understanding the size of the force opposing UNC troops. In that regard, Peng was successful, as four days prior to CPV forces crossing the Yalu River, MacArthur briefed President Truman that the strength of CPV forces was estimated at 100,000 men along the river.<sup>41</sup> However, convinced of China's unwillingness to fight and bolstered by a belief in the superiority of UNC forces, even the presence of 100,000 troops did nothing to change MacArthur's decision making. It is questionable whether MacArthur would have acted differently even if his intelligence had been accurate; he was self-deceived.

Turning to the Ramadan War, the Egyptians were able to secretly obtain advanced weaponry. Egyptian troops also successfully moved bridging equipment to the Suez Canal under the cover of troop mobilizations. In a future war, while actions like these would be more difficult to achieve in secret, it is unlikely they will be impossible. This is because, as the web of sensors grows, so too will investment in countermeasures, including the ability to corrupt, spoof, or misdirect sensors. Furthermore, despite ample additional intelligence indicating an impending Egyptian attack, Israeli leaders failed to properly analyze Egyptian intentions. Taken together, having tools that construct a more accurate picture of adversary dispositions does not eliminate the possibility of deception.

Regarding the ability of AI to offset or overcome human cognition biases, the analysis reaches a similar conclusion. First, it is unlikely that humans will ever remove themselves completely from decision-making at the operational level of war. Though AI can make faster and arguably more rational decisions than a human, AI will remain vulnerable to physical and informational attacks. This threat, and the potential consequences of compromised AI, creates a trust issue that cannot easily be resolved. Therefore, while significant portions of decision-making may be relinquished to AI, humans will remain in the decision loop and therefore vulnerable to the exploitation of their cognition biases.

Second, although AI could reduce the probability of successfully exploiting human cognition by predicting their likelihood at the individual decision-maker level and offering warnings or even preventing certain types of decisions from being made, both AI algorithms and the data they use remain vulnerable to manipulation from cyberspace. Counter-AI could conduct sophisticated alterations of sensor data to produce misleading AI outputs or create malware that slightly alters AI algorithms to provide inaccurate predictions to human decision makers or cause

AI to make faulty decisions. In this way, data or algorithms could be altered to suggest an adversary would attack at a location slightly dislocated from the actual attack location (like Normandy), that an adversary is unlikely to attack (like the Ramadan War of 1973), or that an adversary's forces are smaller than they are (like the First and Second CPV Offensives). Interestingly, this vulnerability exists even if humans are removed from decision-making. In either case, deception will still be possible in future war.

## **RECOMMENDATIONS**

This conclusion—that the nature of deception exploits human cognition biases and FOE technologies poised to reduce or eliminate those biases are themselves vulnerable to manipulation—should inform US military thinking going forward, as it demonstrates the utility of deception during conflict *and* great power competition. This conclusion's importance is magnified by the sheer number of cognition biases available to deception planners—more than 50 by most experts' count.<sup>42</sup> Commanders at all levels should pause to consider how nearly 25 years as the world's sole superpower has affected the intellectual rigor that the US military has devoted to deception as well as its prioritization in campaign planning. Based on that sobering assessment, it becomes worthwhile to consider how the art of deception can be reinvigorated at the operational level of war. This reinvigoration must focus on deterrence and inducement during competition while also recognizing that the ability to achieve surprise will be increasingly critical to achieving military objectives and minimizing casualties in times of conflict. To that end, five recommendations follow.

First, there must be a recognition of the impact that American culture has on deception. There is significant evidence supporting the claim that individualistic cultures like the US view deception as more disreputable and immoral than collectivist cultures like China.<sup>43</sup> This has

been complemented by research showing that more interdependent cultures are more likely to engage in deception and less likely to perceive it as deceptive.<sup>44</sup> In short, Chinese culture is predisposed to view deception as acceptable and necessary, whereas US culture does not.

The roots of this cultural predisposition come from American exceptionalism, a controversial term defined by Dr. Robert Patman as an “informal ideology that endows Americans with a pervasive faith in the uniqueness, immutability and superiority of the country's founding liberal principles.”<sup>45</sup> This definition notes the cultural underpinnings, tying it to the country's founding on Christian beliefs. The resulting US system of government relies on truth and morality as a primary means of maintaining the trust and confidence of the American people and as an instrument for advancing US public and foreign policy.

This isn't meant to suggest that US culture is wrong or should be changed; rather, it illustrates the advantages China has in creating effective deceptions as a collectivist culture with a more centralized political system. In a globally connected world, effective deception planning often requires consistency of signaling across numerous sources of information that adversaries can access and assess —creating a challenge for military commanders seeking to integrate deception into a broader whole of government strategy that advances and protects US national interests. This does not mean that US military members are incapable of effective deception planning. It does suggest, however, that US culture makes it inherently harder to do well. Arguably, that should inform the level of US commander engagement in the deception planning process and the resources applied to it, which serves as a foundation for subsequent recommendations.

Second, the current US joint staff organizational construct lacks adequate capability and capacity to conduct effective large-scale deception on behalf of joint force commanders (JFCs).

Joint Publication 3-0, *Joint Operations*, states that today's "military environment and the threats it presents are increasingly transregional, multidomain, and multifunctional (TMM) in nature."<sup>46</sup> Planning staffs should therefore be organized to create similarly complex TMM deception efforts. This implies a staff robust enough to coordinate planning with the Joint Staff, combatant commands, and other appropriate organizations; with dedicated expertise representative of all warfighting domains and functions; and able to integrate deception operations across great power competition and conflict, with an ability to do *both* simultaneously.

Yet according to Joint Publication 3-13.4, *Military Deception*, military deception is normally planned by an *element* of the J-3 operations staff organized under the IO cell.<sup>47</sup> This is not a robust model and impedes a JFC's ability to effectively craft and integrate operational level deceptions during great power competition that might deter or induce adversaries in place of the US military's eroding technological edge. Should competition fail, this planning element is even more insufficient based on the need to simultaneously conduct deception planning for conflict with a specific adversary, and deception planning for competition based on a security environment with enduring TMM threats. As the necessity for operational deception increases, so too must the capability and capacity of JFC deception planning staffs. The Air Force's recent establishment of an IO career field and technical training school are helpful steps toward meeting this need, but more efforts across the joint force are necessary.<sup>48</sup>

Third, it is important to highlight how critical intelligence support is to deception planning. Creating an effective deception begins with understanding an adversary's goals and objectives and then mapping their decision-making process. This includes understanding the adversary decision-making structure, assessing biases and preconceptions, and understanding how a specific decision maker receives and uses information. Only then can planners begin to

understanding how an adversary might be vulnerable to deception. For example, intelligence might reveal that an adversary receives information primarily from a small group of trusted advisors. If intelligence further reveals that the adversary's decision-making structure makes it very difficult to target them directly, deception planners might instead focus on exploiting an advisor. Obtaining this level of insight requires appropriate resourcing and warrants consideration of whether the joint force has adequately funded appropriate intelligence collection assets and created robust enough connections to existing intelligence resources within the US government, allies, and partners.

Fourth, Professional Military Education across all the services at the intermediate and senior levels should be directed to better incorporate the study of deception, especially at the operational level of war. Rather than start a contentious debate about what to subtract from existing curricula to incorporate a greater focus on deception, look to integrate deception as a thread that weaves itself throughout the major components of the curriculum. This educational undercurrent should strive to include non-Western as well as Western examples, emphasizing Chinese and Russian deception practices. Another practical step would be to revise professional reading lists to focus on human cognition biases, cultural dispositions toward deception, and past examples of successful deception by US and non-US forces.<sup>49</sup> Yet another step would be to encourage writing about deception, especially for professional journals and essay contests. These changes would encourage greater insight into human cognition biases and influences on cultural decision making, key enablers for successful deception and counter-deception operations.

Fifth, considering how drastically the proliferation of sensors and AI will impact the creation of information and disinformation used by decision-makers at all levels across all types

of organizations, the Joint Staff should advocate for the reestablishment of the United States Information Agency or encourage organizational change within the National Security Council to coordinate a whole-of-government approach to the employment of and protection against networked sensors and AI. While the former approach would require Congressional support, the latter requires only executive branch support. A construct proposed by Richard Davenport called the Joint Influence Warfare Element (JIWE), though designed for coordinating strategic influence campaigns, could be adapted to focus on the role of information in creating deception.<sup>50</sup> When necessary, this organization would help coordinate strategic deception or necessary inputs to support a military deception operation. Global interconnectedness demands a more coordinated and synchronized approach to constructing successful deceptions at either the operational or strategic level, and an organization like JIWE would facilitate this.

## **CONCLUSION**

In closing, this paper offers an argument supporting the need for and feasibility of conducting large-scale deceptions in future war. By comparing three historical examples of operational deception using a CIA deception framework, three commonalities emerged, and it was shown that the exploitation of human cognitive biases is the key linkage between all three. Next, forecast changes to the FOE affecting human cognition and decision making were evaluated to understand how they will affect the creation of an effective deception. It was argued that while hiding forces and equipment from an adversary will become harder, it will not become impossible nor is it a prerequisite for creating a successful deception. Furthermore, it was argued that because humans will never remove themselves completely from decision making, human cognition biases will still be targetable. Additionally, it was shown that AI itself or the humans it supports can be successfully misled. Finally, having established the viability of

conducting deception in future war, five recommendations were made for reinvigorating the US military's consideration of deception.

It has been argued that the most important sentence in the 2018 NDS was “America’s military has no preordained right to victory on the battlefield.”<sup>51</sup> This was because it injected humility into conversations about US national defense and highlighted a cognitive bias toward self-deception based on a tendency to promote optimistic projections.<sup>52</sup> Reinvigorating the US military’s consideration of operational deception starts from a place of humility. History has proven the value of deception time and again and this paper has demonstrated its enduring relevance to future war. Deception offers a proven and strong mitigation to the US military’s diminishing technological superiority during great power competition.

## Bibliography

Albert, John. "A New Model Army: The Impact of Human Genome Editing on U.S. Army Manning." Working paper. USMC School of Advanced Warfighting, 2019. Microsoft Word file.

Bean, James W., and Craig S. Girard. "Anwar Al-Sadat's Grand Strategy in the Yom Kippur War." Course 5601/5602 "Long Paper", National War College, 2001. Defense Technical Information Center. <https://apps.dtic.mil/dtic/tr/fulltext/u2/a442407.pdf>.

Babb, Joseph G.D. "Chinese Deception and the 1950 Intervention in the Korean War." In *The Tangled Web: Military Deception in Large-Scale Combat Operations*. Edited by Christopher M. Rein, 155-173. Fort Leavenworth, KS: Army University Press, 2018.

Barno, David and Nora Bensahel. "Jim Mattis Fires a Clear Warning Shot." *War on the Rocks*, March 20, 2018. <https://warontherocks.com/2018/03/jim-mattis-fires-a-clear-warning-shot/>.

Breuer, William B. *Hoodwinking Hitler: The Normandy Deception*. Westport, Conn.: Praeger, 1993.

Central Intelligence Agency Office of Research and Development. *Deception Maxims: Fact and Folklore*. Washington, D.C.: Central Intelligence Agency, June 1981. [https://www.governmentattic.org/18docs/CIAdeceptionMaximsFactFolklore\\_1980.pdf](https://www.governmentattic.org/18docs/CIAdeceptionMaximsFactFolklore_1980.pdf)

Cohen, Eliot A. *The Chinese Intervention in Korea, 1950*. Central Intelligence Agency, 1988. <https://www.cia.gov/library/readingroom/docs/1988-11-01.pdf>.

Columbus, Louis. "2017 Roundup of Internet of Things Forecasts." *Forbes*. December 2017. <https://www.forbes.com/sites/louiscolombus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#385b0a2c1480>.

Davenport, Richard B. "The Need for an Innovative Joint Psychological Warfare Force Structure." *Joint Forces Quarterly*, no. 88 (1<sup>st</sup> Quarter 2018): 64-69. [http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-88/jfq-88\\_64-69\\_Davenport.pdf?ver=2018-01-09-102342-083](http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-88/jfq-88_64-69_Davenport.pdf?ver=2018-01-09-102342-083).

Dehuai, Peng. *Memoirs of a Chinese Marshal: The Autobiographical Notes of Peng Dehuai (1898-1974)*. Translated by Zheng Longpu. Beijing, China: Foreign Languages Press, 1984.

El-Sawah, Ossama M. "Deception in Ramadan War, October 1973." Master's thesis, US Army War College, 1999. Defense Technical Information Center. <http://www.dtic.mil/dtic/tr/fulltext/u2/a382499.pdf>.

Gerwehr, Scott, and Russell W. Glenn. *The Art of Darkness: Deception and Urban Operations*. Santa Monica, CA: RAND Corporation, 2000. [https://www.rand.org/content/dam/rand/pubs/monograph\\_reports/MR1132/MR1132.chap3.pdf](https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1132/MR1132.chap3.pdf)

Gompert, David C., Astrid Stuth Cevallos, and Cristina L. Garafola. *War with China: Thinking Through the Unthinkable*. Santa Monica, CA: RAND Corporation, 2016.  
[https://www.rand.org/pubs/research\\_reports/RR1140.html](https://www.rand.org/pubs/research_reports/RR1140.html).

Gordon, Brian J. *Deception in Covert Nuclear Weapons Development: A Framework to Identify, Analyze, and Mitigate Future Long-Term Deception Efforts*. Santa Monica, CA: RAND Corporation, 2016. [https://www.rand.org/pubs/rgs\\_dissertations/RGSD370.html](https://www.rand.org/pubs/rgs_dissertations/RGSD370.html).

Grohe, Edwin J. "Military Deception: Transparency in the Information Age." Master's thesis, Naval War College, 2007. Defense Technical Information Center.  
<http://www.dtic.mil/dtic/tr/fulltext/u2/a476500.pdf>.

Handel, Michael I. *Perception, deception, and surprise: the case of the Yom Kippur War*. Hebrew University, Jerusalem, 1976.

Handel, Michael I. "The Yom Kippur War and the Inevitability of Surprise." *International Studies Quarterly* 21, no. 3 (September 1977): 461-502. <https://www.jstor.org/stable/2600234>

Headquarters US Army Training and Doctrine Command. *The Operational Environment and the Changing Character of Future War*. Fort Eustis, VA, 2017.  
[http://www.arcic.army.mil/App\\_Documents/The-Operational-Environment-and-the-Changing-Character-of-Future-Warfare.pdf](http://www.arcic.army.mil/App_Documents/The-Operational-Environment-and-the-Changing-Character-of-Future-Warfare.pdf).

Headquarters US Marine Corps. *The Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*. Washington, D.C., September 2016.

Headquarters US Marine Corps. *Warfighting*. MCDP 1. Washington, DC: Headquarters US Marine Corps, June, 20, 1997.

Hesketh, Roger Fleetwood. *Fortitude: the D-Day Deception Campaign*. Woodstock, N.Y.: Overlook Press, 2000.

Interagency Task Force in Fulfillment of Executive Order 13806. *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*. Washington, D.C.: Department of Defense, September 2018.

Joint Chiefs of Staff. *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World*. Washington, D.C.: Joint Chiefs of Staff, 2016.  
[http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe\\_2035\\_july16.pdf?ver=2017-12-28-162059-917](http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917).

Joint Chiefs of Staff. *Joint Operations*. Joint Publication 3-0. Washington, D.C.: Joint Chiefs of Staff, 17 January 2017 Incorporating Change 1, 22 October 2018.  
<http://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/>.

Joint Chiefs of Staff. *Military Deception*. Joint Publication 3-13.4. Washington, D.C.: Joint Chiefs of Staff, 14 February 2017. <http://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/>.

Kim, Dr. Min-Sun, Karadeen Y. Kam, William F. Sharkey, and Theodore M. Singelis. "Deception: Moral Transgression or Social Necessity?: Cultural-Relativity of Deception Motivations and Perceptions of Deceptive Communication." *Journal of International and Intercultural Communication* 1, no. 1 (February 2008): 23-50, <https://doi.org/10.1080/17513050701621228>.

King, Iain. "What do Cognitive Biases Mean for Deterrence." *The Strategy Bridge*, February 12, 2019. <https://thestrategybridge.org/the-bridge/2019/2/12/what-do-cognitive-biases-mean-for-deterrence>.

Mlodinow, Leonard. *Elastic: Flexible Thinking in a Time of Change*. New York: Pantheon Books, 2018.

Murphy, Michael, Jr. "Chinese Principles of Operational Deception." Master's thesis, Naval War College, 2006. Defense Technical Information Center. <http://www.dtic.mil/dtic/tr/fulltext/u2/a463530.pdf>.

Pangelinan, James G. "From Red Cliffs to Chosin: The Chinese Way of War." Master's thesis, School of Advanced Military Studies, 2010. Defense Technical Information Center. <http://www.dtic.mil/dtic/tr/fulltext/u2/a523450.pdf>.

Patman, Robert G. "Globalisation, the New US Exceptionalism and the War on Terror." *Third World Quarterly* 27, no. 6 (2006): 964, <http://www.jstor.org/stable/4017735>.

Riedel, Bruce. "Enigma: The anatomy of Israel's intelligence failure almost 45 years ago." *Brookings Institute*. September 25, 2017, <https://www.brookings.edu/research/enigma-the-anatomy-of-israels-intelligence-failure-almost-45-years-ago/>.

Ryan, Mark A., David M. Finkelstein, and Michael A. McDevitt, ed. *Chinese Warfighting: The PLA Experience Since 1949*. Armonk, NY, 2003.

Stanley, Zell. *An Annotated Bibliography of the Open Literature on Deception*. RAND Corporation, December 1985. <http://www.dtic.mil/dtic/tr/fulltext/u2/a164785.pdf>.

Starry, Michael D. "Deception and the Operational Level of War." Master's thesis, School of Advanced Military Studies, 1986. Defense Technical Information Center. <http://www.dtic.mil/dtic/tr/fulltext/u2/a184731.pdf>.

Tavoy, Tal. "From Maneuvers to War: The Egyptian Deception Plan on the Eve of the Yom-Kippur War." In *The Tangled Web: Military Deception in Large-Scale Combat Operations*. Edited by Christopher M. Rein, 175-191. Fort Leavenworth, KS: Army University Press, 2018.

United Kingdom Ministry of Defence. *Global Strategic Trends: The Future Starts Today (Sixth Edition)*. London, England: United Kingdom Ministry of Defence, 2018. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/760099/20181121-GST\\_The\\_Future\\_Starts\\_Today.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/760099/20181121-GST_The_Future_Starts_Today.pdf).

US Army Training and Doctrine Command. *The Operational Environment, 2035-2050: The Emerging Character of Warfare*. Fort Eustis, VA: US Army Training and Doctrine Command, 2018. <https://community.apan.org/wg/tradoc-g2/mad-scientist/m/articles-of-interest/217736#>

US Department of Defense. *The National Defense Strategy of the United States*. Arlington, VA: Department of Defense, 2018. <https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

Vandepier, Charles. “Self-Deception and the ‘Conspiracy of Optimism.’” *War on the Rocks*, January 31, 2019. <https://warontherocks.com/2019/01/self-deception-and-the-conspiracy-of-optimism/>.

Vego, Milan. “On Military Creativity.” *Joint Force Quarterly*, no. 70 (3rd Quarter 2013): 83-90. [https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-70/JFQ-70\\_83-90\\_Vego.pdf](https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-70/JFQ-70_83-90_Vego.pdf).

Wang, Amy B. “A Suspect Tried to Blend in with 60,000 Concertgoers. China’s Facial-Recognition Cameras Caught Him.” *Washington Post*, April 13, 2018. [https://www.washingtonpost.com/news/worldviews/wp/2018/04/13/china-crime-facial-recognition-cameras-catch-suspect-at-concert-with-60000-people/?utm\\_term=.32b609c9495b](https://www.washingtonpost.com/news/worldviews/wp/2018/04/13/china-crime-facial-recognition-cameras-catch-suspect-at-concert-with-60000-people/?utm_term=.32b609c9495b).

Whaley, Barton. *Stratagem: Deception and Surprise in War*. Boston, Mass.: Artech House, 2007.

---

<sup>1</sup> Barton Whaley, *Stratagem: Surprise and Deception in Warfare* (Norwood, MA: Artech House, 2007), 102-103.

<sup>2</sup> Headquarters US Marine Corps, *Warfighting*, MCDP 1 (Washington, DC: Headquarters US Marine Corps, June, 20, 1997), 42-44.

<sup>3</sup> National Defense Strategy of the United States, January 2018, 4,

<https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

<sup>4</sup> Interagency Task Force in Fulfillment of Executive Order 13806, “Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States,” September 2018, 19-20.

<sup>5</sup> Central Intelligence Agency Office of Research and Development paper, *Deception Maxims: Fact and Folklore*, June 1981, Abstract and 4, [https://www.governmentattic.org/18docs/CIAdeceptionMaximsFactFolklore\\_1980.pdf](https://www.governmentattic.org/18docs/CIAdeceptionMaximsFactFolklore_1980.pdf).

<sup>6</sup> *Ibid.*, Abstract, 5-41.

<sup>7</sup> United States Military Academy’s Department of History, *World War II European Theater Atlases, Allied Invasion Force and German Dispositions, 6 June 1944*,

<https://www.westpoint.edu/history/SiteAssets/SitePages/World%20War%20II%20Europe/WWIIEurope54.gif>.

<sup>8</sup> William B. Breuer, *Hoodwinking Hitler: The Normandy Deception* (Westport, CT: Praeger Publishers, 1993), 101.

<sup>9</sup> Roger F. Hesketh, *Fortitude: The D-Day Deception Campaign*, 351, 388.

<sup>10</sup> *Ibid.*, 41.

<sup>11</sup> *Ibid.*, 227-240.

<sup>12</sup> *Ibid.*, 5.

<sup>13</sup> *Ibid.*, 10.

<sup>14</sup> *Ibid.*, 22.

<sup>15</sup> *Ibid.*, 27.

<sup>16</sup> *Ibid.*, 34.

- 
- <sup>17</sup> James W. Bean and Craig S. Girard, “Anwar Al-Sadat’s Grand Strategy in the Yom Kippur War” (Course 5601/5602 “Long Paper”, National War College, 2001), 2, Defense Technical Information Center, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a442407.pdf>.
- <sup>18</sup> Bruce Riedel, “Enigma: The anatomy of Israel’s intelligence failure almost 45 years ago,” *Brookings Institute*, September 25, 2017, <https://www.brookings.edu/research/enigma-the-anatomy-of-israels-intelligence-failure-almost-45-years-ago/>.
- <sup>19</sup> Bruce Riedel, “Enigma: The anatomy of Israel’s intelligence failure almost 45 years ago.”
- <sup>20</sup> Christopher M. Rein, ed., *Weaving the Tangled Web: Military Deception in Large-Scale Combat Operations*, 181.
- <sup>21</sup> James W. Bean and Craig S. Girard, “Anwar Al-Sadat’s Grand Strategy in the Yom Kippur War” 11, 14.
- <sup>22</sup> *Ibid.*, 17.
- <sup>23</sup> Sanaa’ Farouk, “Architect of the October War,” *Watani Online Newspaper*, <http://en.wataninet.com/news-2/occasions/october-war/architect-of-the-october-war/21487/>.
- <sup>24</sup> Gammal Hammad, “Military Battles on the Egyptian Front,” published by Dār al-Shurūq, Egypt and accessed at Wikipedia, <https://commons.wikimedia.org/wiki/File:Egyptianbridge.jpg>.
- <sup>25</sup> James G. Pangelinan, “From Red Cliffs to Chosin: The Chinese Way of War” (master’s thesis, School of Advanced Military Studies, 2010), 66, Defense Technical Information Center, <http://www.dtic.mil/dtic/tr/fulltext/u2/a523450.pdf>.
- <sup>26</sup> Peng Dehuai, *Memoirs of a Chinese Marshal: The Autobiographical Notes of Peng Dehuai (1898-1974)*, trans. Zheng Longpu (Beijing, China: Foreign Languages Press, 1984), 476.
- <sup>27</sup> United States Military Academy’s Department of History, *The Korean War Atlases, North Korea, UN Advance to the Yalu River and Initial Chinese Counterattack, Situation 26 October 1950 and Operations Since 7 October*, <https://www.westpoint.edu/history/SiteAssets/SitePages/Korean%20War/Korea13.gif>.
- <sup>28</sup> Central Intelligence Agency paper, *Deception Maxims: Fact and Folklore*, 15.
- <sup>29</sup> US Joint Chiefs of Staff, *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World*, JOE 2035 (Washington, DC: US Joint Chiefs of Staff, 14 July 2016), 4, [http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe\\_2035\\_july16.pdf?ver=2017-12-28-162059-917](http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917).
- <sup>30</sup> US Joint Chiefs of Staff, *Joint Operating Environment 2035*, 5-13.
- <sup>31</sup> US Joint Chiefs of Staff, *Joint Operating Environment 2035*, 15-19.
- <sup>32</sup> National Institutes of Health, “Is Intelligence Determined by Genetics” (Washington, DC: US National Library of Medicine, 18 December 2018), <https://ghr.nlm.nih.gov/primer/traits/intelligence>.
- <sup>33</sup> Ewen Callaway, “Smart Genes Prove Elusive,” *Nature International Journal of Science* (2018): <https://www.nature.com/news/smart-genes-prove-elusive-1.15858>.
- <sup>34</sup> National Institutes of Health, “The Human Genome Project Completion: Frequently Asked Questions” (Washington, DC: National Human Genome Research Institute, 30 October 2010), <https://www.genome.gov/11006943/>; John Albert, “A New Model Army: The Impact of Human Genome Editing on U.S. Army Manning,” (working paper, USMC School of Advanced Warfighting, 2019), 11-12. Microsoft Word file.
- <sup>35</sup> US Army Training and Doctrine Command, *The Operational Environment, 2035-2050: The Emerging Character of Warfare* (Fort Eustis, VA: US Army Training and Doctrine Command, 2018), 10-11, <https://community.apan.org/wg/tradoc-g2/mad-scientist/m/articles-of-interest/217736#>; United Kingdom Ministry of Defence, *Global Strategic Trends: The Future Starts Today (Sixth Edition)*, (London, England: United Kingdom Ministry of Defence, 2018), 11, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/760099/20181121-GST\\_The\\_Future\\_Starts\\_Today.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/760099/20181121-GST_The_Future_Starts_Today.pdf); Headquarters US Marine Corps, *The Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century* (Washington, DC: Headquarters US Marine Corps, 2016), 6, <https://apps.dtic.mil/dtic/tr/fulltext/u2/1039982.pdf>.
- <sup>36</sup> US Joint Chiefs of Staff, *Joint Operating Environment 2035*, 17-19.
- <sup>37</sup> Louis Columbus, “2017 Roundup of Internet of Things Forecasts,” *Forbes*, December 10, 2017, <https://www.forbes.com/sites/louiscolombus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#385b0a2c1480>.
- <sup>38</sup> Amy B. Wang, “A Suspect Tried to Blend in with 60,000 Concertgoers. China’s Facial-Recognition Cameras Caught Him,” *Washington Post*, April 13, 2018, [https://www.washingtonpost.com/news/worldviews/wp/2018/04/13/china-crime-facial-recognition-cameras-catch-suspect-at-concert-with-60000-people/?utm\\_term=.32b609c9495b](https://www.washingtonpost.com/news/worldviews/wp/2018/04/13/china-crime-facial-recognition-cameras-catch-suspect-at-concert-with-60000-people/?utm_term=.32b609c9495b).
- <sup>39</sup> US Joint Chiefs of Staff, *Joint Operating Environment 2035*, 18-19.
- <sup>40</sup> US Joint Chiefs of Staff, *Joint Operating Environment 2035*, 18-19.

- 
- <sup>41</sup> Christopher M. Rein, ed., *Weaving the Tangled Web: Military Deception in Large-Scale Combat Operations*, 162.
- <sup>42</sup> Iain King, "What do Cognitive Biases Mean for Deterrence," *The Strategy Bridge*, February 12, 2019, <https://thestrategybridge.org/the-bridge/2019/2/12/what-do-cognitive-biases-mean-for-deterrence>.
- <sup>43</sup> Dr Min-Sun Kim et al., "Deception: Moral Transgression or Social Necessity?: Cultural-Relativity of Deception Motivations and Perceptions of Deceptive Communication," *Journal of International and Intercultural Communication*, 1, no. 1 (February 2008): 25, <https://doi.org/10.1080/17513050701621228>. This insight comes from the article's literature review, and relies heavily on behavioral research conducted by Takie Sugiyama Lebra in her 1976 book titled, *Japanese Patterns of Behavior*.
- <sup>44</sup> Dr Min-Sun Kim et al., "Deception: Moral Transgression or Social Necessity?: Cultural-Relativity of Deception Motivations and Perceptions of Deceptive Communication," 23-50.
- <sup>45</sup> Robert G. Patman, "Globalisation, the New US Exceptionalism and the War on Terror," *Third World Quarterly* 27, no. 6 (2006): 964, <http://www.jstor.org/stable/4017735>.
- <sup>46</sup> US Joint Chiefs of Staff, *Joint Operations*, Joint Publication (JP) 3-0, Change 1 (Washington, DC: US Joint Chiefs of Staff, 17 January 2017 Incorporating Change 1 22 October 2018), I-2, [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_0ch1.pdf?ver=2018-11-27-160457-910](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910).
- <sup>47</sup> US Joint Chiefs of Staff, *Military Deception*, Joint Publication (JP) 3-13.4 (Washington, DC: US Joint Chiefs of Staff, 14 February 2017), III-1-III-6, <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/>.
- <sup>48</sup> Secretary of the Air Force Public Affairs, "AF Officials Announce Creation of Info Ops Tech School," March 5, 2018, <https://www.hill.af.mil/News/Article-Display/Article/1457978/af-officials-announce-creation-of-info-ops-tech-school/>.
- <sup>49</sup> For further study on the role of cognitive and cultural biases during the Arab-Israeli Ramadan War of 1973, for example, see Leonard Mlodinow, *Elastic: Flexible Thinking in a Time of Change*, (NYC, NY: Pantheon Books, 2018), 161-166.
- <sup>50</sup> Richard B Davenport, "The Need for an Innovative Joint Psychological Warfare Force Structure," *Joint Forces Quarterly*, no. 88 (1<sup>st</sup> Quarter 2018): 64-69, [http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-88/jfq-88\\_64-69\\_Davenport.pdf?ver=2018-01-09-102342-083](http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-88/jfq-88_64-69_Davenport.pdf?ver=2018-01-09-102342-083).
- <sup>51</sup> David Barno and Nora Bensahel, "Jim Mattis Fires a Clear Warning Shot," *War on the Rocks*, March 20, 2018, <https://warontherocks.com/2018/03/jim-mattis-fires-a-clear-warning-shot/>.
- <sup>52</sup> Charles Vandeeper, "Self-Deception and the 'Conspiracy of Optimism,'" *War on the Rocks*, January 31, 2019, <https://warontherocks.com/2019/01/self-deception-and-the-conspiracy-of-optimism/>.