2021

Strategic Culture and Cyber Strategy

Andrew S. Olejarski
University of Central Florida

STRATEGIC CULTURE AND CYBER STRATEGY

by

ANDREW S. OLEJARSKI

A thesis submitted in partial fulfillment of the requirements

for the Honors in the Major Program in Political Science

in the College of Sciences

and in the Burnett Honors College

at the University of Central Florida

Orlando, Florida

Spring 2021

Thesis Chair: Ted Reynolds, Ph.D.

ABSTRACT

The intent of this paper is to explore the relationship between strategic culture theory and how it interacts with war-parallel usage of cyber methods. Cyber methods, at times incorrectly classified as “cyberwarfare”, as a means of statecraft are becoming increasingly prevalent, and developing an understanding of how states use them, particularly during conflicts, would be a great boon to the field of security studies. Strategic culture theory, an international relations theory focusing on the relationship between culture and strategy, may be an effective means to analyze conflict-parallel use of cyber methods. This paper will consider the relationship between strategic culture and cyber strategy, and develop a model through which to analyze it.

ACKNOWLEDGEMENTS

Thanks to my committee members, Dr. Reynolds and Dr. Dolan, for their invaluable guidance and incredible patience.

Thanks to my friends, family, and loved ones for support along the way.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE: INTRODUCTION

This paper seeks to analyze a state's development of cyberstrategy through the scope of strategic culture theory. Cyber actions taken by states, in the modern world, are becoming increasingly prevalent and significant. Due to the unique properties of cyber methods, and being a new form of statecraft and exerting influence, it presents a complex problem for political science and security studies. Discerning an effective way to study cyber activity would be a great boon for the discipline, and strategic culture theory may be an effective way to do so. Strategic culture theory seeks to explain strategic choice using a culture's values and attitudes toward strategy. The term "strategic culture" was first coined by Jack Snyder in *The Soviet Strategic Culture: Implications for Limited Nuclear Options* in 1977, in the midst of the Cold War. In this paper, he supposed that the American and Soviet modes of thinking differed, and that manifested itself in their strategy - in this case, nuclear strategy. He specifically described strategic culture as the "sum total of ideals, conditional emotional responses, and patterns of habitual behaviour that members of the national strategic community have acquired through instruction or imitation and share with each other with regard to [...] strategy"[1]. More simply: the manifestation of a state's culture on its strategic thinking. Snyder's report was a departure from the typically realist strategic thinking at the time, which was a welcome perspective. When dealing with such a complex and vital subject, analysts and policymakers should assess foreign strategy not by

objective standards, but by a constructivist model of foreign decision-makers that considers the culture and history from which they came. Strategic culture theory and its application is merely an expansion of that constructivism.

While the report was written for the Cold War era, the concepts it introduced persist in international relations theory. Like nuclear strategy, cyber strategy is a novel form of interaction between states, with little comprehensive history to cover, and as such requires careful theory to fully evaluate. This thesis suggests that, in the absence of extensive historical outcome to rely on, strategic culture theory offers a viable alternative to approximating how a nation will act in scenarios of cyber interaction. The development of cyber technologies greatly expanded a state's means of exerting strategic influence internationally, and so its relationship with a state's strategic culture may be an important indicator of choice.

Cyber interaction is essentially any method performed by a state on another state using computers or information technology. Cyber warfare is a commonly used term, but this may be a misnomer. Quite often cyber attacks can occur without any loss of life, merely property, data, or finances. However, their commonly non-violent nature does not diminish their strategic significance.

After a thorough assessment of strategic culture literature, the methodology of the paper will be addressed, including independent and dependent variables and their values, as well as a hypothesis, based on strategic culture theory. Then, three case studies will be analyzed using this

methodology. Finally, the paper will conclude by considering the results of the analysis and notable conclusions drawn during the process.

Strategic Culture Theory

Snyder's report and the framework it proposed were novel, but rudimentary. Since its advent, other scholars expanded upon it through the 1980s and onward, retrospectively being delineated into three different generations of strategic culture theory. The first generation was pioneered in the 1980s, by scholars such as Colin Gray or David Jones. These scholars expanded upon Snyder's idea with more rigorous academic care. Gray described the effects of a nation's historical experience being strategic culture, or "modes of thought and action with respect to force" that led to "dominant [strategic] national beliefs". Jones outlined three inputs to strategic culture being a macro-environmental level, geography and history, societal level, social structures, and micro level, military institutions and civil-military relations[2]. The first generation specified the concepts introduced by Snyder and made efforts to establish some methodological principles. However, the initial writings on strategic culture proved to have major issues. The definition of strategic culture was broad and poorly delineated, including a massive amount of cultural and societal variables. As Iain Alistair Johnson, a later scholar, criticized of first-generation work, "if strategic culture is said to be the product of nearly all relevant explanatory variables, then there is little conceptual space for a non-strategic culture explanation of strategic choice"[3]. In defining strategic culture in such vague terms, there left little room for consistency across scholarly works on strategic culture, as any variable vaguely relating to

culture or society could be analyzed in its effect on strategic choice, even incredibly broad generalizations of culture. Moreover, the first generation also considered behavior to be a *part* of culture, creating crossover between dependent and independent variables. This caused strategic culture theory to be self-affirming by definition, and rendered it difficult to appropriately test.

The second generation of strategic culture theory began in the late 1980s, and addressed the incongruence between states' operational and declaratory strategies, considering the differences between leaders' publicly stated motivations for actions and their "real" motivations. The orientations of strategic culture "undergird a declaratory strategy that legitimizes the authority of those in charge of strategic decision-making. Operational strategy, on the other hand, reflects the specific interests of these decision makers."[4]. Simply, the strategic culture influences a state's declaratory strategy, which is merely a justification or interpretation (or, in cases, a falsehood) of a state's operational strategy. Many second generation scholars suppose that state strategic behavior, or its operational strategy, derives from "hegemonistic groups", whereas its "official" stated strategy, or declaratory strategy, derives from the strategic culture, in an effort to "fashion a culturally and linguistically acceptable justification for operational strategy, and to silence or mislead potential political challengers" - appease the global or domestic theater. One scholar, Bradley Klein, doubted the influence of political and military influence on strategic culture, focusing on the power of historical experience in determining strategic culture. He supposed that the difference across states' strategic cultures is derived from the difference across their historical experiences[5]. While some second generation scholars believed strategic culture

has little or no effect on behavior, as "decision-making elites can rise above strategic cultural constraints", others found it possible that those elites, too, are subject to the strategic culture of a state, having been socialized within it and thus *their* behavior is beholden to it in the same way that first-generation scholars suppose a state's behavior is. Thus, there was no consensus within the second generation of strategic culture theory on the degree to which it affects state behavior.

The third generation of strategic culture theory affirmed a belief that strategic culture influences behavior, pulling back from second generation doubts. It became stricter in its definition of independent variables, narrowing the field of study from the vague concept of "strategic culture" as a whole into variables such as politico-military culture or organizational culture. Typically, the independent variables of the third generation forewent the historical focus of the other generations, emphasizing more recent experience. Additionally, it narrowed the dependent variable from a broad assessment of behavior into more specific strategic choices. The third generation's strength over the first two methodologically is its use of competitive theory testing, or "pitting alternative explanations against each other". Scholars such as Jeffrey Legro or Elizabeth Kier test different explanations in their models, and thus emerge with a stronger strategic culture theory[6]. While the third generation does demonstrate strengths over the other two, it is not fully refined. Its definition of culture exhibits the same issue of breadth, despite its narrowing. Nor does it fully address the questions raised by the second generation about the incongruence between declaratory and operational strategy.

Iain Alistair Johnson, in his 1995 article *Thinking About Strategic Culture*, critiques the state of strategic culture theory for overwhelmingly relying on the methodology and ideas of the first generation literature. He outlines his reconceptualization of strategic culture theory. Johnson sets out to define strategic culture in a way distinct from non-strategic cultural variables. He lands on defining strategic culture as "a system of symbols which acts to establish pervasive and long-lasting strategic preferences by formulating concepts of the role and efficacy of military force in interstate political affairs, and by clothing these conceptions with such an aura of factuality that the strategic preferences seem uniquely realistic and efficacious". He describes the "system of symbols" as being a combination of basic assumptions about the orderliness of the strategic environment - the role of war in human affairs (inevitable or aberration?), the nature of the adversary and threat (zero-sum or variable sum?), and the efficacy of the use of force (effective and to what degree?) - and operational assumptions and preferences (defense or offense?) that flow from the theoretical assumptions - i.e. principle of mutually assured destruction flowing from the idea of nuclear war being a negative sum threat[7].

Johnston graphically displays these spectra of variables, and defines the determinant spectrum as being between "hard realpolitik" and "soft idealpolitik", a state's place between the two being determined by what their variables' values are.

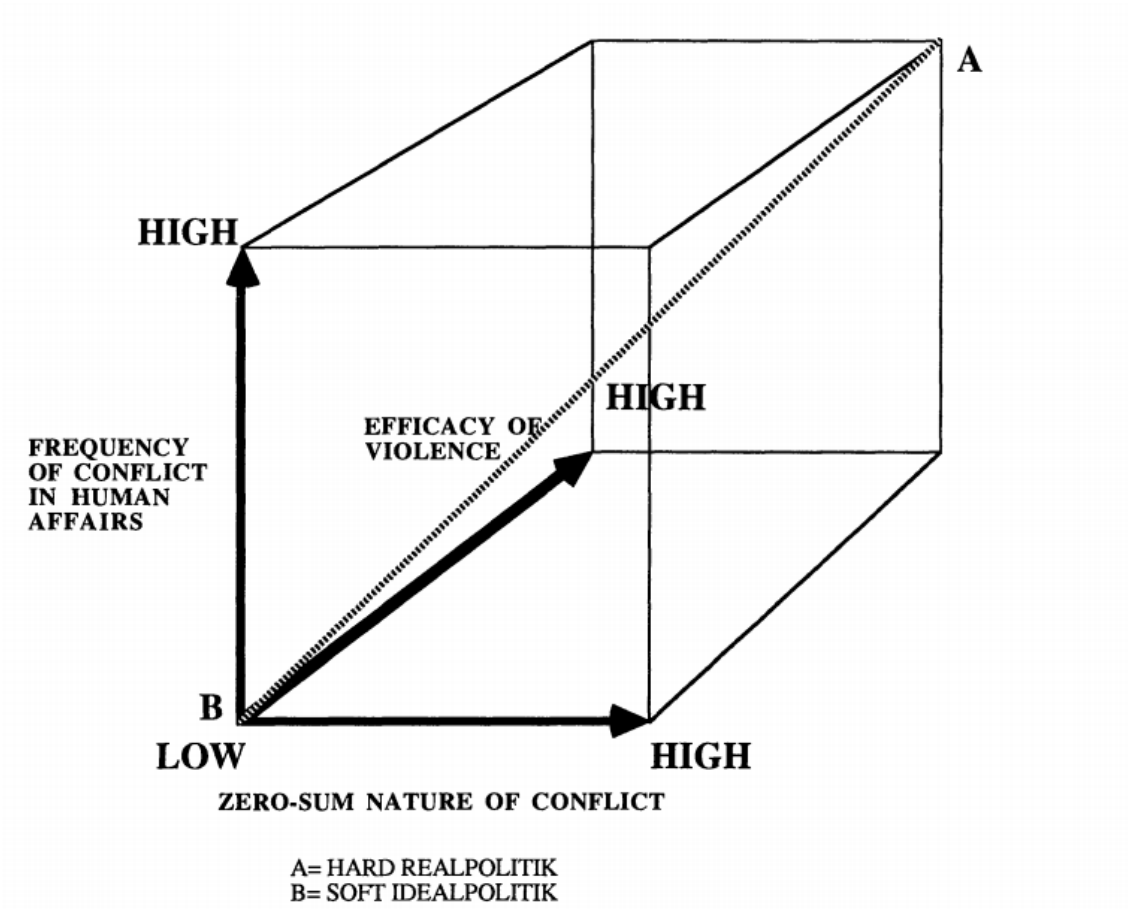

Figure 1: Johnston's visualized analytical model[8]

———In determining where on these assumption spectrums a given strategic culture lies, one must identify and analyze objects of analysis. These could vary widely - the declarations of strategists or politicians, weapon designs, technological focus, images of war in media, or general public opinion on these assumptions could be objects of analysis. Johnson suggests that by comparing objects of analysis across periods of time, one can identify the persistence of strategic culture across a nation's history.

Colin Gray struck back at Iain Alistair Johnson's criticisms of the first generation theorists in his 1999 article *Strategic Culture as Context: The First Generation of Theory Strikes Back,* using theory he had developed in his book *Modern Strategy*. There, while he recognizes the flaws of the first generation, he expands upon his ideas and criticizes Johnson's attempts to separate culture from behavior. Gray sates that "the traffic between ideas and behavior in strategic affairs is continuous, hence my preference for the idea that context is more about 'that which weaves together' than it is about 'that which it surrounds'". Gray supposes that strategic culture is inseparable from strategic experience, or a state's past strategic behavior. Additionally, Gray disagrees with Johnson that strategic culture is moreso beholden to more recent experience than it is long-standing historical experience or ideals[9].

Where he agrees with Johnston is the point that any given security community may have several strategic cultures, and may comprise "more a litany of canonical idealised beliefs than a set of attitude, perspectives, and preferences that are operational as real guides to action". He also acknowledges the validity of Johnston's criticism that the breadth of formative strategic culture was too much.

In regards to Johnston's criticism on the "lack of methodological rigor" in strategic culture theory beforehand, Gray only offers concession, stating that "it is in the nature of strategy to be subject to a paradoxical logic" and that "strategic culture … is a useful notion provided one does not ask too much of it". Gray retreats to the notion that strategic culture can only offer

"context, not reliable causality". He outlines six general points regarding the nature of strategic culture:

1. Strategic behavior cannot be beyond culture - claims of strategic culture do not imply that all decision-makers are in ubiquitous agreement.
2. Adversity cannot cancel culture - "the grimmer the national circumstance, the less scope for exercising strategic cultural preferences". However, with less decision time, strategic behavior will fall to strategic cultural preferences.
3. Strategic culture is a guide to action - while "adverse strategic necessity can subvert," strategic culture "has to be a guide to action"
4. Strategic culture expresses comparative advantage - in those situations where states are forced to act in situations they are disadvantaged, they will act poorly.
5. Strategic culture can be dysfunctional - strategic cultures are not necessarily consistently advantageous attitudes
6. Strategic cultures can be variously categorized

In his 6th point, Gray outlines what he considers to be beliefs and behavior that constitute a state's strategic culture. These are: nationality, geography, weapons and functions, simplicity-complexity of strategic approach, generation, and grand strategy[10].

The Debates of Strategic Culture

Over nearly four decades, scholarship on strategic culture theory is still deeply divided on many issues, the division primarily manifesting in the Johnston-Gray debate. Rather than restrictively prescribe itself to one school of thought, this paper will examine the points of contention, consider both arguments, and develop a perspective on each one.

Context vs. Causality

A highlight of the Johnston-Gray debate is whether to, in analyses, approach strategic culture from a sense of causality with respect to strategic choice, or as a context to understand it. Causality is the approach that should be taken, as it both demands methodological rigor and has stronger meaning.

Recent vs. Ancient Historical Experience

There is some debate on the relative focus on ancient historical experience. Some strategic culture theorists would suppose that a strategic culture needs to be firmly grounded in history both recent and ancient, but this paper disagrees. After all, strategic culture, while a function of traditions and older philosophies, is more a function of the people themselves. The thought of the people defines a strategic culture, and in turn, a strategic culture informs the thought of the people. And the people at hand are only a product of at most, approximately, the past 100 years. While certainly ancient teachings on strategic thought persist, textbooks, curricula, and cultural attitudes change across generations. It is the opinion of this paper that

objects of analysis of more recency hold greater strength to a strategic culture, if it can demonstrate a strong consistency across that recent period of time.

The Role of Behavior

The role of behavior is one of the biggest points of contention in the Johnston-Gray debate. Johnston warns of the "tautological traps" of considering behavior a determiner of strategic culture, and strategic culture a determiner of behavior. Gray strikes back, stating that strategic culture and behavior are inherently intertwined in both directions.

Certainly, Johnston's fear of the determinism caused by this relationship is valid. However, Johnston does not make the distinction between past and present or recent strategic behavior. Undoubtedly, if one were to examine strategic culture as a function of current strategic behavior, and then claim that that strategic culture causes that behavior, they would fall into the recursive trap. But strategic choice changes over time, and across situations. If behavior is a symptom of strategic culture, then surely, couldn't one use it to diagnose a strategic culture, albeit with lesser weight? To avoid Johnston's feared tautological trappings, current or recent strategic behavior should not be used as an independent variable in determining strategic culture. However, historical strategic behavior should be - just as much as any other element of history that strategic culture studies draw from. For this paper, even relatively recent strategic behavior could be used, as the examples of strategic behavior from which conclusions about strategic culture may be drawn are of a different type of strategic behavior than cyber methods.

Declaratory statements v. Reality

As second generation scholars of strategic culture theory are wont to point out, there may be a disparity between leaders' expressed beliefs and their actual beliefs. Scholars warn that while strategic culture may be reflected in the declarations of leaders, "decision-making elites can rise above strategic cultural constraints", and that because of that, strategic culture's effects on behavior are negligible. However, this notion fails to acknowledge the exact nature of those strategic cultural constraints. Quite often, "rising above" strategic cultural constraints may lead to dissent among any level of a society. A voting populace, socialized to a strategic cultural belief, may become discontent and threaten the elite's position. If a voting populace is a lesser factor, such as in states where the elections are controlled or manipulated, then there is still potential for dissent among higher ranks of society, as those elites were still socialized within a strategic culture and their decisions more beholden to it. So, while there is potential for "decision-making elites" to rise above the dictations of strategic culture, and that warrants acknowledgement and consideration on a case-by-case basis, it is not a strong enough factor to completely disregard leader statements that may have a disparity with their actual beliefs.

Objects of Analysis

The objects of analysis proposed by strategic culture scholarship in assessing a state's strategic cultural values still apply to an exploration of the variables. For the purposes of this paper, those used will be described.

Declaratory Strategy

Declaratory strategy refers to a broad span of writings and statements that come from leaders, strategists, public and government records. It is the "declared" strategy of a state - that strategy which is publicly known. However, as second generation strategic culture theorists are wont to point out, there can be disparity between the declaratory and operational (or actual) strategy of a state. In any analysis of declaratory strategy in this paper, it will make note of examples of operational strategy directly related to a given piece of declaratory strategy. Thus, any piece of declaratory strategy used for analysis will be either backed up by an instance of operational strategy, or at the very least, not contradicted by any operational strategy for the given time period. Certainly, pieces of declaratory strategy that are backed up by operational strategy are more powerful indicators of a strategic culture. But some decalaratory strategies are long-term, or cannot be backed up by operational strategy for some other reason, and are deserving of note as well. However, the strength of a piece of declaratory strategy will be addressed.

Technology

Technology is an effective object of analysis. This term will broadly refer to the collection of technologies used by state militaries as well as R&D efforts supported or undergone by their governments. One can discern a state's intention by analyzing its technological efforts. If they develop technologies to exert influence and power in novel ways, then the way in which these technologies are used can discern strategic cultural preferences.

Organizational

Organizational structures are other important factors in assessing these independent variables. The organization and groups within a government/military can discern their intent. The mere name and function of organizational-level groups could indicate a state's intended strategy, as well as their priorities. Additionally, organizational congruence is a significant factor to consider. As the classification of "actor" becomes more specific - from state, to institution, to organization, to group, to individual - it becomes easier for that actor to act unbeholden to strategic culture. For an action to be considered derivative of a strategic culture, it must be enacted with a degree of interorganizational congruence - agreement between intelligence, diplomatic, and military wings, as well as necessary approval of the particular political process. These factors will be considered in viewing a strategic culture.

Strategic Behavior

While Johnston may warn against the tautological trappings of strategic behavior existing as anything other than the dependent variable in the methodological analysis of strategic culture, other scholars disagree, as does this paper. Additionally, this paper is even further removed from the tautological trappings. While strategic behavior is at hand as an object of analysis, it differs from the strategic behavior the paper seeks to explain. The latter regards cyberstrategic behavior, whereas the majority of elements of the former will concern non-cyber-related behavior.

Existing Literature

There are many pre-existing analyses of strategic culture, for many states. Beyond the primary sources, these secondary, scholarly sources can both strengthen and expand the conclusions that this paper draws from primary sources. A great deal of thinking has been applied to the way of waging war, and there are strong works to borrow from when considering a strategic cultural attitude toward warfare.

Structure and Methodology

Often, cyber warfare does not fit into Johnston's and similar conceptions of strategic culture theory - their conceptions focus on the use of force and, by their nature, cyber methods are often devoid of force. Gray's framework of analysis - his seven variables by which one can analyze strategic culture - can fit with an examination of cyber strategy, being that they are more generic in nature and can be removed from the context of use of force. One might expect such a paper dealing with non-force analyses of strategic culture to use Gray's framework. However, there remains methodological issues with Gray's framework. His variables do not offer clean, quasi-quantitative spectrums by which to compare states' values, unlike Johnston's model. Johnston's variables can be evaluated in such a way - saying "State A is further towards X on the XY spectrum than state B" - Gray's variables cannot. The breadth of Gray's variables are also an issue. For the scope of this paper, to evaluate three case studies in the context of Gray's variables would be to not give each variable the attention it deserves.

However, that is not to diminish the value of Gray's ideas of strategic culture. His variables certainly have great strategic relevance and are essential to an exploration of a state's strategic culture. Rather than dismiss them, this paper will attempt to incorporate Gray's variables into more quantifiable spectra. Additionally, this author finds that many of Gray's variables are more useful as *objects of analysis* in analyzing some more select and quantitative variables. Geography, weapons, generation, etc. can be useful in informing one particular cultural attitude.

So, in avoidance of the constraints or flaws of Johnston's or Gray's model, a hybrid of the two will be created for the purposes of this paper and its application to cyber strategy. After all, as Colin Gray ends his critique with, "readers are recommended not to pick either this author's, or Johnston's, approach to strategic culture, but rather to move on to a creative accommodation of the two"[11]. Such a principle applies even moreso in a novel, unique application of strategic culture.

Johnston's use of multiple quasi-quantitative variables will be used as a part of this research structure. The independent variables under observation must still be inherent to strategy and warfare, but also be ingrained enough in the history of statecraft for attitudes towards them to have fully developed. Past scholarship on strategic culture theory can give valuable precedent to any analysis using strategic culture. The works of Johnston, Gray, and other scholars elucidate the details of strategic culture theory, which can inform the selection of a research's variables.

Independent Variable

On the nature of war

One factor of note is the importance of the perceived nature of war in strategic culture. All strategic culture scholarship to some degree considers a state's attitude toward the nature of war. Johnston considers a strategic culture's view of the natural frequency of war in human affairs, and other scholars are extensively concerned with war, as it has been the prevalent method by which a state exerts strategic influence. Indeed, war is inherently intertwined with a cultural mindset - as Thomas Hobbes wrote in *Leviathan*, "as the nature of foul weather lieth not in a shower or two of rain, but in an inclination thereto of many days together; so the nature of war consisteth not in actual fighting, but in the known disposition thereto during all the time there is no assurance to the contrary"[12]. While only coined in 1977, the concepts behind strategic culture theory have persisted for centuries.

A perception of the nature of war is essential to a state's usage of cyber methods as a means to exert strategic influence, as how a strategic culture views war can elucidate their view of other means of exerting strategic influence internationally. Thus, one independent variable under observation in this paper will be a strategic culture's attitude toward the nature of war. This begs further elaboration, including more definitive values for the variable.

To some degree, most strategic culture scholarship addresses attitudes towards the nature of war, as war is one of the most prevalent means to exert strategic influence. Johnston considers whether a culture views war as inevitable in human affairs. Gray tangentially considers it by

viewing a culture's weapons, grand strategy, and historical behavior (in wars). A strategic culture's attitude toward the nature of war is essential to an exploration of it.

However, despite the methodological strength of Johnston's model, the paper finds little applicability of his values of the nature of war to the topic at hand. Johnston considers whether a culture finds war to be inevitable or an aberration, and takes that into account of their strategic preference ranking. This paper addresses cyber methods - at first glance, one would not expect there to be a relationship between a state's usage of cyber methods and their cultural perspective on the inevitability of war.

So, the task comes to developing an independent variable to test that fulfills three criteria: being concerned with the nature of war, being at least seemingly related to a state's usage of cyber methods, and being reasonably quantifiable. An attitude toward the nature of war can be broad, and there are many factors at hand. Cultures' view on war could vary widely in a number of different aspects - its inevitability, its scope, the relative importance of different kinds of war, what constitutes war, the way in which it should be fought, among others. This is only exacerbated by the broadening application of the term war, to a plethora of different kinds - cold, unconventional, asymmetric, economic, political, guerilla, civil, revolutionary, psychological, information, and more. To properly identify a variable out of this extensive nature to be observed, and to clarify a central aspect of the paper, the nature of war is deserving of a literature review as well.

One of the most classic definitions of war comes from Carl von Clausewitz, renowned 1800s military theorist. He describes war as “an act of violence intended to compel our opponents to fulfill our will”. Further, he recognizes the multi-faceted nature of war and its place in political context, stating that “war is nothing but a continuation of political intercourse, with a mixture of other means”[13].

Modern society is inundated with the use of the term “war” to describe any number of non-violent or non-destructive conflicts, such as information war, psychological war, trade war, etc. But in political science, this may be a misnomer. Most political scientists adhere to the stricter definition by which war necessitates a kind of organized violence, not just strategic competition. There are different standards - one quantitative standard proposed is at least “1000 deaths” - but the presence of violence is consistent.

That said, where definition varies is the consideration of non-violent means as a part of war. How integral is having multiple facets to a war? Is war just fought on the battlefield, or is it accompanied by the many other tools of statecraft that persist during peace? In their “way of war”, states vary widely. Some use overwhelming conventional force and forego nontraditional methods. Others consider the political and psychological, or public opinion, aspects of war just as important as the kinetic battles, but more notably, they take action within those spheres as a part of a war effort.

Tactical adaptability also plays into the breadth with which a nation considers the nature of war. As the world has broadly over the latter half of the 20th century from conventional,

state-to-state warfare to dealing with increased non-state actors, civil wars, and insurgencies, states vary in their efficacy in adapting the new "way of war" that the latter conflicts necessitate. How a state deals with these conflicts - whether they consider them legitimate threats that warrant strategic and tactical reform - can be indicative of the rigidity with which they do or do not view the nature of war.

A state's consideration of the nature of war can be narrow, rigid, and inflexible, or it can be broad, adaptive, and multi-faceted. A strategic culture, to some degree, will indicate a state's view of the nature of war. There are some clear values with which to evaluate attitude towards the nature of war, but for the sake of brevity, it would be beneficial to note a single word for each end of the value. On the broad, adaptive, multi-faceted end, the paper will use "hybrid" as the term. This is a term that has found use in war studies before, and one classification is that it can "be used informally to describe the ever-changing complexity and dynamics of the battlefield" [14]. On the narrow, rigid end, the paper will use the term "conventional" - classic warfare that is predominant throughout history and concerns the simplest use of force.

The independent variable's new concern with the breadth of a state's attitude toward the nature of war fits the aforementioned criteria. It is inherently concerned with the nature of war. It is reasonably quantifiable, with two well-defined opposing ends, conventional and hybrid, on the variable's spectrum of values. One can say "this state views the nature of war as hybrid" or "this state has a conventional view of the nature of war". And finally, at face value, it seemingly concerns a state's usage of cyber methods. Cyber is a new form of technology-enabled statecraft

that can be applied in a number of situations. One would naturally expect that a state's attitude toward hybrid war could inform how well they adapt to the usage of cyber methods. Thus, an independent variable has been identified.

Dependent Variable

The dependent variable whose relationship with the independent variables is being sought is a state's strategic choice - more specifically, their strategic choices made in "cyberwarfare" or more aptly cyber strategy. This could include a variety of classifications, but for the purposes of analysis, this paper will limit itself to one quantitative variable.

The variable under observation will be "usage of offensive cyber methods parallel to conventional conflict". It is important to limit the range of observation of cyber strategy - cyber operations are incredibly broad in variety and quantity. They may include subversion, espionage, sabotage, or more. Should one consider *all* cyber operations of any given state, the data at hand would be excessive, and its quantity would be more a function of a state's organizational manpower and capability than it is a function of their strategic cultural values.

One way the scope of cyberstrategy covered is limited is by only addressing offensive, active cyber methods. Defense, generally, is broad, and from the paper's research appears more beholden to operational strategy than it is to strategic culture. After all, while the efficacy of any particular kind of cyber method can be debated, if it is recognized then certainly a state will take measures of defense. Defense is a necessity, offense is optional, and thus whether or not a state engages in offensive cyber methods, and what type, depends on its strategic culture. The term

offensive does not necessitate violence or destruction - it merely is a descriptor of a proactive action.

The term “parallel to conflict” in the dependent variable must be elaborated upon. This is the second way in which the scope of the independent variable is limited. For the purposes of this paper, defining actions as “conflict-parallel” is shorthand for denoting actions which have two characteristics: occuring in war, and being designed to affect a war’s outcome. Due to the nature of cyber methods, unrestrained by geography, there may be cyber methods that are explicitly designed to affect the outcome of a war, yet are superficially detached from that war. This could include, for example, an economic cyber attack that is retaliation for a conventional action in war, or a cyber operation designed to influence public opinion on the war. Both of these, despite not attacking the war-making military institutions of a state, can still be explicitly designed to affect a conflict’s outcome, and thus should come under consideration.

The selection of conflicts and consideration of the actors within them must also be considered. In many modern conflicts, states have strategic interests in the outcome, and yet will not have a single boot on the ground, for a plethora of reasons. As a result of this, states will often supply aid designed to affect the outcome of a conflict while not directly involving themselves, quite often to small state administrations or non-state actors. This is commonly how larger powers involve themselves in a conflict where they cannot, for whatever reason, act directly. As such, this extends the scope of how a cyber method could affect the outcome of a war. A cyber operation - performed by a state indirectly involved in a given conflict, on another

state indirectly involved in the same conflict, designed to affect the target state's involvement in the conflict, and therefore the outcome of the conflict - can thus be considered "conflict-parallel" despite being at face-value irrelevant to the conflict, because it can affect the outcome. If it occurs in the time of war, then it satisfies the two prongs of being conflict-parallel - it is occurring in war, and designed to affect the outcome of that war.

Hypothesis

After identifying independent and dependent variables, a hypothesis can be formed. The basic hypothesis of this paper is that the greater the hybrid nature of a state's attitude toward the nature of war, the greater their usage of cyber methods parallel to conventional warfare will be. The dependent variables' respective influences may vary, and that will be addressed in the findings of this paper.

The study will examine three case studies. Based on the variables, the cases selected will be states who have examples of armed conflict in the modern era and who have cyber capability. For each one, it will conduct a strategic cultural analysis of their attitude toward the nature of war, focusing on the breadth (or lack thereof) of it. Each state will then be rated qualitatively on the hybrid nature of their view of war.

While states' cyber power can vary greatly, to fully encompass both total and cyber power of a state, actors' threat levels will be generalized according to their size. The paper will use a common classification of state type in international relations coined in the 1600s by Italian diplomat Giovanni Botero in his book *The Reason of State*. He, and many other international

relations scholars, delineated states into being large, great strength and global influence, middle, primarily regional influence, or small powers, without much power relative to other kinds[15]. Additionally, to consider the relevant organizations that exert cyber influence, non-state actor will be another classification.

From there, each state's major involvement in armed conflicts since 2000 will be assessed regarding the state's usage of cyber methods parallel to that conflict. "Involvement in armed conflicts" is an important distinction - it expands the scope from conflicts where the state is a direct combatant to conflicts where their conventional contribution could be air or training or material support. This is particularly important, as proxy warfare becomes more prevalent. Should these involvements be ignored, then the paper would lose sight of such strategically essential conflicts like the Syrian civil war or Middle Eastern proxy wars. The state's cyber usage of all forms will be explored.

Finally, the state's cyber efforts across conflicts and over time will be generalized. From that conclusions will be drawn about how the state fits into the hypothesis - did a hybrid perspective of warfare lead to greater quantities of cyber usage?

The study will also make note of regional context. Many of the conventional conflicts of the 21st century take place in impoverished or underdeveloped regions. Due to this, there is less potential for the use of cyber methods, as the means to these methods may not exist or be extensive. That said, this may differ within a given combative organization - while the majority of Iraq may not have cyber infrastructure, the same may not be true for ISIS or al-Qaeda. In an

assessment of a state's cyber usage, it is essential to consider the *potential* for that usage. Otherwise, faulty conclusions may be drawn about the lack of cyber methods. The paper will examine factors of cyber usage at both regional and organizational levels, and use the findings to weigh the significance of case state cyber usage.

The final chapter, the conclusion, will address the outcome of the hypothesis and various findings of the paper. In addition to concisely summarizing the research of the paper, it will discuss the observed relationship between a state's attitude toward the nature of war and their cyberstrategy. Finally, it will address the findings' broader implications on strategic culture theory.

CHAPTER TWO: RUSSIA

Russian Strategic Culture

Hybrid nature of war

Historically, the Russians exhibit a high adaptation to instances of irregular warfare. Their defeat of Napoleon in 1812 was due, in part, to their forces, which demonstrated a mobility, flexibility, and decentralized command that was irregular to warfare at the time. During the 1840s, the Tsar at the time Nicholas I began a campaign against nomadic tribes of Central Asia. This campaign made use of novel tactics and even a primitive form of proxy warfare. During World War 2, Soviets used a form of guerilla warfare against the more centralized Nazi occupation[16]. While exhibiting great differences from modern irregular warfare, these are examples of the Russian military's treatment of warfare - it is no stranger to employing novel, irregular tactics when the need calls for it. This historical basis strengthens the strategic cultural attitude towards the efficacy of irregular conflict.

In a discussion of Russian adaptability to changing conflict, a discussion of the 1980-1989 Soviet-Afghan War is essential. The Afghan war was not an example of Russia's adaptability to novel forms of conflict - it was a failure. Much like the U.S. in Vietnam, the Soviets were not adequately prepared to deal with the guerilla tactics of the Mujahideen[17]. This presents an issue with a theoretical Russian strategic culture, and their attitude toward the nature of conflict. If the Soviets failed due to the rigid conventionality of their tactics, then does that demonstrate a rigid view of the nature of conflict? While certainly, the Soviet-Afghan War is a

significant case to consider in an examination of Russian conventionality, one needs to consider the dissolution of the USSR on Russia's cultural attitudes in an assessment of modern Russia. The reaction to the fall of the Soviet Union was tumultuous for Russian strategic culture. As previously mentioned, there was a period where Russians practically forewent it in favor of a more Western strategic culture. While they eventually returned to their traditions, it was certainly not without change. The massive failure embodied by the fall of the Soviet Union was treated as a cautionary tale for the future of Russia - and their military culture. So emerged an opinion that was fundamental to Russian strategic culture not only after their brief West-friendly period, but during it as well. There was a general consensus, after the fall of the Soviet Union, of the need for "fundamental military reform and modernization"[18]. The Russian people and government recognized the rigidity of some Soviet military strategies and their great failure prompted a strong reaction against that rigidity. That said, while the Soviet Union experienced failures tactically in irregular conflict, they successfully implemented many strategies of irregular conflict - such as their adeptness in information warfare. But hybrid warfare has two prongs, a tactical and strategic level, and even tactical failures are worth noting.

When considering the persistence of Russian strategic culture, there is one era of note. In the Yeltsin administration, from 1992-1996, there was a period where the public and the government expressed ideals antithetical to traditional Russian strategic culture - a desire to essentially join up with the West and look to them as a source of assistance. This was due to the failures and fall of the Soviet Union. However, these ideals faded towards the end of the Yeltsin

administration. For many reasons - in part the failures of the West and NATO - Russians became disillusioned with their newfound Western identity and began to regress to a more traditional Russian strategic culture[19]. The evolution of Russian strategic culture throughout the 1990s, from tentative West-friendly reformation to an emboldening alteration of traditional strategic culture, was best represented by the two Chechen wars, in 1994 and 1999. The first was under the Yeltsin administration, with more Western sentiments, and was a failure. The second was under the Putin administration, coinciding with a regression to more traditional Russian sentiments towards strategy, and was a success. There was a clear difference across the two periods' attitude toward the nature of war. The Yeltsin administration demonstrated a great failure at the hands of irregular warfare in their involvement in the First Chechen War. Not only did they fail to deal with the hybrid conflict on a tactical level, like the USSR in Afghanistan, but they failed on a strategic level. In 1994, the public sentiment was clear - Russian press was "hostile to the very fact that troops entered Chechnya". Yet in 1999, mere years later, the Russian press "showed no visible passion with regard to the civilians killed" and the war was treated as nothing out of the ordinary. As one scholar writes, "one can only be surprised at the scale and swiftness of the changes in public opinion on the Chechen war, which reflects the militarization of the public consciousness"[20]. While the difference in press opinion may have been a machination of the Putin administration, it remained a strong influence on the Russian strategic culture. From a poll by Russian Public Opinion and Market Research, in 1995 the number of "those who supported maintaining Russia's integrity by military means" was a mere third. By

2001, it raised to two-thirds. Similar polls on Chechen independence demonstrated the same trends[21]. This massive change in public opinion directly coincided with the advent of the Putin administration.

After the fact, the failure in the First Chechen War was recognized as a failure in assessing the nature of conflict and using their full extent of capabilities. The Russian government "considered their main misjudgment a failure in the information war" and then advocated "reprogramming the public consciousness as a main tool in fighting Chechen separatism"[22]. They redirected their efforts toward spreading their agenda-based information on the Chechen wars in order to inundate it into the Russian population.

The evolving Russian attitude toward the nature of war was represented in their handlings of new conflicts. The Second Chechen War began in October 1999, and Putin came to power a few months later for the entire year of 2000. By 2009 the Chechen separatist movement had all but dissolved, and any major fighting ended, resulting in a decisive Russian victory, merely dealing with low-level insurgency afterward. As previously mentioned, the Russian Federation took great care to support the Second Chechen War on every level, where the First failed. They controlled the information of the media and successfully ingratiated the Russian peoples toward Russia's campaign in Chechnya. This led to increased soldier morale, which was a large deficiency in the first war.

The Russians also utilized proxy tactics, with the recruitment of formerly anti-Russian Chechen militia leader Ramzan Kadyrov, who was later installed as the Russia-loyal head of the

Chechen Republic. The readoption of more hybrid warfare practices is in line with the readoption of a traditional Russian strategic culture, abandoning Soviet or Yeltsin-era strategic cultures.

With regards to Russia's adaptability towards conflict, the Afghan War and First Chechen War represented isolated instances of an operational disparity with the modern declaratory strategy of the Russian Federation regarding the nature of conflict. Both were failures due to Russian rigidity in waging the wars. The Afghan War was a tactical failure akin to Vietnam - unable to adapt to the guerrilla tactics of the Mujahideen - and the First Chechen War a strategic failure - failing to consider the importance of non-combat aspects in waging war. However, in part, the modern declaratory strategy was borne of the failures of these wars. The poor adaptability of the Russians in the Afghan war and First Chechen War should not be reflective of their attitude toward the nature of conflict, as it came with massive upheaval *of* that attitude. For those reasons, modern era objects of analysis after 1996 should be given greater weight, due to the fact that this is the approximate point in time where the Russian strategic culture ended its period of tumult and solidified to reach some consistency for decades - the prior one, after the dissolution of the USSR, lasted less than a decade and experienced more dissent within Russians' strategic thinking. While perhaps not an ideally sized period of time to consider persistence of a strategic culture, it still spans 25 years, and that is a significant portion of the time that unconventional warfare has become more prevalent. Additionally, as previously mentioned, there is a historic Russian basis for the use of hybrid warfare. Despite setbacks in the

latter half of the 20th century, there is a trend for Russia's positive attitude towards the use of hybrid warfare. Even though it failed in parts, the USSR too demonstrated facets of hybrid warfare, albeit on a more strategic level. The failures of the 1980s and 90s highlighted the need for change, and the Russian strategic culture demonstrably responded promptly and decisively. It would be worth considering whether the U.S. experienced the same need for change, as their failure in Vietnam did not coincide with such massive societal breakdown, and thus did not spark a more major response.

That said, while the Second Chechen War represented an improvement in terms of the strategic hybridity of warfare, particularly in the integration of information control, the tactics of the Russian army retained the conventional rigidity it displayed during the Cold War. Rather than adapt to the insurgent nature of the Chechen opposition, Russia responded with overwhelming conventional force, consisting of a massive aerial campaign[23], and extensive usage of artillery, both of which lead to great collateral damage[24]. After the bulk of the war ended, guerrilla opposition within Chechnya persisted to 2009. Russia continued to respond conventionally, with artillery and airstrike, though eventually adopting some counterinsurgency methods.

The organizational cultures within Russian organizations may account for this disparity between hybrid strategy and conventional tactics. The tactics derive from the organization actually fighting in Chechnya - the Russian Armed Forces. The personnel of the RAF, established by Yeltsin in 1992, largely carried over from the Soviet Armed Forces. Like the strategic cultural reforms pushed by Yeltsin, his Defense Minister Pavel Grachev made efforts

towards reform within the RAF, promoting the creation of a "Mobile Force" focus on rapid deployment and a more mobile fighting force, which would represent a shift towards the tactical irregularity needed to fight insurgency. Also like the pro-Western strategic cultural reforms, however, these military reforms failed, in part due to the military officials of the RAF. The General Staff of the RAF, composed of some former Soviet military officials, pushed back against this reform, reportedly believing that "for the time being the best policy was to keep as much of the structures and armaments of the good old Soviet Army alive as possible"[25]. Indeed, the rigidity of the RAF persisted - not only through Yeltsin's administration, but Putin's as well.

Russian armed forces focus on conventional power with little adaptation to insurgent conflicts let alone multi-dimensional strategy. Yet, despite this, as demonstrated in the Cold War, Chechen conflicts, and other conflicts, Russia exhibits a multi-dimensional view of warfare. This may be accounted for by intelligence and government involvement in waging war. There is a clear discrepancy in the Russian institutions that wage war or support a war effort and their strategic hybridity.

The majority of Russian hybrid war efforts come from its intelligence services - namely, the KGB and its successor the FSB. Indeed, the KGB was not only the intelligence service of Russia up to the dissolution of the Soviet Union, but was officially a military service and subject to the same kinds of regulations. This classification indicates the importance of the KGB to the Russian way of war. And from the KGB came the hybrid warfare of Russia - their intense focus on information operations and proxy support lead to the instances of Russian hybrid warfare, a

long history of subversion and proliferation accompanying the conflicts in which they are involved.

One persistent element of the Russian strategic culture is the perception of persecution from its rivals - that such a persecution is persistent and threatens the very life of Russia. A spokesperson for President Vladimir Putin in 2004 said "there is the continuous threat of an attack by the West"[26]. While such a principle may hold true in the Russian populace, and lower levels of the military, this principle is likely just a tool for Russian leaders to socialize the populace. Decades ago in 1947, American diplomat George Kennan wrote that "there is ample evidence that the stress laid in Moscow on the menace confronting Soviet society from the world outside its borders is founded not in the realities of foreign antagonism, but in the necessity of explaining away dictatorial authority at home". The same principle persists to the modern age. In 2007 several government officials expressed support of a textbook, which was rolled out to schools in 2008 - *The Modern History of Russia* - citing its necessity in the wake of "acute problems in the teaching of modern Russian history". The editor of this book later confirmed that the Putin administration and Ministry of Education had tasked him with assembling the textbook. The tenets promoted by Putin and this new textbook included the idea that Russia was a "besieged fortress", dealing with the constant threat of Western attack[27]. While it is questionable whether the Russian government officials believe in this or are merely using it as a tool for the populace is irrelevant - it exists as an aspect of strategic culture, and Russia acts accordingly to

it. The persistence of this principle across 60 years reinforces its place in the Russian strategic culture

This threat perception, as a key tenet of Russian strategic culture, is inherent to their attitude toward the nature of war. The “besieged fortress” principle presumes covert action by Russia’s enemies - considering there is not always an armed conflict going, the victimization complex must manifest itself in a different form, a form that can be unseen and remain unproven. By accusing the West of these subversive methods, Russian authorities can maintain the justification for their own all-scope form of warfare. Certainly, it is sometimes true that they are victim to Western covert action. However, the Russian government has bolstered that idea to unrealistic extent and used it as a justification for strategic choice. The natural reaction to a perceived Western multi-faceted campaign is, of course, a multi-faceted campaign of their own. Therein lies the philosophical foundation of Russia’s modern perception of war - if the West is doing it to them, then they must retaliate in the same manner.

Today, Russian strategic culture is full of declaratory strategy espousing the merits of unconventional forms of warfare. Chief of the Russian General Staff, General Valeri Gerasimov, said in 2013 that “the role of non-military means in achieving political goals, and, in many cases, they have exceeded the power of weapons in their effectiveness. The lines between war and peace have been blurred, wars are no longer declared, and after they have begun, they proceed according to an unfamiliar template”. Gerasimov also mentioned the failure in the 1980s Afghan war, where he makes note of the novel methods of military operation that were born as a

response. He goes on to compare the necessities of the Afghan war to hypothetical future conflicts with advanced technologies, and urges Russian military thinkers to reflect on the possibilities.[28]

The Military Doctrine (Russia's review of current conflicts and threats) 2014 cites some "characteristic features" of modern military conflicts. Their first feature mentioned is the complex combination of measures - military, political, economic, informational, and other measures which they cite as "implemented with the widespread use of the protest potential of the population and special operations forces". They also make mention of the use of externally financed and controlled political forces and social movements.[29]

In the book *The Russian Understanding of War: Blurring the Lines Between War and Peace*, Oscar Jonsson supposes that the advent of the information revolution changed the Russian view of the nature of war - now information warfare is "so potent that it can achieve political goals commensurate with war without recourse to military means"[30]. While certainly, the Russians have historically considered information warfare an integral part of a war effort, the information revolution expands the possibilities massively.

Russia demonstrates a clear recognition of the changing landscape of conflict - perhaps in no small part due to their standing in the world. As a revisionist power, who seeks to change the world order, unconventional means of doing so is a necessity for them. An open conflict with America or allied Western powers would spell certain doom for them, and so promoting their

agenda with one of the key tenets of gray zone warfare, “beneath the threshold of war”, is a necessity. Cyber operations are merely an effective means of doing so.

While the Russian Armed Forces lag in their adoption of hybrid warfare, they are supplemented by Russian intelligence and state efforts in war that do exhibit a hybrid nature of warfare. It is evident that Russia demonstrates a high level of recognition of the value of irregular conflict, and a high level of adaptability to the changing landscape of conflict. Thus, the Russian strategic culture will be considered as having a highly positive attitude toward the efficacy of hybrid warfare.

Russian cyber methods parallel to conflict

2008 Russo-Georgian War

Table 1: 2008 Russo-Georgian War

Allied combatants	*Enemy combatants*	*Enemy actor type*
Russia	Georgia	Small state

This was perhaps the first explicit incident of “cyber war” that the world has seen. Although the actual operations within it may not be the image that term provokes, nonetheless, it was the first war to use cyber methods in parallel with conventional warfare, and ushered in a new, poorly understood threat to global politics.

Russia launched DDOS attacks on 38 Georgian and Western websites, including several government and financial websites. These attacks took place over the course of two months, over

two major periods - July 18th and August 8th - August 11th. The first set of attacks focused on the Georgian president's website, overloading it and taking it down for 24 hours. This was weeks before the conflict began on August 1st. The second set of attacks were much broader in extent.

The attacks served primarily to assault information in Georgia. News sites were attacked and much of Georgian internet traffic rerouted to servers in Russia or Turkey, then blocked or diverted. News sites were taken down via DDOS attacks, or spoofed with fake news sites. The President's site was defaced again with images of Hitler.[31]

Attribution of these attacks is a point of dispute. A few aspects are clear - the attacks had knowledge of Russia's military movements, given that they began before conflict officially began and ended in concurrence with the ceasefire, and the large part of them were coordinated by some centralized command, given that the attacks all began and ended within 30 mins of each other. Many attribute the attacks to the Russian crime network, Russian Business Network (RBN), a notorious purveyor of cyber crime[32]. Given the extreme coordination of the attack, it is highly likely there was some direct collaboration between RBN and some facet of the Russian government or military.

It is evident that these attacks had some particular intentions - discourage open dissemination of information to or from the Georgian public, and set the stage for an international political image of Russia in this conflict. The closing of communication lines left the world in the dark when it came to the Georgian crisis and its context, while Russia was free

to give their illustration of the conflict. At the end of the war, Russia occupied the formerly Georgian Abkhazia and South Ossetia, and does to this day.

While the idea of DDOS attacks and disinformation and political posturing may seem like mere harassment, almost an afterthought to conventional war, the cyber campaign of the Russo-Georgian War had great implications for the war effort. The first actual Russian military intervention began on August 8th, the same time as the media cyberattacks and the occupation of internet servers, indicating there may have been a high degree of collaboration between conventional and cyber efforts.

Suppressing media coverage of the war and Georgian international internet communication served some key purposes. In doing so, Russia prevented themselves from being portrayed as the aggressive actor in the conflict. They also downplayed the severity of the conflict. In fact, knowledge of the conflict was reduced to claims made by the leaders of the two countries - for example, a New York Times article from August 9th, 2008 includes only claims made by each government, and said "each side's figures were impossible to confirm independently"[33]. The EU was adamant that both Russia and Georgia were to blame for escalation of the conflict.

The disinformation purported by this cyber campaign clouded international knowledge of the conflict, and by doing so, may have postponed any preventative action by NATO. The Russian campaign in Georgia was quick and decisive. Without consistent reporting, and only conflicting statements from leaders to follow, the war retained a certain degree of ambiguity that

may have served to prevent foreign intervention. This may have been vital for Russia - should another country have so much as moved forces toward the Georgian border, Russia may have hit its aggression limit and been forced to withdraw rather than attack a NATO member and initiate full-scale war. The Russo-Georgian War is of incredible significance - not only is it the first "cyber war", it is an example of the incredible strategic use of cyber operations parallel to conventional warfare.

The extensive usage of cyber methods is also notable when considering the small portion of Georgian citizens who used the internet at the time. In 2008, at the time of the attack, the percentage of population who used the internet in Georgia was a mere 10%[34]. While this may seem a small portion for an informational attack on the domestic population, its effects may have been exponential. While the overall population's internet usage is low, it was likely higher for Georgian bloggers, reporters, and news networks. Any misinformation fed through those avenues could have disseminated via the media to a broader part of the population via non-cyber means like TV or radio, fostering Russia's information campaign.

2014 Russo-Ukrainian War

Table 2: 2014 Russo-Ukrainian War

Allied combatants	*Actor type*	*Enemy combatants*	*Actor type*
Russia	Large state	Ukraine	Middle state

While Russia's war on Georgia was the first instance of full-fledged cyber warfare, it was fledgling compared to their campaign on Ukraine. What precedent was set by the Georgian war was only bolstered 6 years later in 2014, when Russia engaged in new, unconventional cyber methods to parallel their conventional war efforts. In November 2014, Russia moved troops into separatist areas of eastern Ukraine, attempting to claim territory.

Leading up to the war, German cybersecurity expert Volker Kozok noticed signs indicating what was to come. In January 2014, Kozok and his colleagues noticed that Russia was installing an undersea cable in the nearby Strait of Kerch, and concluded that its endpoint was Crimea, suggesting Russia planned to connect to Ukrainian critical infrastructure that could provide internet communications, bypassing Ukrainian service providers. According to Kozok, "it was the first time a country had organized a military attack while also being very smart about planning for connectivity with a sea cable"[35].

In May, months after the start of the war, CyberBerkut, a pro-Russian hacking group, days prior to the election destroyed key vote tallying files and leaked information from Ukraine's Central Election Commission, using similar software to Russia's APT28 group. This led to the delayed release of the election results. The government website was also set to be compromised, before defense was made, to display a far-right fringe candidate with less than 1% of the vote as the winner. Given the ongoing military conflict between Russia and Ukraine, this was likely an attempt to destabilize the electoral process and thus administrative capabilities of the Ukrainian government, as well as foster confusion in the Ukrainian people.

Russia made use of telecommunicative psychological operations in their conflict with Ukraine, from 2014 to 2017. They sent texts to numbers of Ukrainian soldiers' cell phones, ranging from deceptive - claiming to be commanders giving orders - or aggressive - sending threatening messages. According to *Associated Press*, this was facilitated by cell site simulators, which could impersonate cell phone towers and consequently intercept or fake data. In 2016, Ukrainian group InformNapalm published imagery showing a LEER-3, a Russian electronic warfare system mounted on a truck, in the Donetsk area, as well as leaked documents about its deployment to Luhansk. Russian Military Review magazine says that the LEER-3 has a cell site simulator built into a drone capable of acting over a 6 km wide area and hijacking up to 2,000 cell phone connections at once, which indicates that this is the source of spoofed texts sent in Ukraine[36].

CrowdStrike, a cybersecurity company that has investigated several major cyber incidents, analyzed a major physical cyberattack performed by Russia on Ukraine. The end consequence of this attack was the destruction of a large portion of Ukrainian artillery. Reported estimates vary and claimed numbers have changed over time. In summer 2016, CrowdStrike analysts began investigating an Android package, or APK (a file used for the distribution and installation of apps on Android systems), entitled Попр-Д30.apk. This translates to "Popr-D30.apk" - the latter part of which indicates reference to the Soviet artillery weapon D-30 122m towed howitzer, still used today. CrowdStrike's analysis revealed that the APK contained a variant of X-Agent. This deduction was based on certain similarities between the code and a

known Windows version of X-Agent - their command and control protocols, and a cryptographic algorithm called RC4[37].

Despite its eventual use, the origins of the app, at least in its initial form, were Ukrainian. The filename Попр-Д30.apk is shared with a legitimate application by a Ukrainian app developer, 55th Artillery Brigade officer Yaroslav Sherstuk, who developed the app "sometime between 20 February and 13 April 2013". Its intended purpose, as reported by Sherstuk himself, was to reduce the fire time of the D-30 from minutes to seconds. Sherstuk promoted this app on a Russian social networking site named VKontakte. Despite sharing it on a Russian media site, it seems unlikely Sherstuk intended for this app to be utilized by the Russian military. Rather, it is more likely that he merely used VKontakte as a quick and effective way to distribute it to other Ukrainian soldiers, not expecting the covert repurpose of this app. This tactic was evidently effective - in media interviews, the developer claimed its usage by about 9000 artillery personnel. Sherstuk also put in a safety against free usage of this app - the program was only activated for use after he was contacted and issued a code to the downloader. At the time, Russo-Ukrainian relations were also more cooperative, so there may have been less hesitation on his part about proliferating it through Russian sites.

After its development and proliferation on VKontakte, it is likely the app came to the attention of Russian officials due to their surveillance of VKontakte communications. The app was then taken, rewritten to include malicious code, then redistributed through alternate means. On 21 December 2014, the malicious variant of Popr-D30 was observed by CrowdStrike on a

Russian language Ukrainian military forum. CrowdStrike Intelligence has “assessed that the distribution of the malicious application targeted [brigades operating in eastern Ukraine]”. They suggest the sabotaged app version has the ability to map out a unit’s “composition and hierarchy, determine their plans, and even triangulate their approximate location”. Concisely, the X-Agent infected Popr-D30 was not intended for destructive purposes, rather reconnaissance[38].

Despite the general sense of restraint when it comes to energy infrastructure cyberattacks on Russia’s larger enemies, lesser rivals of Russia have been subject to actual energy attacks, most prominently used in their Ukrainian campaign. On December 23rd, 2015, there were disruptions of up to 27 distribution stations and 3 power plants in western Ukraine. The government blames Russia for these outages. In an investigation using internal and friendly international support, assessments have determined that components used to damage computers were previously used by Russian groups. They also cite the relative cyber capability of Russia.

Several security companies’ analyses point to the Russian state-affiliated group Sandworm. iSight, a security company, was monitoring Sandworm up to a year prior, and discovered the group has collected “information from the computers of Ukrainian administration officials, and from agencies in the EU and NATO”. Security company ESET reported that the attackers used a backdoor software that allows operations on target computers from a remote control server. In Ukraine, a BlackEnergy component - a Trojan horse that was developed in 2014 - was used to spy on Ukraine admin computers and plant the malware program KillDisk on power station computers[39].

A release from the Ukrainian Ministry of Energy detailed the claims made by their investigation into the attacks. They claimed that the initial infection of information networks was at least 6 months prior to the attacks, in the summer of 2015. This was done via social engineering methods - fake emails, or "spearphishing", intended to trick employees into downloading the malicious BlackEnergy virus bootloader. 3 energy suppliers were attacked - Prykarpattya Oblenegro, Chernivtsi Oblenegro, and Kiev Oblenegro. One of these suppliers claims the attackers connected to its information networks from the internet[40]

Whereas the Russo-Georgian war's cyber operations had exclusively grander strategic implications, the Russo-Ukrainian war included cyber operations which were more tactical in nature, focusing on ground-level troops and manipulating the defensive campaign. These cyber methods were undertaken in addition to more strategically focused one, such as the election interference, which was an attempt to destabilize the Ukrainian government and foster confusion and dissent among the people.

Given the relevance of cyber methods to conventional movements this time, it is worthwhile to examine cyber usage in a more regional sense. The Russian conventional campaign focused on Crimea and eastern Ukraine, and so did their cyber focus. The dispersal of VKontakte on a Russian language Ukrainian military forum betrayed their intentions - their targeted regions were primarily Russian speaking.

Syrian Civil War

Table 3: Syrian civil war, Russia

Allied combatants/supporters	*Actor type*	*Enemy combatants/supporters*	*Actor type*
Assad regime	Small state	Syrian opposition groups	Non-state
Russia	Large state	United States	Large state
Iran	Middle state	France	Large state
Syrian Electronic Army	Non-state	United Kingdom	Large state

The Russian involvement in Syria, beginning in 2015, is distinct from its campaigns in Georgia or Ukraine. Russia merely supports the Assad regime and provides them with minor conventional assistance. Russian support primarily is in the form of materiel - supplying equipment, air support, and training to Assad's forces.

While their direct intervention in the war is small, their strategic interest in it is anything but. The U.S. sought to defeat ISIS, who was a player in the Syrian war, and was disapproving of the Assad regime. One of the primary Russian interests in the Syrian conflict is the prevention of U.S. military presence in the region. In that, Russia also has interests in defeating ISIS presence in the region, taking away a reason for the Americans to be there. The major powers on both sides, for their own reasons, are reluctant to escalate their respective military presences. So, Russia seeks its strategic goals through methods even more unconventional than those used in

Georgia or Ukraine - including election interference, misinformation, and espionage, as well as direct and indirect support to the Assad regime.

Russia has undertaken a number of cyber operations that directly support the Assad administration in the Syrian war. These operations include "action in cyberspace [that] consists of propaganda and espionage campaigns focused on gathering information on anti-government groups and NGOs, with spying malware being delivered by spear phishing emails and fake websites with malicious links"[41].

A representative from cybersecurity company Imperva said that "Russia was very involved in setting up the Syrian signals intelligence system and it is possible they still have access to Russian expertise and even experts", citing the success of "fake online Facebook profiles, SSL certificates, and other methods to break into the opposition"[42]. The Syrian Electronic Army is a loosely united group of cyberactors that engages in the Syrian war. Any official link to the Syrian government is lacking, but some argue that it acts as a proxy group for Assad and is more or less directed by Syria. Assad even personally thanked the SEA for their actions in a speech[43]. One study found "two degrees of separation" between the SEA and a senior politician of the Assad regime, concluding that there was a relationship "close enough to ensure the strategic alignment of the SEA. There was notable improvement of the SEA's techniques over the course of the war, which some suggest indicates assistance from the more sophisticated Iran or Russia[44]. Opposition activists claim that Assad's cousin Rami Makhlouf funds the SEA,

citing a defected SEA member. They also claim that it "receives sporadic technical assistance from Russia"[45].

Cyber experts also claim SEA may be state-supported. Kenneth Geers suggests that SEA is an APT (advanced persistent threat); due to the duration and gravity of their attacks, they may have direct or indirect support of a nation state, and that the U.S. should be concerned about Russian hackers training the Syrian Electronic Army[46].

Unfortunately, despite ponderings by scholars and cybersecurity experts, there is nothing conclusive linking Russia and the Syrian Electronic Army. Should the rumors of Russian support prove true, it is still merely, as one rumor described it, "sporadic". Thus, it could not be conclusively said that Russia offered cyber support to the SEA during the Syrian civil war.

In addition to direct support to the Assad regime, Russia sought to discredit U.S. legitimacy in the region and drive them out. Russia used propaganda and information campaigns to further this interest. The most famous example of this is the Russian interference in the 2016 U.S. presidential election. A 2017 report on Russia's interference in the 2016 U.S. presidential election was prepared by the American intelligence community. In it, they stated: "Moscow's influence campaign followed a messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by the Russian Government agencies, state owned media, third party intermediaries, and paid social media users"[47]. For their relations with America, this interference was perhaps the most prominent example of Russian cyber strategy at work. To exert political influence through the use of information technologies is the

finest example of the non-violent threat cyber capabilities can pose - to upend the political processes of strategically critical rivals without firing a single bullet.

While subject to political debate, among the American intelligence community there is unanimous agreement that "Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election"[48]. This campaign was not only an effort to promote the presidential campaign of Donald Trump, but in a more general sense, to sow discord within the American public, spread disinformation, and promote division. This campaign was entirely enabled by cyber methods, particularly via social media.

A number of inflammatory emails from the Democratic Party were leaked after a hack on their servers. These emails served to discredit the party and undermine their trustworthiness and incite conflict within the party between its base and the more progressive wing, as much of the emails contained derogatory comments about Clinton's more progressive primary rival, Bernie Sanders. These emails were released on the site WikiLeaks. U.S. intelligence and several cybersecurity firms found it highly likely Russia was responsible for the attack. An internet hacking persona with the moniker "Guccifer 2.0" took credit for the leaks. Guccifer, in an interview, alleged himself to be Romanian with "no strong political leanings", however there was no evidence offered as to his identity. The U.S. intelligence community in their report on interference in the 2016 election stated it was "highly likely" that Guccifer 2.0 was a persona created by Russian intelligence[49]. There are some facts indicating this - such as his inability to speak in the Romanian language fluently and his source being a Russian-language VPN. Given

the strategic timing of this release, and these other factors, it is very likely that the persona was fabricated by Russian intelligence in an attempt to absolve themselves of blame, or at the very least, retain plausible deniability.

Beyond a broader strategic goal, the 2016 U.S. election had a direct influence on the Syrian war. While certainly not the only reason Russia undertook this cyber operation, their interests in Syria may have been a strong factor. It was widely understood that the two candidates, Donald Trump and Hillary Clinton, would have very different approaches to the Syrian conflict. The traditional U.S. preference for Assad to step down was supported by Clinton and disparaged by Trump. In October 2016, Trump said "Assad is secondary, to me, to ISIS" and purported the idea that the election of Clinton would "lead to World War Three" because of her potential for conflict with Russia. Clinton supported the establishment of no-fly zones and safe zones on the ground in Syria, which some feared would create confrontation between U.S. and Russian forces[50]. Trump's declared preference in Syria was in direct accordance with the Russian preferences - for the U.S. to leave Assad alone and focus only on ISIS, a shared enemy. Given that, the influence on the Syrian civil war was clearly one of the motives for the 2016 Russian cyber operation, and their efforts towards the election of Trump. Although Trump later changed his stance on Assad, the Russians were concerned with his campaign promises.

The Western allies most heavily involved in the Syrian conflict were the U.S., France, and the U.K., and these were also the states subject to Russian cyber influence over the latter half of the 2010s.

In 2017, a leak of hacked emails occurred that were akin to America's DNC leak in 2016. These were known as the "Macron leaks", attempting to discredit and harm the campaign of French presidential candidate Emmanuel Macron. Like Clinton, Macron was critical of Assad and suggested the potential for France to take further action against him. Macron criticized Assad's possible use of chemical weapons in 2017, shortly before the election, and stated that his preference was that "there should be an intervention under the auspices of the United Nations. A military intervention" - a UN-led intervention which had previously been vetoed by Russia[51]. Macron's primary opponent, Marine Le Pen, espoused views more in line with Russian interests, stating that Assad was "the most reassuring solution for France"[52].

This was ultimately an unsuccessful influence operation, demonstrating no palpable influence on the election. Jean-Baptiste Vilmer of CSIS compares it to the success of the U.S. election influence, citing a number of key points - the coordinated government defense against misinformation, a unified media, and the imprecision of Russian tactics[53]. The imprecise tactics cited are that misinformation and anti-Macron sentiment was primarily spread via English language channels. Given that, there is a possibility that an ulterior or perhaps the primary motive of the Russian bots was to further influence American domestic politics. The report cites that it was spread through common English "alt-right" sources, which is another source of polarization for American politics. This may discern Putin's goals as being less the prevention of French intervention, but moreso the prevention of American-French collaboration. Putin said in a discussion with Macron that "he wasn't sure if France's Syria policy was 'independent' because

it was part of a U.S.-lead alliance". This may indicate that Russia is more concerned with the collaboration of Western powers in Syria than France itself.

The third major instance of Russian cyber operation was its influence campaign in the U.K. concerning Brexit. Where the Americans produced a comprehensive government report, the British did not - a report from their parliamentary intelligence committee states that "the written evidence provided to us appeared to suggest HMG [Her Majesty's Government] had not seen or sought evidence of successful interference in UK democratic processes"[54]. Despite the British government's reluctance to investigate, the issue has been covered by other research. Russian language bots were identified to have executed social media campaigns amplifying pro-Brexit rhetoric. These bots originated from the Internet Research Agency (IRA), the same group who supported interference in the 2016 U.S. election. On the very day of the Brexit vote, the UK Energy Network was targeted and the British referendum "may have been hacked". The respective influences of these actions is not known, but the result of the vote was close, with only 1.89% above a majority for leaving the EU[55].

That said, Brexit appeared to have no large effect on the British activity in the Syrian war, neither for nor against Russian interests. The motives behind Brexit interference are unclear, but likely irrelevant to the Syrian war. However, given Russian interference efforts in France, the similarities between Trump and Le Pen regarding Syria, it appears likely that Russia's Middle Eastern interests was a significant motive in their election interference campaign.

While some may question the influence of the Syrian war on Russia's reasons for U.S. and French election interference, the idea may be backed up by other Russian cyber-disinformation campaigns that were more explicitly related to Syria.

One report details the extent of Russian social media disinformation, often purported by bots, stating that it has reached an "estimated 56 million people with tweets attacking Syria's search and rescue organization, the Syria Civil Defense". The Syria Civil Defense, also known as the White Helmets, is known for saving Syrian lives and providing essential evidence of Assad war crimes to international organizations. This had the aim of undermining the SCD as well as "promoting false information about the sarin chemical attack of April 2017. The Russian disinformation efforts concerning the Syrian war are pervasive at all levels of their government - from both Russian media RT all the way down to bot farms[56].

In April 2018, following a U.S. bombing of suspected Assad chemical weapon sites, a Pentagon representative reported a "2,000% increase in Russian trolls in the last 24 hours". While one digital forensics group disagrees with the magnitude, they do note an increase in bot disinformation activities, as well as crossover between Russian and Iranian narratives on the U.S. airstrikes[57].

These represent Russian cyber-enabled information operations that are more explicitly linked to the Syrian war, as opposed to the more indirect link of their instances of election interference. Regardless, it is clear that Russia engages in social media disinformation operations in order to affect the outcome of the Syrian civil war.

Syria's cyber infrastructure, ruined by years of war, was lacking, and thus its potential for being utilized in cyber attacks is also lacking. A notable distinction between Syria and Russia's other cyber-wars is that more tactical cyber attacks were limited in quantity in the Syrian war. Some suggest that the reason for this is an MAD-esque fear of retaliation - in a conflict with such major cyber powers, tactical cyberattacks may be restrained for fear of retaliation by the powerful adversaries[58]. However, it may also just be a product of Russia's limited military presence in the region. This raises the question of if tactical cyber-wars can truly be fought from anywhere.

Conclusions

Russia fits into the hypothesis posed - with a strategic culture disposed to have a highly positive attitude towards the efficacy of hybrid warfare, the hypothesis would imply an extensive usage of offensive cyber methods to supplement conventional wars. In this case, the hypothesis proves true, based on the large amount of Russian cyber operations that appear to be, at least in part, part of a war effort. While lacking in relative cyber power, a notable observation of Russian cyberstrategy is that much of their cyber operability does not necessitate a high technological sophistication. In fact, most of the methods involve, at some point, human manipulation.

The Russo-Georgian and Russo-Ukrainian wars are perfectly exemplary of what a cyber war looks like - Russia made use of cyber methods to bolster their positioning both strategically, with broad political influences and disinformation, and tactically, with more targeted effects on

troops or energy systems. These were wars against a small and a middle power - their cyber capability lacking, making any kind of consequential retaliation unlikely

The Syrian conflict, on the other hand, was not. While the primary combatants were insurgent opposition groups, they had great support from large powers such as the U.S., U.K., and France. Being large powers, each one, though particularly the U.S., have great cyber capability, and a consequential retaliation to any hypothetical Russian cyber attack was much more likely. However, this did not stall Russian use of cyber methods - merely changed it. The outcomes of the U.S. and French presidential elections, both of which Russia used cyber methods to attempt to manipulate, were expected to have a profound effect on the Syrian war. While the Russians did not engage in cyber methods at the more tactical, direct level in Syria, they did on a level of "grand strategy", and with a more "soft power" attack than their efforts in Georgia or Ukraine. Due to their covert and soft power nature, Russia may have expected any retaliation to be soft power in nature as well, and thus an acceptable risk. They would have proved correct - the only form of retaliation came in the form of economic sanctions[59].

The influence of the attitudes toward nature of war and threat are clear. Russia demonstrates a broad view of war and how to win it, and has worked towards their goals unconventionally using cyber methods. It appears that dealing with a great threat does not subdue their cyber usage, merely changes it.

CHAPTER THREE: UNITED STATES

U.S. Strategic Culture

Hybrid nature of war

American and other Western entities historically tend to think of war in a purely conventional sense. Even as it may change tactically, it still exclusively concerns violence and physical force. Any discussion of non-violent means of political coercion is referred to as "soft power". Yet this is a perspective exclusive to the West. China uses a principle of Three Warfares that uses public opinion, psychological warfare, and legal warfare. Russia refers to conflicts of soft power as "low-level conflicts". While it is only a definitional disparity, it is an important one. The term "war" has the utmost importance attached to it, and if Russia, China, or other states abroad consider exertions of soft power as "war", then they clearly have a very different philosophy of the nature of war.

The United States, demonstrating such massive conventional superiority, presents an interesting case in the study of adaptation to the changing state warfare. Colin Gray wrote that "at least for several decades into the 21st century, all warfare involving the American superstate cannot be other than highly asymmetrical in character"[60]. Because of the U.S.'s incredible conventional advantage over other states, they demonstrate conventional superiority in any conflict they engage in. Inherently, enemies of the U.S. will resort to asymmetrical means as a method of victory, or at the very least survival, against massively powerful conventional force. The asymmetry with which American enemies fight has proven effective, as in all the decades of

clear American hegemony since 1945, they rarely achieve a decisive, meaningful victory in the wars they engage in. Unable to handle a changing landscape of war, the U.S. reaches ambiguous results in their conflicts, overwhelming with military force while at the same time being undercut by unconventional methods. The ambiguity of outcome may be due to the disparity seen between tactical and overall success. As one scholar writes, the U.S. exhibited "tremendous success at the tactical level followed by strategic muddling and eventual failure"[61]. This is a clear indication of a fundamental issue with how America approaches war. There is a systemic issue with the American strategy, and it may derive from the strategic cultural view of the nature of war.

In a consideration of U.S. flexibility towards novel forms of warfare, the most obvious example is their military involvement in Vietnam. Prior to Vietnam, there was in fact tactical doctrine regarding fighting irregular warfare - in this form, counterinsurgency and counter-guerrilla methods. On the battlefield, adherence to this doctrine was mixed, as some generals forewent it in favor of the tactics they were used to, and others tried and failed to implement it. Following the failure in Vietnam, the U.S. Army made little effort for reform. Rather than taking their strategic failure as a lesson, like the Soviets did after the Afghan War, they considered that failure to be a product of novel strategy. In 1976, the primary source of Army doctrine, the newest edition of the Field Manual, was published, and focused on "how to fight and win on an armor-dominated battlefield against an enemy who enjoyed vast quantitative superiority in both men and equipment."[62]. This is, of course, not the reality of the dangers faced by the U.S. at the time, nor where they had failed prior. This focus was borne out of a fear of a

land war on Europe against the Warsaw Pact. This focus, throughout the 1970s, led the Army to "an institutional identity of focusing on conventional operations"[63]. Between a misinterpretation of the failure in Vietnam, and an obsession with a hypothetical Soviet land threat, American strategic culture ingrained itself in its conventional view of the nature of war, while in the meantime, rivals of the U.S. broadened theirs.

While America demonstrated strategic deficiency in Vietnam, it and the Cold War as a whole did represent an increase in hybrid warfare by the U.S. Covert support of militant groups in order to enable violence is a form of waging hybrid war, and that form ran rampant in the decades-long tension between the U.S. and Russia.

A region ripe with instances of hybrid warfare usage is Central America. U.S. efforts in Central America were inundated with controversy. The U.S. offered support to many controversial figures in Latin America. In Guatemala, in 1952, after a domestic revolution, the state seized farmland, affecting the American company United Fruit. In 1953, CIA began training Guatemalan militants who shortly thereafter overthrew the new Guatemalan government. In the Dominican Republic, a long-time U.S. backed dictator Rafael Trujillo had his support cut off by Kennedy, and was later assassinated by CIA-backed rebels. 20,000 American troops under Johnson entered the DR in 1965, with the intent of stopping a communist revolution. After 1966, the country was ruled by Joaquin Balaguer, who had the same moral deficiencies as Trujillo. Their relationship with the bloody reign of right-wing leader Efrain Rios Montt in Guatemala, for one. Where President Carter had cut off aid to Guatemala in 1977 due to

human rights violations by their government, Reagan quickly rebuked that in 1982, sending military supplies to Rios Montt[64].

The U.S. has demonstrated a hybrid nature of warfare in their use of proxy support through the Cold War. However, whether this constitutes a significant factor in its strategic culture is dubious. There are a few reasons for this. Firstly, U.S. proxy warfare has no interstructural congruence. Much of support to proxy groups came from American intelligence, and often by subverting the congressional process, or without advice from military or diplomatic sectors. The result of this was a large degree of pushback from the American public and government which may have hindered any future efforts. Secondly, while the U.S. did provide aid to these militant groups, they exerted little control over them. Thirdly, while these examples of proxy support were instances of hybrid warfare, as the conflicts were not ones the U.S. was directly, significantly involved in, their strength as examples are weaker.

That said, there are many instances where the U.S. performed proxy warfare. Even in the modern era the U.S. engages in proxy warfare with agreement between civil and military institutions. While certainly, they do not exhibit the same kind of control as other patrons of proxy warfare do over the proxy groups, it is still a significant part of the American way of war. Thus, in assessing the hybrid nature of the American view of war, their extensive use of proxy warfare throughout the latter 20th century and 21st century will be given weight.

Despite their focus on conventional warfare, there were technological developments that fostered change in American strategy. After the Gulf War, during the 1990s, came the increasing

prevalence of "precision strike" weapons. In the early 90s, many considered it likely that the technology would proliferate widely and rapidly. However, years later, according to a 2013 report, nearly all long-range precision strike capability rests in the hands of the U.S., with China as a second and most of its rivals seeking the development of precision-strike capabilities[65]. The broad logistic and intelligence capabilities of the U.S. facilitate the use of precision-strike methods, as a proper identification of a target is essential to a precision strike, and good intelligence helps identify targets. Long-range strike capability certainly changed the way America fought wars, but not without restraint. American or allied forces in a region could be subject to an enemy's short-range strikes, leading to an MAD-esque reluctance to use precision strike. Regardless, precision-strike capabilities enhanced the tactical potential of American conflicts. The necessity of precision-strike technologies, such as good intelligence collection, may have facilitated a change from strictly conventional strategy. However, any such change did not come to fruition doctrinally until the 21st-century.

Strategic scholars have affirmed the idea that American strategic culture is not well-equipped to deal with changing warfare. In his 2004 book, *Blitzkreig to Desert Storm,* Robert Citino writes that "the US Army never did come to grips with the problems of guerrilla warfare, never reformed itself into a force that could successfully prosecute a guerrilla war and outside its Special Forces components, never regarded irregular warfare as normative in any way"[66]. Colin Gray, one of the aforementioned renowned strategic scholars, wrote on the American way of war in his 2006 paper *Irregular Enemies and the Essence of Strategy: Can the*

American Way of War Adapt?. Gray concludes that the U.S. military is best prepared for a "symmetrical" enemy rather than an asymmetrical one - in other terms, best prepared for conventional warfare. Some key terms Gray uses to describe the American way of war are "astrategic", "apolitical", and "profoundly regular". Gray is particularly pessimistic about the reform of this strategy, claiming that "most likely, Americans can remake their strategic performance only if they first remake their society, and that is a task beyond the ability of even the most optimistic agents of transformation". However, Gray goes on to acknowledge that the American way of war can identify pathways to improvement, thanks to a recognition of irregular enemies in the U.S. military[67].

Gray's foreboding paper and its pessimism toward the possibility of change in U.S. strategy was put to the test at the same time it was written. The US neglect of any real, widespread, focused counterinsurgency doctrine persisted through the Iraq War to 2005, where a man named General Petraeus became commander of the Combined Arms Center (CAC). Petraeus established a team to develop a counterinsurgency field manual, and used his influence to spread the ideas across the American strategic landscape. The field manual, FM 3-24, was "written with a broad and reflective focus, which engages on both strategy and political conditions"[68]. Petraeus's manual was the first indication of America's broadening horizon of the nature of war, on both tactical and strategic levels. The emphasis on an understanding of political conditions was a novel and important development for U.S. strategic culture, and addressed Gray's concerns of the American strategic culture being astrategic and apolitical. Beyond dealing

with counterinsurgency tactically, America needed to broaden their strategic perspective on war, fully considering the complex political situations of many of these insurgencies. The manual was published in 2006, and shortly after, Petraeus went to Iraq as the Commander of US forces, prepared to implement his newfound doctrine. General Petraeus, along with General Odierno, experienced great success implementing newly founded counterinsurgency techniques.

The heightened success in Iraq ingratiated American strategic culture toward straying away from conventional warfare in favor of counterinsurgency techniques, where the failure in Vietnam had scared them away. Thanks to military reform and operational application, the benefit of a broader, more flexible view of the nature of war had been demonstrated to the people of America, and its strategic culture quickly adapted. This was exemplified in the 2010 National Security Strategy, which stated that "our military must maintain its conventional superiority. It must also prevent and deter threats against the United States, its interests, and our allies and partners, and prepare to defend the United States in a wide range of contingencies against state and non-state actors"[69]. The mention of "wide range of contingencies" and the threat of non-state actors was emblematic of the newfound attention being paid to more hybrid warfare. That said, there was still an undue focus on conventionality, and with little mention of a broader strategic scope.

Even today, the U.S.'s definitional tendencies betrays their stance on warfare. "Irregular warfare", unlike in this paper, is described by the U.S. military doctrine as merely a violent struggle between state and non-state actors over certain populations. "Unconventional warfare"

is defined as just support provided by the military to a foreign resistance group. These are specific, operational definitions, and are still primarily concerned with the use of conventional violence. The U.S. still values hard power above all else. They "tend to be wedded to a hard power approach to strategy and statecraft that underplays the importance of soft power". It has been described as a "soft-power dynamo that tends to think in hard-power terms" and think largely "about achieving physical effects"[70].

There has been change, in more recent years, to the American view of warfare. Obama national security adviser Susan Rice said that "the fight agains the Islamic State had to be thought of as a multifront war" citing computers as just another "weapon in the arsenal"[71]. The 2018 U.S. National Defense Strategy states that the new predominant challenge is the "reemergence of long-term, strategic competition" with revisionist powers, such as Russia or China[72]. The U.S. Chairman of the Joint Chiefs of Staff Gen. Joseph Dunford said that the mindset that "we are either at peace or at war is insufficient" to handle the use by foreign adversaries of "economic coercion, political influence, unconventional warfare information ops, and cyber ops to advance their interests"[73]. Recent American scholarship has denoted this concept as "gray zone warfare". A RAND report defines gray zone warfare as "activities by quasi-revisionist states that seek to alter the status quo of the international order through coercive military or political means just below a threshold that would elicit a conventional military response"[74]. While the American attitude toward hybrid warfare is adapting, for the majority of "cyberwarfare history" it has remained fairly rigid.

Unlike the Russians, the U.S. does not have as much of a "whole concept" view of warfare. Their most "irregular" or "unconventional" definitions of it still only concern the use of conventional force. Where the Russians have a strong sense in the breadth of waging war, comprising a battlefield on many levels - conventional, economic, information, political, and more - the Americans do not. While certainly, there are examples of American use of non-violent methods in influencing the outcome of a conflict, in the scope of American strategic culture, these values do not appear to exist as strong influences. Americans adapted to hybrid warfare in the Middle East due to select forward-thinkers in the military. This adaptation was primarily tactical, but with some attention paid to strategy - the political conditions of a situation were paid more attention by the military itself, not just policymakers. While the U.S. demonstrated remarkable improvements in the flexibility of their view of the nature of war, it still pales in comparison to rivals like Russia.

The U.S., the dominant power of the world, is a quintessential example of a status quo state. But in a rapidly changing world, this plays to their disadvantage. The pervasive sense of superiority due to actual overwhelming power leads to a sense of complacency. Not faced with massive failure, like the Russians after the fall of the USSR, the Americans had no reason to seek revolution or even reform in the way they wage war. A few individuals made attempts to change this, seeing these failures, but strategic culture is strong, and steps are incremental. While America made progress in its treatment of warfare thanks to prescient individuals like General Petraeus, it has not reached a point where it wages war on all levels. More is necessary than

simple acknowledgment of the modern nature of war by select single individuals, even those in power. It requires congruence across all levels of strategic power in a society - military, government, intelligence, and elites. That congruence is inherently structural, and structure is more beholden to strategic culture than individuals are. Without that, steps are like those made by Petraeus - unfortunately incremental.

U.S. Cyber Methods Parallel to Conflict

Iraq War

Table 4: Iraq War

Allied combatants/supporters	*Actor type*	*Enemy combatants/supporters*	*Actor type*
United States	Large state	Hussein administration (2003)	Small state
Coalition forces	Varied	al-Qaeda	Non-state

In 2003, there was a notable large cyber operation planned for the Iraq war that was scrapped. American military and intelligence created a plan for a cyberattack that could "freeze billions of dollars in the bank accounts of Saddam Hussein and cripple his government's financial system before the United States invaded Iraq", which would destroy Hussein's war efforts. However, the Bush administration shot it down, citing the potential for worldwide financial damage[75]. The targeted banks had connections to French banking networks, and had the potential to disrupt banking activities across Europe[76]. This collateral damage to allied countries

was not a risk the Bush administration found acceptable. While certainly, the denial of a massive planned operation may suggest an avoidance of strategic cyber methods, the circumstances negate that implication. The U.S. being unwilling to potentially harm their allies was the primary reason for denial of this operation. The mere acknowledgement of the potential benefit of economic attacks is a strong indicator of how the U.S. may use cyber methods. However, it is ultimately indicative of a deeper nature of the American attitude toward cyberwarfare. The fear of collateral damage derives from cyberwarfare being waged with imprecise weapons. America's desire to maintain good relations, its extensive ally network, and its democratic mores make it inherently averse to collateral damage, namely, when it is on a global and unknown scale.

While this large operation was denied, similar operations took place alongside the advent of the Iraq war. The U.S. undertook electronic jamming and attacks on Iraqi telephone networks, including collaboration with large telecom companies. This proved to have a degree of collateral damage, though not to the level Bush expected from the larger attack - only a few neighboring countries had their communications affected[77]. This further discerns the American perspective on collateral damage in cyberwarfare. What Bush considered to be "acceptable" collateral damage were states U.S. foreign relations were not dependent on.

In 2007, President Bush directed the NSA to conduct a cyberattack on cell phones and computers being used to coordinate roadside bombings by Iraqi insurgents. According to an administration official, the operation "helped U.S. forces to commandeer the Iraqi fighters' communications system"[78]. This attack was tactical in nature, but the notable part is the

collaboration between intelligence and military. As has been mentioned, interorganizational congruence may be a good indicator of the strategic importance a state places on cyber methods.

War in Afghanistan

Table 5: War in Afghanistan

Allied combatants/supporters	*Actor type*	*Enemy combatants/supporters*	*Actor type*
Afghanistan	Small state	Taliban	Non-state
United States	Large state		
Coalition forces	Varied		

There is unfortunately little open information on the use of cyberwarfare by the U.S. in Afghanistan. However, there is confirmation that it was used, at least to a degree. Marine Lt. Gen. Richard Mills, who led international forces in Afghanistan from 2010-2011, acknowledge the use of cyber attacks in Afghanistan, stating that he was "able to use [his] cyber operations against [his] adversary with great impact", stating that he was able to "get inside his nets, infect his command-and-control, and in fact defend [himself] against his almost constant incursions to get inside my wire, toa affect my operations"[79]. From Mills' comments, he appears to be referring to primarily tactical cyber operations, focusing on getting a tactical advantage. The focus on nets and command-and-control suggest it was used to glean intelligence or informational sabotage.

The lack of extensive cyber methods employed may have to do with the cyber infrastructure of the state. Afghanistan had only 1.1% of computer usage across the population in 2006, totaling 300,000 users. At the time of President Obama's withdrawal in 2016, this rose to only 12.0% of the population[80].

While internet usage was limited, cellular usage was broader, with up to 2.52 million users in Afghanistan in 2006. It may be possible the vague cyber methods referred to by Mills were undertaken via telecommunicative channels.

Syrian Civil War

Table 6: Syrian civil war, U.S.

Allied combatants/supporters	*Actor type*	*Enemy combatants/supporters*	*Actor type*
Syrian opposition groups	Non-state	Assad administration	Small state
United States	Large state	Russia	Large state
France	Large state	Iran	Middle state
United Kingdom	Large state	Syrian Electronic Army	Non-state
Coalition forces	Varied		

The Syrian civil war is a backdrop for a complex myriad of conflicts. The U.S., directly and indirectly, has been involved in these conventional conflicts. Their most prominent conflict is with ISIL (Islamic State of Iraq and the Levant), radical insurgent group, and this conflict extends to Syria. The U.S. has increased their military presence in the Middle East as a means of

combating ISIL, and its rivals oppose that. As a part of this, the U.S. has committed military support to several Syrian anti-Assad opposition groups in the region.

There has been very minor indication of cyber support given to independent Syrian groups. The U.S. Department of State 2013 fact sheet "U.S. Government Assistance to Syria" states that the U.S. provides media outlet support to "citizen journalists, bloggers, and cyber-activists" including "technical assistance and equipment to enhance the information and communications security of Syrian activists within Syria"[81]. While the specific details of this support is unclear, it appears as though the U.S. has provided cyber support to groups within Syria. However, it is not evident whether this was limited to media groups or if the support extended to armed Syrian opposition groups

There was also the *potential* for a U.S. cyber offensive to promote their ideals in the region. In 2014 there was "discussion at the highest levels of government concerning a possible humanitarian mission that could be conducted via cyber attack", the details of which were unknown[82]. While this was a vague reference, it likely concerned internet freedom or information, given that has the least potential for collateral damage of cyberattacks. Of course, this attack never came to fruition - the Obama administration cited the usual fears such as cyber-escalation with Iran and Russia.

The lack of severity of the U.S. cyber involvement in Syria likely derives from the limited extent of their involvement. When there are no American boots on the ground, it

becomes more difficult to justify any direct offense, even when that offense can be conducted non-violently and without risk to American life.

War with ISIS

Table 7: War with ISIS

Allied combatants/supporters	*Actor type*	*Enemy combatants/supporters*	*Actor type*
United States	Large state	ISIS	Non-state
Coalition forces	Varied		

The Islamic State of Iraq and the Levant, or the Islamic State of Iraq and Syria (ISIS), was a radical terrorist group. During the first half of 2014 they made rapid territorial gains, and committed many human rights violations, often intentionally spread across social media. Following these developments, the U.S., Russia, Iran, and a Western coalition began the fight against ISIS.

The U.S. campaign against ISIS is a hotbed of American active, offensive cyber methods. Under the relatively newly formed Cyber Command, American cyberwarfare found new structure and direction. A *New York Times* report described the cyber campaign against ISIS. They stated that its goal was to "disrupt [its] ability to spread its message, attract new adherents, circulate orders from commanders, and carry out day-to-day functions, like paying its fighters". They state their goal into doing so is to "rattle" commanders and deter potential recruits by undermining ISIS security.

The *Times* reports the U.S. counter-ISIS cyber operations consist of "national mission teams", which are cyber units vaguely organized like Special Operations forces. They outline some more operational methods. They "learn the online habits of commanders", then "imitate them or alter their messages, with the aim of redirecting militants to areas more vulnerable to attack by American drones or local ground forces". General Jospeh Dunford Jr., chairman of the Joint Chiefs of Staff, described it as "trying to both physically and virtually isolate ISIL, limit their ability to conduct command and control, limit their ability to conduct operations locally and tactically"[83].

The majority of American cyber usage against ISIS appears to be tactical - directly in support of military operation, maneuvering troops or hindering ISIS logistics. However, in a notable disparity with the previously discussed American way of waging war, there were some efforts made toward information warfare.

In 2014, the State Department embarked on a counterpropaganda campaign against ISIS. They created a propaganda video called "Welcome to ISIS Land" which was spread on social media. It was essentially an ISIS recruitment satire, promising learning skills such as "crucifying and executing Muslims", including graphic imagery. This effort was begun by a State unit called Center for Strategic Counterterrorism Communications (CSCC) and was backed by President Obama. The CSCC was to act "like a war room in a political campaign", being prepared to "monitor every utterance by the adversary and respond rapidly". The campaign had incredibly mixed reactions - experts in Washington described it as "embarrassing" or "helpful to the

enemy". American media lambasted it. The video achieved less than a million views, and there was no proof that it had discouraged ISIS recruitment. Considering the low view count, it appears unlikely. This was one of many failures of the CSCC. It was given little care by the American government, with a very small budget[84]. After administrative support dwindled, the State Department established the Information Coordination Cell. This, unlike the propaganda of the CSCC, would be more fact-based - if ISIS made a false claim, it would be met by proof of reality via picture. It would also rectify a flaw of the CSCC by integrating their campaign with other parts of the federal government rather than acting independently. However, the information efforts were still inherently flawed. Nicholas Rasmussen, director of the National Counterterrorism Center, said that "we try to find ways to stimulate this kind of counternarrative...without having a U.S. government hand in it...people who are attracted to this don't go to the government for their guidance on what to do, not the U.S. government and certainly not their governments in the Middle East"[85].

Following these failures, the U.S. government "turned to non-government entities to take over creating counter narratives". These non-government entities, underfunded, could not match the cyber manpower of ISIS propaganda spread and creation[86].

In 2016, deputy national security adviser to President Obama, Lisa Monaco, met with technology executives to "come up with a more integrated plan for both taking down social media posts and encouraging the development of a counternarrative", which includes "amplifying the testimony of Islamic State recruits who have escaped and now describe the

group's brutality and question its adherence to the true tenets of Islam"[87]. Overall, there have been fundamental flaws in American active information campaigns.

Between flawed execution or structural incongruence, America has not proven itself adept at broad information warfare waged on social media. Additionally, these methods are cyber only in name. Their implementation is rudimentary - posts through official accounts of the state or non-government entities. Where ISIS and Russian cyber-propaganda necessitates some degree of technical sophistication, whether that be bots or other means of spreading, the State efforts did not integrate those. This may be due to Department of State deficiencies at an organizational level, lacking the technical expertise of its military counterparts.

Separate from administration and State, the U.S. Cyber Command and National Security Agency (NSA) took alternative routes. Joint Task Force ARES was a cyber team established in 2016 aimed at dismantling the cyber propaganda wing of ISIS. Their five tenets of operation were to "keep the media operation under pressure, make it difficult for ISIS to operate on the web more generally, use cyber forces to help forces on the ground fighting ISIS, hobble its ability to raise money, and work with other agencies in the U.S. and allies abroad". They systemically identified the internet distribution hubs of ISIS and dismantled them. Beyond that, they underwent some psychological operations on ISIS members. They would cause IT issues, "slow downloads, dropped connections, access denied, program glitches", "change passwords, or buy domain names, delete content", in a way subtle enough that it would pass without suspicion

[88]. This was a notable method, as it is the first example of creative psychological cyber operations undertaken by the U.S.

While this program proved a massive success, it was dismantling and deterrence, the same cyberstrategy the U.S. adhered to for any of their tactical conflicts. The military wing of the U.S. government still lacked any offensive informational cyber methods - no counterpropaganda campaign. In fact, exemplary of the lack of cyber information methods demonstrated by the U.S. military against ISIS, the Army even engaged in a form of information warfare that was almost a century old. As the Allies did over Europe decades ago, the U.S. dropped anti-ISIS leaflets over Syria in an effort to discourage ISIS recruiting[89].

Between the repeated inefficacy of the State program and the lack of one by the military, U.S. strategy remained without effective offensive cyber information operations. The informational application of cyber methods went unregarded by the military, and while other facets of the government that made attempts at it, there was no structural congruence for a broad operational implementation.

Iranian proxy conflicts

Iranian conflicts in the Middle East are strategically relevant. Through proxy groups, Iran engages in conflict across all countries in the Middle East, particularly in Syria, Iraq, and Lebanon. Its primary rivals are Israel and Saudi Arabia. As their ally, the U.S. has a level of involvement in these conflicts. While not a conventional war, they are violent and strategically significant for the U.S., and thus will be used as part of this paper. This section focuses on U.S.

involvement in these conflicts using cyber methods. The U.S. also engages in non-conflict specific general cyber attacks, which will be addressed first.

Iran-Israeli proxy conflict

Table 8: Iran-Israeli proxy conflict

Allied combatants/supporters	*Actor type*	*Enemy combatants/supporters*	*Actor type*
Israel	Middle state	Iran	Middle state
United States	Large state	Proxy groups	Non-state

U.S., a long-time ally of Israel, is involved in its conflict for regional hegemony with Iran. Israel's control over the Middle East is inherently linked to the U.S.'s influence there.

The most well-known and foremost example of cyber action against Iran by the U.S. is Operation Olympic Games - better known as the weapon called Stuxnet. A cyber weapon using a worm known as Stuxnet was implanted in the Iranian nuclear facility at Natanz and sabotaged centrifuges, crippling Iran's nuclear program. Stuxnet destroyed upwards of 1,000 nuclear centrifuges and reportedly set Iran's nuclear program back at least 2 years. Stuxnet was discovered in 2010 and reportedly had been in development since 2005 - at the time, prior to Stuxnet, Iran had very little cyber capability[90].

Stuxnet is an inherently strategic, kinetic cyber attack. Unassociated with any direct battle or military movement, it exclusively focused on Iranian long-term technology. Akin to Russian election interference and its interests in Syria, Stuxnet had wide-reaching strategic benefits for

the U.S., but also benefits in the Iran-Israeli conflict and other ongoing Middle Eastern conflicts Iran has a hand in. By deterring the development of nuclear power, the U.S. can subdue the potential of a nuclear weapon-enabled Iran, which may entirely change the political landscape of the Middle East. Particularly, it would pose much greater threat to Israel. With nuclear weaponry, Iran would have much broader room with which to act aggressively without fearing retaliation from the conventionally supreme United States.

Iran-Saudi Arabia proxy conflict

Table 9: Iran-Saudi Arabia proxy conflict, U.S.

Allied combatants/supporters	*Actor type*	*Enemy combatants/supporters*	*Actor type*
Saudi Arabia	Middle state	Iran	Middle state
United States	Large state	Proxy groups	Non-state

U.S. officials claimed that a 2018 cyberattack "destroyed digital resources that helped Iranians shipping traffic in the Persian Gulf", in retaliation to Iranian downing of a U.S. drone[91]. This would serve as an effective example of cyber-enabled economic warfare, as it assaults the trade status and economy of Iran.

In June 2019, Iran downed a U.S. drone over the Persian Gulf. As a response, the U.S. "wiped clean an IRGC database used to plan attacks against tankers in the Persina Gulf". Reportedly, there was also "widespread internet disruption" in Iran after the drone attack[92]. This

was a cyberattack aimed at displacing the tactical positioning of Iran, and a psychological one, causing disruption of internet access.

In October 2019, after an Iranian attack on Saudi Arabian oil facilities, the U.S. launched a cyberattack against Iran that focused on "Tehran's ability to spread propaganda", and claimed the strike "affected physical hardware"[93]. This was a deterrent method against cyber-propaganda, conducted via a kinetic strike that may be akin to a precision strike.

Conclusions

The U.S. does conform to the posed hypothesis. An analysis of American strategic culture reveals a relatively lesser attitude toward the use of hybrid warfare. While the U.S. has used forms of offensive hybrid warfare, such as their use of proxies in Latin America and the Middle East, or their tactical adaptation during the Iraq War, changes are incremental, and often there is often not structural consensus toward the use of hybrid warfare, with American organizations sometimes engaging in actions on their lonesome and even bypassing governmental approval. Official statements deceive a more rigid view of warfare than that of Russia. The U.S. still has a heavy reliance on overwhelming conventional force, though it is slowly progressing.

Given that, the hypothesis would dictate a lesser usage of conflict-parallel cyber methods. This proved true - while in their conflicts they engage in cyber methods liberally on the tactical level, the strategic level usage is lacking. The U.S. engages in very minor or no informational, proliferative, or economic cyber operations. Additionally, the U.S. is lacking in its usage of

offensive cyber methods against larger powers. Certainly, this is to some degree a result of their lack of open conflict with middle or large powers, but that does not account for the lack of strategic or soft power-esque cyber methods. While there are some efforts toward informational and proliferative cyber methods, those efforts are rudimentary if not failures.

Even against Iran, most cyber attacks are not proactive but rather retaliatory - in response to a kinetic or cyber Iranian attack. Stuxnet, the most prominent proactive, offensive attack on Iran, came at a time when Iran had little cyber power and was thus a small threat to the U.S., certainly so in the cyber realm (although arguably, the action was detrimental in the long term, as it led to the development of Iran's cyber program).

The restraint of the U.S. towards those states can be compared to its use of cyber methods in Iraq, Afghanistan, or particularly against ISIS. These conflicts - consisting of either small states or non-state actors - offered little threat of retaliation. The groups - while they may have their own certain type of cyber capability - do not possess any ability that poses a real threat to the U.S. or its forces.

CHAPTER FOUR: IRAN

Iranian Strategic Culture

Hybrid nature of war

A number of historical factors play into Iranian strategic culture. Between ancient Persian traditions, the 1979 Islamic Revolution, and several wars in between, Iran has cultivated an influential strategic culture.

While much less significant in determining Iranian strategic culture than recent history, given the large amount of revolution and reform, earlier history still holds significance, as well as an understanding of the context that led to modern Iranian strategic culture. In 1925, Iran began its transition towards modernism following a violent transfer of power between Shahs. This involved Westernization, as society grew more secular and power was transferred from the clerics to non-religious government. During the early years of the Cold War, Iran experienced foreign intervention from the superpowers. Iranian Prime Minister at the time, Muhammad Mossadeq, took power from Shah Muhammad Reza, relying on "violent street demonstrations", in 1952, taking power of both the military and economy. The Shah fled, but returned in 1953, as CIA and British supported anti-Mossadeq militants arose throughout Iraq. Following Reza's return to power, he ensured his complete control over it, and continued modernization effort. He began a "white revolution" in which his influence invaded every level of Iranian society.

Notably, he made religious decisions, as he "intruded on spheres normally reserved for the judgment of learned Shia scholars"[94].

The aforementioned Shia scholars had been actively combating the trend of secularization and Westernization seen in Iran in the 1950s and afterward. They viewed the Shah's white revolution as merely an extension of Western interests. The clerics' resistance soon grew to revolution, led by the Ayatollah Ruhollah Khomenei, who had been exiled for resisting the Shah. This revolution was the 1979 Revolution, which is the foundation of modern Iran. Rebelling against the Shah's perceived embrace of the West, the Iranians rebelled, with Khomenei and his clerics seizing power in the wake of this revolution, using their religious authority. During the Revolution, they reformed the government, with a new constitution. Clerical authority was pervasive in their new system of government, with clerics overseeing many levels of authority[95].

A lynchpin in Iranian strategic culture was the 1980-1988 Iran-Iraq War following the Iranian Revolution. Whatever Shah-era military elites that had survived the revolution had been dismantled by both the grueling war and the machinations of the religious authorities. What they were replaced by was the Islamic Revolutionary Guard Corps (IRGC), which rose from "the military arm of the Islamic revolution in 1979 to a major political player". In the new government, IRGC was given great military authority.

Additionally, the Iran-Iraq War affected the strategic way of war. In 1987, after Iran harassed Arabian oil tankers sailing through the Gulf, the U.S. Navy began escorting them. Iran

continued their harassment, and engaged in a conventional navy campaign against the U.S. forces, then was soundly defeated. Iran adapted to this defeat, utilizing different unconventional tactics with different technologies, and experienced increased success[96].

Another consequence of the Iran-Iraq War that affected the Iranian perception of war was U.S. sanctions. Bombarded by economic sanctions from the U.S. and allies, Iran was unable to purchase conventional arms as used by other modern countries. Rather, they developed alternative weapons to fit their specific needs. "Instead of a conventional air force, Iran developed ballistic missiles. Instead of traditional naval capabilities, Iran relied on swarms of small, fast-attack speedboats. Instead of conventional land forces, Iran built up terrorist proxies like Hezbollah"[97].

After the Iran-Iraq War drew to a close, the charismatic leader who took control of the Iranian revolution, Ruhollah Khomeini, died, in June 1989. Elections for new Supreme Leader were held, and Ali Khamenei, who was President during Khomenei's tenure, was elected. Many suggest that the voting clerics chose Khamenei because they believed he would not have the religious authority to garner much loyalty as Supreme Leader - thus giving them more influence over him, and consequently, Iran. However, Khamenei, rather than forging a strong bond with the clerics, became closely intertwined with the IRGC. Not only did this solidify Khamenei's strength in his position, but it gave the IRGC non-military societal influence as well, both political and economic. The symbiotic partnership between the Supreme Leader and IRGC led to

a heightened strength of military culture, and the culture of the revolution, on the strategic culture of Iran[98].

In efforts to expand its military influence while avoiding direct confrontation, Iran has fostered a unique way of waging war - through proxy groups. After the Islamic Revolution of 1979, Iran created the military proxy Lebanese Hizbollah in 1982. Over the decades, multiple other proxy groups have been created. While the autonomy of these groups vary, Iran exerts a degree of control over all of them significant enough to consider them military proxies. Significant proxy groups include the Popular Mobilization Forces in Iraq and National Defense Forces in Syria. There is a religious component to the formation of these groups - the majority of them are composed of Shi'ite members. The process of proxy formation by Iran is undergone by its military and intelligence facets, including the IRGC-QF, other parts of the IRGC, and Iran's primary intelligence service, the Ministry of Intelligence (MOIS).

The beginning of Iranian proxy warfare was borne from the revolution. Seeing the benefit of the Shi'ite revolution, and the benefits it reaped, Iran sought to export it abroad, particularly to areas "marked by Shi'ite marginalization in the Persian Gulf states and Lebanon"[99]. The influence of the Iranian Revolution was broad, and the government sought to use its legacy to their advantage - its success "encouraged disenfranchised, pious, and militant individuals and groups to overturn the status quo in such diverse states as Algeria, Egypt, Lebanon, Syria, Israel, and the Phillippines … in the name of a brand of Islamism that has only existed for a brief time in Iran"[100]. Iran continued to give support to militant groups to use them as strategic pressure

against Iran's state-level rivals . By empowering radicals seeking conflict within a region, Iran can destabilize that region, which is particularly beneficial when it is their rival.

The support to Iranian proxies comes in many different forms. Iran will supply large amounts of financial support which groups may use to support their efforts. It provides armaments and weaponry, as well as the elite training necessary to handle those weapons. Additionally, Iran has taught how to effectively perform non-military services, such as aid. Reportedly "groups that can step in and provide for … basic humans needs are likely to gain loyalty and support, even among people who do not have a natural ideological affinity for the group's goals". Finally, Iran spreads its religious dominance throughout these groups. Iran considers itself a religious leader and espouses that belief to the proxies it has throughout the Middle East, which only emboldens the proxies in the idea of their mission and bolsters their loyalty to Iran. That said, across all these proxies, Iranian support "does not buy unconditional loyalty"[101]. There are a few key developments in Iranian strategic culture that lead to the extensive reliance on proxy warfare - a sense of international isolation and religious fervor.

Fighting against Saddam Hussein's Iraq led to great consequences, and the intense war heavily shaped the fledgling government's way of waging war. A key facet of this was the cultivation of a sense of international isolation. The idea of a theocracy did not please the competing superpowers, the United States or the atheistic USSR. Nor did the radicalism brought by the Iranian revolution please its fellow Arab countries, who were alienated by the "Shiism and revolutionary zeal". The exception, on the state level, was Syria[102]. Their isolation in both the

region and the world may have led to their reliance on proxy warfare. With less capability to exert soft power diplomatically or economically, as a regional leper, Iran is forced to turn to an exertion of power more violent in nature, enabled by proxy groups that Iran can support and forego any responsibility for violence.

During the revolution and the following war, the Iranian government made efforts of inspiring a "culture of resistance, jihad, and martyrdom" within the Iranian people. This doctrine was cultivated with the intent of creating "a society that is energized and strengthened by conflict". This principle proved effective in the revolution - deaths of protestors only galvanized the population towards further action. However, it did not persist through the Iran-Iraq war, nor the Iranian government's oppressive regime. While the Iranian people certainly inherited a strong sense of religion, they did not to the extent of martyrdom. Indeed, today the "jihadi martyrdom culture is embraced only by hardcore Hizballahis and Basijis, who make up only a small, albeit influential, part of Iranian society"[103]. This may be yet another explanatory factor for the extensive use of proxies. Where Iran could not find that martyrdom in their own soldiers, they may find it in Lebanese or Iraqi militants.

Beyond their use of proxy warfare, Iran places significant importance on soft power. Iran has decided to "eschew a large, balanced conventional force structure" which may indicate "an approach to national security that places greater emphasis on guile than on brute force, and on soft power than hard power"[104]. Its leaders believe in "the primacy of the moral, spiritual, and psychological dimensions of statecraft and strategy". This is fitting when considering the

formation of modern Iranian strategic culture. The event of its conception, the 1979 Revolution, was founded upon spiritual and psychological morale in the Iranian people, so it comes as no shock that the ruling clerics would continue this sense of spiritual authority, both within their borders and abroad.

Iran has an intense aversion to any idea of submission or defeat to a foreign power. Article 152 of the Iranian constitution states "the foreign policy of the Islamic Republic of Iran is based upon the rejection of all forms of domination, both the exertion of it and submission to it, the preservation of the independence of the country in all respects and its territorial integrity"[105].

On a structural level, there is a high degree of congruence across all levels of strategy. The Supreme Leader Ali Khamenei, preceded by Ruhollah Khomenei, is the absolute authority, and has "built a superstructure of ideology, security, intelligence, government, and economy in Iran"[106]. The Iranian government has the same intermingling. The IRGC, a major (though not majority) wing of the Iranian military is very well-integrated with unconventional military aspects. The IRGC "has primacy over Iranian unconventional warfare options" and "wields an external terrorism capability through its elite Qods Force"[107]. The Qods Force (IRGC-QF) is the covert wing of the IRGC - the mere existence of a major covert organization being integrated into the military is exemplary of the strategic congruence Iran has. U.S. General Stanley McChrystal describes the Quds Force as "analogous to a combination of the CIA and Joint Special Operations Command in the U.S."[108].

The IRGC also has strong influence within non-military aspects of statecraft. Iranian political and economic leadership is inundated with former and current IRGC soldiers, including several cabinet ministers, corporation heads, and the President Ahmadinejad himself. The IRGC is ingrained within the Iranian government - since the 1979 Revolution, it has played an important role in Iranian politics.

Another factor in the centralized structure of Iranian society is the authority granted to clerics. As previously mentioned, after their grasp of power during the 1979 Revolution, clerics inundated themselves as a source of societal authority.

In 2004, Iranian Deputy Defense Minister described the Iranian defense strategy as "diverse", and claimed that it made up for any conventional inferiority[109].

Iranian leaders have said as much. IRGC official Hojjat al-Eslam Ali Saidi said in 2014 that "our war with the dominant system is an asymmetrical war. What makes [it an even struggle] is the element of spirituality, motivation, and will".

The Iranian war is not fought in a clearly delineated time period, nor is it defined by being or not being in a state of war. Rather, it is ongoing, and obscured, as some scholars describe as "the Middle Eastern cold war". Iran avoids open conflict, viewing it perhaps rightfully so as an existential threat for their conventionally inferior military. Instead, they seek deterrence - through "exaggeration, ambiguity, and obfuscation". Iran will use "official statements, well-publicized parades, set-piece exercises and shows of force, and tests of

advanced systems such as intermediate-range ballistic missiles to deter adversaries from initiating conflict"[110].

The Iranian goal of deterrence is inherently linked to their nuclear ambitions. Obtaining a nuclear weapon would greatly assuage their fears of aggression by a great power, and give Iran greater flexibility to act in the Middle East. Unrestrained by a fear of Western intervention, Iran could go to great lengths to exert influence across the Middle East. These nuclear ambitions were eventually quelled, first by Stuxnet in 2012, and later by the diplomatic agreement JCPOA. The IAEA has certified their compliance, though Israel suggests otherwise. In the wake of increasing tensions with the U.S., including the U.S. withdrawing from the JCPOA and their assassination of Iranian general Soleimani, Iran has declared that it would "no longer abide by the limitations of the deal", though was open to further negotiations.

In more recent years, Supreme Leader Khamenei is aging, and considering his successor. According to the constitution, he selected an Assembly of Experts to choose his successor, though he was careful to choose those loyal to him as voters. Many suspected that, regardless of the new Supreme Leader, Qasem Soleimani, head of the IRGC, would be selected as President, granting the IRGC even more influence[111]. His surprise assassination by the U.S. in 2020, though, created a power struggle within Iranian politics, the ultimate consequences of which are yet to be seen.

Overall, Iran exhibits a view of the nature of war that is highly hybrid in nature. Their unique political positioning has forced them into a unique way of warfare - alienated both

regionally and abroad, marked by theocratic authority, and borne of religious uprising, Iran has turned to proxies full of dogmatic soldiers to exert its influence abroad. Iran, lacking in overwhelming conventional power, has been forced to adapt, and found that adaptation in heavy covert action. Iran was born from an ideological revolution, so its current government's understanding of the importance of politics and identity in war is paramount, contributing to its hybrid nature. Moreover, without the same hard power capabilities as its rivals, Iran utilizes soft power extensively. All these factors lead to the conclusion that Iran's way of waging war is very hybrid in nature.

Iranian Cyber Methods Parallel to Conflict

Iran-Saudi Arabia proxy conflicts

Table 10: Iran-Saudi Arabia proxy conflicts, Iran

Allied combatants/supporters	*Actor type*	*Enemy combatants/supporters*	*Actor type*
Iran	Middle state	Saudi Arabia	Middle state
Yemen Cyber Army	Non-state	United States	Large state

One of the most significant cyber attacks of the ongoing conflict between Iran and Saudi Arabia is the sabotage of Saudi-Aramco, one of the largest oil companies. A group named "Cutting Sword of Justice" claimed responsibility for the release of Shamoon, the virus that caused the hack. US officials claimed that the group is merely an Iranian proxy, though offered no evidence towards that claim. One cybersecurity expert said that he "heard speculation from

more than one source in Saudi Rabia that the malware attack...was an Iranian operation to discourage Saudi Aramco from increasing its oil production"[112].

Additionally, in August 2017, a series of cyberattacks occurred at petrochemical plants in Saudi Arabia. Saudi Arabia, U.S. officials, and cybersecurity firms tend to agree that it was likely to be Iran. Some of these attacks could have triggered explosions - representing a significant attack[113].

APT33 is a cyber group that launches campaigns against Saudi Arabia. They target Saudi Arabian business conglomerates with ties to the aviation sector. Cybersecurity firm FireEye reports APT33 as working on behalf of the government of Iran, and targeting critical infrastructure, energy, and military sectors with cyber-espionage. The FireEye report states that they believe the "targeting of the Saudi organization may have been an attempt to gain insight into regional rivals". Additionally, in 2019 Microsoft researchers reported that APT33 shifted its targeting to industrial control systems in the energy sector[114] . Another Iran-linked cyber group, as mentioned in a report by Israeli firm ClearSky, is CopyKittens, which has acted since 2013 and primarily engages in cyber espionage, including against Saudi Arabia. APT 34 is another group which has attacked Saudi Arabia on behalf of Iran, releasing data-wiping malware[111].

Houthis

A significant Iranian proxy which is disposed against Saudi Arabia are the Houthis in Yemen, who combat the Yemeni government supported by the Saudis. A notable cyber actor in this conflict is the Yemen Cyber Army (YCA). The YCA, in April 2015, defaced the website of

London newspaper al-Hayat, where they leaked information and spread messages supporting the "Yemen revolution". The YCA has also attacked Saudi Arabian government ministries to gain espionage, obtaining a multitude of classified information and data[116].

The YCA link to Iran has been researched. Shortly after its conception, security experts began to believe that its sudden creation and coincidence with similar Iranian attacks indicate that the YCA is not even composed of hackers from Yemen, but rather Iran itself. Fars, a "semi-official Iranian media outlet" is typically the first to report YCA activity and acts as a "mouthpiece" for it. Though no definitive link has been identified, several cybersecurity experts concur in their belief that the YCA is not even trained by Iran, but composed of Iranians.

Iraq War

Table 11: Iraq War, Iran

Allied combatants/supporters	*Actor type*	*Enemy combatants/supporters*	*Actor type*
Iran	Middle state	United States	Large state
Hezbollah	Non-state	Coalition forces	Middle state
Kata'ib Hezbollah	Non-state		

Hezbollah has engaged in disinformation-based recruitment efforts in Iraq, in order to recruit for Kata'ib Hezbollah which engages in combat with U.S. and coalition forces. A precursor for the methods of ISIS, they would film attacks and spread them online as propaganda. Beyond the use of social media to spread propaganda, there was no significant Iran

proxy activity in the 2003-2011 Iraq War. This is likely due to the fact that, up to that point, Iranian cyber aspirations were limited. It was only after the Stuxnet attack that their priority shifted towards cyber capabilities.

War on ISIS

Table 12: War on ISIS, Iran

Allied combatants/supporters	***Actor type***	***Enemy combatants/supporters***	***Actor type***
Iran	Middle state	ISIS	Non-state
Kata'ib Hezbollah	Non-state		

Much of Iran's conflict with ISIS occurs in Iraq, where one of their larger proxies is Kata'ib Hezbollah. Kata'ib Hezbollah has developed their own digital propaganda team, which was "flooding facebook with fake accounts and promoting fake news". The US government reported that "Kata'ib Hezbollah and other Iraqi electronic armies have reportedly floated millions of dollars in advertising expenses to Facebook". Additionally, playing off of Hezbollah's cyber expertise, Kata'ib Hezbollah would fly militants to Lebanon to be trained in cyber methods[117]. Being a large Iranian proxy in Iraq, they may use this cyber capability against ISIS, or at least make use of it tangentially by recruiting. Beyond their indirect cyber influence on Kata'ib Hezbollah, Iran makes little effort to utilize cyber methods against ISIS.

Syrian Civil War

Table 13: Syrian civil war, Iran

Allied combatants/supporters	*Actor type*	*Enemy combatants/supporters*	*Actor type*
Assad administration	Small state	Syrian opposition groups	Middle state
Iran	Middle state	United States	Large state
Russia	Large state	Coalition forces	Varied
Syrian Electronic Army	Non-state		

There is dissent on whether the Syrian Electronic Army receives assistance from Iran. Cybersecurity firm Recorded Future, using open-source data, claimed that it is not[118]. However, U.S. officials such as NSA Director Michael Hayden or White House advisor RIchard Clarke said that it has the indications of an Iranian proxy[119]. Additionally, the SEA experienced large amounts of improvement in the technical sophistication of their attacks between 2011 and 2012, something which cyber experts attribute to Iranian assistance[120]. Given that the Recorded Future report was based only on open-source data, whereas other cyber experts and government officials claim otherwise, it is likely that there is a link of aid between the Syrian Electronic Army and Iran. After all, open-source data can be inconclusive - about the Saudi Aramco attack, which is now accepted to be Iran's responsibility, a CSIS director said "nothing in open source intelligence pointed to Iran"[121]. In 2011, there was crossover between SEA website defacement and a hacker claiming to be Iranian[122].

Coinciding with the enhancement of SEA abilities was the dispatch of IRGC-QF support to pro-Assad forces. While this extended beyond mere cyber support, cyber support was a significant part of it. They brought advanced equipment "designed to disrupt communications, the Internet, email, and cell phone communications" and taught them how to "fight people without killing; how to use force to cause injury, without being accused of a massacre… teaching them how to control websites and social media and how to jam television channels". The SEA "aggressively engaged in a wide range of online activities to punish perceived opponents and to force the online narrative in favor of the Assad regime"[123].

Despite the cyber aid provided by Iran to SEA and Assad, there has been no significant cyber attack as part of the Syrian conflict. Some scholars suggest this is an indication that Iran withheld certain cyber capabilities from them, as an anti-proliferation measure. Indeed, the more kinetic cyber capabilities utilized by the SEA included only "distributed DDOS attacks, jammed online portals, overloaded networks, and...malware to thwart opponents' messages and actions" - relatively rudimentary cyber capabilities. Much of Iran's direct cyber activity involved spreading propaganda in the larger Internet, particularly propaganda aimed at absolving Iran's culpability in the Syrian involvement[124].

There is indication of more direct minor Iranian cyber support, as groups more closely linked to the Iranian government launch attacks on Syria. Researchers in Toronto's Citizen Lab identified an Iran-based cyber group named Group5 which targets anti-Assad groups. This group primarily acted by dispersing infected documents and files by masquerading as legitimate

sources. A link to Iran was identified by a tool commonly known to be used by Iran as well as another Persian-language tool[125].

Another hacking group was identified, operating from Lebanon in 2013-2014. They engaged in a honeypot-esque operation, where they would masquerade as a female and lure enemies into downloading pictures with hidden viruses. FireEye experts identified this group as acting out of Lebanon, which may indicate that it is the work of the leading Lebanese cyber power and known Iranian proxy, Hezbollah[126].

Iran-Israeli proxy conflicts

Table 14: Iran-Israeli proxy conflict, Iran

Allied combatants/supporters	*Actor type*	*Enemy combatants/supporters*	*Actor type*
Iran	Middle state	Israel	Middle state
Hezbollah	Non-state	United States	Large state
Hamas	Non-state		

Hamas

In the Gaza Strip, militant organization Hamas operates with support from Iran. This is a facet of its support of the Palestinians. In 2014, fighting between Israel and Hamas increased, culminating in another war, the 2014 Gaza Strip War. After attacks by Hamas, the IDF launched a full campaign in the Gaza Strip, with troops on the ground in July 17th, 2014. The war ended on August 26th, 2014, after over 2,000 Palestinian deaths and under 100 Israeli deaths[127].

Immediately prior to the conflict in early July, the IDF twitter account was hacked and sent out a tweet stating that two Hamas rockets hit an Israeli nuclear reactor and caused a leak. The hack was quickly noticed and removed[128].

Over the course of the conflict, Iranian hackers launched significant attacks against the Israeli internet infrastructure. These attacks were largely blocked, but they intended to block Israeli internet access on the end of Ramadan, a religious holiday, which in 2014 ended on July 28th, or almost two weeks after the advent of the conflict. An Israeli official reported that it was "a very intense cyber effort", that was "unlike any we had seen before"[129]. This report from *Politico* and similar news reports came on August 17th. Notably, days after this report, on August 19th, Hamas violated a ceasefire that had lasted over a week, firing 29 rockets[130]. While, as always, there are issues of attribution, many cyber experts suspect Iran's involvement in the more sophisticated hacks that came alongside this conflict[131].

Despite Iran's extensive use of cyber proxies, there appears to have been no cyber proliferation to Hamas, or at least, much less than to other Iranian military proxies. While Hamas has exhibited some cyber capability, IDF and cyber experts emphasize that their "cyber unit is nowhere near the level of state actors like Iran". This may derive from a lesser trust in the alignment of Hamas interests with Iran. In 2009, Iran expert said "Hamas is certainly not an Iranian puppet"[132]. Hamas, since the Arab Spring in 2011, has exhibited increasing departure from Iranian interests. This includes a better relationship with Iranian rivals in Cairo, disputes

with Hezbollah, and the inherent religious difference - Hamas is a Sunni Muslim group, while Iran and most of its proxies are primarily Shia[133].

That said, one element of note is the fact that Hamas has increased its cyber capability independent of Iranian assistance. An espionage malware called Pierogi discovered in 2019 was assessed by Israeli researchers which, based on its use of the Ukrainian language, determined that it was obtained by Hamas via the dark web[134].

While it may be difficult to discern the source of any given instance of cyber proliferation, one can consider and compare the different cyber capabilities of given groups at different times, and consider the context of geopolitics and their relationship with patron states. With Hamas, while in the latter half of the 2010s their sophistication increased, their cyber capabilities remained primitive or stagnant during the same time that closer Iranian proxies' cyber capabilities flourished[135]. Additionally, since then, their relationship with Iran has only deteriorated due to political differences. Due to that, it may be that their increased cyber capability derives from their own development and not Iran's intervention.

Hezbollah

Hezbollah is one of the largest Iranian proxies in the region, and primarily operates in Lebanon, north of Israel. They have engaged in several skirmishes with Israel, the largest being the month-long 2006 Lebanese War.

Hezbollah undertook cyberattacks as part of their war effort. In Israel's allies across the world, Hezbollah attacked websites and spread propaganda[136]. Not only was this a means of

spreading propaganda, but it was a means of crowdfunding as well. The hijacking of legitimate websites included the creation of channels on those websites for financial donations to be made directly to Hezbollah.

Iran's cyber support to Hezbollah is both direct and foundational. From its conception, Iran has provided Hezbollah with tremendous material and financial support, some of which has come in the form of technical expertise. This is the form of foundational support - rather than needing direct training or advisement, Hezbollah has grown to be self-sufficient in technical expertise. This includes the creation of a sophisticated communications network within Lebanon, which Hezbollah has later used to bolster its cyber capabilities[137].

In 2015, Hezbollah's greatly improved cyber capabilities manifested in their deployment of "Volatile Cedar", a persistent cyber campaign aimed at espionage, primarily targeting Israeli defenses[138]. This was considered to be more sophisticated than Hezbollah's prior cyber operations, indicating either internal development or further assistance from Iran.

Iran

Stuxnet may have kicked off the full-scale "cyber war" between Iran and Israel. Perhaps as a direct response, in September 2012, Iranian hackers conducted a DDOS attack agianst U.S. banks, in an effort anmed Operation Ababil. This blocked access to major U.S. financial institutions, which allegedly "cost Western firms millions in lost business"[139].

Iran has engaged in extensive cyber espionage against Israel, as well. The Iran-linked cyber group dubbed by researchers as CopyKittens is known to target Israel. In recent years,

Iranian cyberattacks on Israel have grown more severe. 2020 consisted of a series of kinetic cyberattack exchanges between Iran and Israel. In April 2020, Iran conducted a cyberattack aimed at sabotaging the Israeli water system, which was thwarted by Israeli defense. According to Israeli cyber chief Yigal Unna, the attack could have caused chemicals to mix into the country's water source, causing a "harmful and disastrous outcome"[140]. This was met by retaliation in the form of an Israeli cyberattack on an Iranian port, disrupting logistics temporarily.

More water infrastructure attacks came in July, on small rural sectors, which allegedly were simple to fix, being "immediately and independently repaired by the locals, causing no harm"[141]

Over June and July of 2020, a series of explosions occurred across Iran on various infrastructure, though most notably, the Natanz nuclear facility, which was also the target of Stuxnet. The source is unconfirmed, though several intelligence officials internationally state that Israel was behind the attacks. It is unknown whether these attacks were cyber-enabled or a form of traditional sabotage.

Iran vowed to "respond" if these explosions turned out to be the result of a cyberattack. However, no significant response has yet been made. Other international intelligence officials doubt it was a cyberattack. Indeed, it is very possible this was conventional sabotage - Israel is known to have agents implanted within Iran[142].

In December 2020, security firm Otorio reported a hacking group named “Unidentified TEAM” published a video showing their access to an Israeli water reservoir control system. The group stated that their hack was a response to the November assassination of Iranian nuclear scientist Mohsen Fakhrizadeh, which Iran blamed Israel for. Unlike earlier attacks, there appeared to be no attempt to cause harm - merely demonstrating the access[143].

Considering the reported motivation of the December attacks, and the cyber-escalation beginning shortly after the assassination of major Iranian figure Qassem Soleimani, it may be that the initial infrastructure attacks, which were also the most significant, were a response to that. Iran, earlier in January 2020, had engaged in light hacking as a response to the assassination of Soleimani, primarily website defacement and propaganda spreading on U.S. sites, but their primary response was conventional. The attempted April hack of water systems may represent their true cyber response.

It is unlikely that the attacks in June and July were cyberattacks - if they were, it would be the most destructive instance of cyber sabotage in history and change the landscape of cyberwarfare permanently, if not warrant severe retaliation from Iran, as they threatened. Not only that, but it would represent a significant escalation by Israel, from their prior cyberattack which only hindered a port’s logistics. The infrastructure cyberattacks between Iran and Israel appear to have simmered down - this may be due to the fact that the U.S. election was approaching, and the potential of a Biden administration could mean the U.S. rejoining the

JCPOA, something that Iran would not want to jeopardize by escalating a cyberwar with a U.S. ally.

However, a similar attack came later, one which Israeli officials suggest was a cyber attack. On April 10th, 2021, Iranian president Rouhani made a public broadcast in which he unveiled new centrifuges at the Natanz nuclear site. The day after, a sabotage occurred on Natanz's power network. The consequences of this sabotage are unknown. Several Israeli media outlets report that their intelligence sources claim this sabotage was the result of a cyber operation[144].

While a cyberattack would represent an escalation, Israel considers Iranian nuclear capability an existential threat, and the attack came on the heels on a public announcement of Iran's progress in nuclear development, so drastic measures are certainly expected. Additionally, given Iran's previous vows of retaliation against cyber activity, their failed 2020 cyber operations against Israel, and the intentional claim of cyber activity by Israel, this may be an instance of Israel "testing the waters" of Iranian cyber capability. Should Iran make good on their claim and launch a significant cyberattack, Israel will obtain a better idea of their capabilities. Regardless of the outcome, this may indicate an escalation in the fledgling Iran-Israeli cyber war. If Iran launches a strong cyber attack, it may kick off increasing cyber hostilities. If they do not, Israel may take that as an indication that they do not have extensive cyber power, and feel open to use cyber methods more liberally against Iran, less fearful of retaliation.

Conclusions

Iran conforms to the posed hypothesis. The hybrid nature with which it considers how to wage war is great, and so is its implementation of cyber methods. That said, their cyber focus was greatly catalyzed as a response to Stuxnet.

As in their way of waging war, Iran exerts cyber influence largely through "arming" proxies with cyber capability. A notable finding is the care they seemingly take in disseminating cyber power compared to their proliferation of conventional arms. Where the power of a conventional weapon Iran supplies will not vary whether it is supplying to a highly loyal proxy, like Hezbollah, versus a more tentative proxy, like Hamas, the power of cyber capabilities disseminated will. This is likely due to the lack of control that can be exerted over cyber capability. Conventional arms are easier to manage - if Iran supplies a certain number of rockets, then they can know that the group can only use that amount of rockets. Cyber attacks, on the other hand, are unlimited, and easier deployed, unrestrained by physicality. By varying the power of cyber capabilities they disseminate to their proxies based on the group's attitudes and loyalty, Iran can achieve a number of safety measures - prevent the cyberweapons from ever being turned back on Iran or Iranian allies, or being turned on a more powerful enemy which would lead to greater retaliation against Iran, should it be traced back. Conventional proliferation can be curated and restrained by limited quantity and geographic considerations. Cyber proliferation cannot be restrained in the same way. Thus, while Iran continues their trend of proxy war, it does so in a more cautious, limited manner.

Iran is liberal in their use of cyber methods even in conflicts where great powers are involved, such as the Syrian war. However, they have never directly made an aggressive, offensive cyberattack on a large power - not beyond mere espionage, information, and economic warfare. The same cannot be said of the regional middle power it conducts attacks against. Iran has been known to conduct kinetic cyberattacks on both Israel and Saudi Arabia, attacking infrastructure or industry. Their cyber action against these two states is commensurate with their regional aggression. Additionally, quite often Iran uses cyber methods as a retaliatory means, where conventional retaliation may not be available to them. They also exhibit relatively high proliferative restraint with cyber means. Should they proliferate more powerful attacks to a radical group, if that group were to use it against the U.S., that may warrant retaliation against Iran and thus lead to losses for it.

CHAPTER FIVE: CONCLUSION

Hypothesis Results

In conclusion, the hypothesis has proved to be true. There appears to be a strong link between a strategic culture's attitude toward hybrid warfare and its engagement in cyber methods parallel to conventional warfare - the U.S., appearing to have a strategic culture not as ingratiated towards the use of hybrid warfare, demonstrates a lesser amount of usage of cyber methods in the conventional conflicts of the 21st century, compared to Iran and Russia.

Strategic culture exerts strong influence not only on the quantity of cyber usage, but in its quality as well. A strategic culture's attitude toward the nature of war appears to be able to determine the particular way in which they engage in cyber methods, relative to other states.

The Russians, with a long history of considering information warfare an integral part of war, tend to utilize cyber methods that concern information and public opinion. For them, politics are as much a battlefield as conventional war itself, and they use cyberwarfare in both. The Russian view of war is that it is fought on multiple strategic planes, much beyond the conventional. They utilize cyber methods accordingly - broad in scope and target, Russian cyber methods quite often fulfill multiple goals in a single effort.

The Americans, without so much concern for a multi-dimensional concept of war, tend to utilize cyber methods that are more tactical in nature, focusing on military or kinetic targets and using it as a more direct disruption to conventional movements. The U.S. has engaged in broader, strategic cyber operations essential to conflicts - their use of Stuxnet, particularly - but even this

betrays how deeply strategic culture is ingrained in their usage of cyberwarfare. Stuxnet was focused on a single, strategic target with a single strategic goal - the sabotage of the Iranian nuclear efforts. This is in line with the American principle of "precision strike" that is essential to modern conventional war efforts.

The U.S. has made minimal efforts indicative of a multi-dimensional view of conflict - their information campaign against ISIS, notably - but these are marred. Even disregarding poor execution of these campaigns, there is a structural incongruence. American social media cyber campaigns are overt (openly coming from the government) and most efforts have been from the State Department or non-government entities. There appears to be little collaboration in offensive information warfare with the military or intelligence. This is compared with Russian information campaigns, which are covert and are well-integrated with the efforts of military and intelligence services.

Iran's particular form of hybrid warfare informs their cyber strategy, as well. The Iranians, forced into proxy warfare by their unique circumstances, demonstrate significant use of cyber proliferation, despite those unique circumstances not necessitating cyber proxies. Their state being born out of modern revolution, they understand the power of culture and information, and demonstrate that in their cyber usage.

Table 15: Cyber methods, conflicts, and threat levels

		Usage of conflict-parallel cyber methods, by area						
		Tactical	Economic	Espionage	Information	Kinetic	Proliferation	Threat level
U.S.	Iraq war 2003-2011	Yes	Yes	Yes	No	No	No	Small
	Afghanistan	Yes	No	No	Yes	Yes	No	Non-state
	Syrian civil war	No	No	No	No	No	Partly	Large
	War on ISIS	Yes	Yes	Yes	Partly	Yes	No	Non-state
	Iranian proxy conflicts	No	Yes	Yes	No	Yes	No	Middle
Russia	2008 Russo-Georgian War	Yes	Yes	Yes	Yes	Yes	No	Small
	2014 Russo-Ukrainian war	Yes	Yes	Yes	Yes	Yes	No	Middle
	Syrian civil war	No	No	Yes	Yes	No	No	Large
Iran	Iran-Israel proxy conflict	Yes	Yes	Yes	Yes	No	Yes	Middle
	Iran-Saudi Arabia proxy conflict	Yes	Yes	Yes	Yes	No	Yes	Middle
	War on ISIS	No	No	No	Yes	No	No	Non-state
	Syrian civil war	Yes	No	Yes	Yes	No	Yes	Large

The chart above provides a broad look at threat level, cyber action, and how they intertwine. As seen, the smaller the threat level of the target, the greater the variety of cyber methods employed. This also varies across states - Russia tends to be slightly bolder than the U.S. in offensive cyber usage, whereas Iran is bolder than both. While there is disparity between how these three states act towards different threat levels, there appears to be a consistent maintenance of strategic action that minimizes the risk of retaliation or escalation. When the threat level changes, there is greater threat of retaliation. The U.S. exhibits great restraint when dealing with the higher cyber threat level of large states, while using it very liberally in conflicts with small powers and non-state actors. Russia and Iran do not decrease the extent of their cyber usage with threat level, but rather the way in which it is delivered, or the severity of it. For Russia, this means the switch to cyber support in soft power struggle. In fighting the U.S., as opposed to the tactical and kinetic attacks in Georgia and Ukraine, Russia utilized cyber-enabled information and political warfare. Due to their covert and soft power nature, the Russian cyber operations that aimed to help its strategic standing in Syria were less likely to provoke retaliation than the more aggressive cyberattacks of its prior wars. Iran also strives towards this in its cyber methods, though it is less averse to escalation or retaliation than the great powers. Iran strives toward a non-escalatory conflict using its many proxies - by both proliferating cyber methods to non-state actors and employing preexisting cyber groups, Iran acts covertly and attempts to evade responsibility and thus retaliation.

Iran's use of kinetic cyber methods may represent a disparity with this trend. However, the context of these kinetic cyber attacks are notable. For Israel in particular, they represent retaliation commensurate with an attack by Israel, like the assassination of key Iranian figures. Any observed difference in the amount of cyber usage across threat levels could be accounted for by the breadth of cyber methods employed by a state. A state that knows how to effectively use cyber methods to convey soft power - of information, political, espionage, economic, or other influence - will be better equipped to act offensively against their rivals using their cyber capabilities. This is due to the fact that these soft power aspects are inherently less escalatory than more "hard power" cyber methods - such as tactical, sabotage, or kinetic attacks. So a state such as the U.S., that favors hard power offensive cyber methods, will be less equipped to fight higher threat levels. There is also varying escalatory nature across soft power methods - U.S. has used economic cyberattacks against Iran, but not Russia. Whereas states such as Russia or Iran, which utilize both soft and hard cyber methods, can selectively change their cyber methods in accordance with the threat. That is not to say the U.S. does not take cyber action against large states - it certainly does. But the key distinction is the offensive and strategically consequential nature of the cyber methods deployed. While the U.S. has extensively used cyberespionage, or demonstrations to show their capability or pose threat, such as energy systems penetrations, when it comes to *active, offensive* cyber measures, whether soft or hard, they are lacking. What is evident is that the diversity of a state's cyber methods can dictate its efficacy in cyber offense across all threat levels.

Another evident factor is the disparity between tactical and strategic cyber methods. In reference to the above chart, every cyber method listed that is not "tactical" can be considered strategic. A state can exhibit high usage of tactical cyber methods, but low usage of strategic ones, such as with the United States. On the other hand, a state can exhibit low usage of tactical cyber methods, but high usage of strategic ones, such as with Iran (though this is likely more so due to the lack of direct conflicts). This may be a notable explanatory factor - the U.S., the state with the lowest degree of hybrid warfare, exhibited low usage of strategic cyber methods, whereas Russia and Iran, with high degrees of hybrid warfare, exhibited high usage of strategic cyber methods. All of the states that directly engaged in combat exhibited usage of tactical cyber methods.

Moreover, there is a notable link between organizational structure of a state's warmaking institutions and its usage of cyber methods. It appears, upon closer inspection, that cyber usage is strongly a function of organizations. There is sometimes great disparity in hybrid warfare usage across different organizations within a government - such as the RAF and FSB, or the IRGC and Iranian army. From this a distinction emerges - conventional militaries, the obvious foremost warmaking component of any state, will tend towards conventionality. A state will be more likely to engage in offensive, strategic cyber methods if it has warmaking institutions that are traditionally non-conventional. Russia, their intelligence services having always been a facet of war efforts, and having always exhibited hybrid methods, will thus be more likely to use strategic cyber methods. The same goes for Iran, whose IRGC is highly hybrid in nature. The

U.S., whose efforts in hybrid warfare by its own intelligence services are marred and incongruent with military campaigns, are less likely to use strategic cyber methods. The tactical usage of cyber methods by the U.S. comes from the cyber capabilities of the conventional military. The primary wing of U.S. cyber capability, U.S. Cyber Command, is a part of the military, and more beholden to its organizational culture of conventionality. This is in contrast with the cyber dominant organizations of Russia and Iran, the FSB (and ancillary groups) and the IRGC, who have more hybrid organizational cultures, and thus lend themselves towards more strategic use of offensive cyber methods.

Through organizational culture, strategic culture can be linked to usage of strategic cyber methods. The aforementioned organizational cultures formed within a strategic cultural context, and are beholden to it. The IRGC was borne of radical revolution and had the potential to form itself towards the necessities of the 1979 global context, as well as having great liberty in forming the fledgling strategy. The same is true for the roots of the FSB - its predecessors and their government, the Soviet Union, were formed in the 1917 October Revolution. The United States, on the other hand, has a much older strategic culture, and is not only more rigid towards change but was formed and designed in a context more radically different from the modern era than the 20th century is. The long-standing strategic culture may affect these organizational cultures, and thus a state's usage of cyber methods.

Other Conclusions

Strategic deficiency, or moral constraint?

The natural question raised when one considers the lack of use of a particular cyber method is: is it really a strategic deficiency? Or do some states simply have different moral constraints? Certainly, there are some cyberattacks that should never be undertaken - such as attacks on energy grids that threaten civilian lives. But the more ambiguous question comes in a consideration of information warfare. A lynchpin of Russia's cyber strategy and nearly defunct in the U.S., there may be some who question if, as this paper poses, the lack of cyber-enabled information warfare by the U.S. is a strategic deficiency. or if it is simply a moral choice.

Information warfare is commonly associated with both information suppression or misinformation. Russia spreads confusion and misleads populations with their information warfare. Cyber jihadists spread radical messages to recruit for their ranks. Often, these lies come with ethically abhorrent consequences - a fabricated mistrust between demographic groups, or the endangerment of young militants who have been radicalized towards violence.

However, information warfare concerns nothing more than the spread of information, whether fact or falsehood. While certainly, there is an American ethical constraint against spreading direct lies, it does not need to. If the truth has any power, and if an operation is justified then it should, then it can influence the minds of people. The war of propaganda goes both ways - truth can be used as propaganda just as effectively as falsehood. Those people could include, for example, the pro-Assad Syrian forces. If a U.S.-taught FSA could use cyber-enabled

information warfare, they could reach lines of information dissemination used by either current pro-Assad fighters or potential ones, and imbue those lines of communication with anti-Assad propaganda. The word propaganda has negative connotations, but it need not necessarily be false information. After all, the official stance of the Assad administration is that it has not used chemical weapons, accusing rebels of faking attacks for international sympathy. Considering that, it is likely the view of low-level pro-Assad fighting forces that he has not used chemical weapons. If Americans were to inundate lines of Syrian digital communication with evidence about Assad's use of chemical weapons, that would be a form of factual information warfare, and may influence the beliefs of some combatants.

There have been some efforts towards this, by the State Department in combating ISIS indoctrination, but they were at best misguided and ineffective and at worst detrimental. A fundamental problem in information operations is the source. People are inherently more mistrustful of information coming from an officially state-sanctioned source, as State Department used, as such a source has an inherent presumed ulterior motive. Whereas in other states' information operations, the information is disseminated through a mass number of bots posing as real people. This fosters the idea that a large amount of real people hold a given perspective, and thus makes actual people more receptive to it. The American ethical perspective would be to scoff at the use of bots posing as real people, but that may be one of the only methods to truly wage information warfare on a high level. This may be an indication that the relative lack of American information operations is a moral constraint against the use of bots.

Regardless of the reason, it is clear that there is more the U.S. could do in information warfare, or at the least more discourse to be had. Of course, there are operational concerns. Convincing a radicalized force of a reality that they believe to be false is a monumental task. That said, it is not impossible. The U.S. has not engaged in information warfare to the extent of their rivals, nor have they attempted to.

Decreased Proliferation

A notable finding is the disparity between past proliferative strategies and cyber proliferation. The U.S., Russia, and Iran have all engaged in extensive proliferation and proxy methods, albeit in different ways. However, there is a marked decrease in their cyber proliferation methods to allied groups in conflicts. Russia does not engage in definitive cyber proliferation to any conventional militant groups. The U.S. has dabbled in technical support to Syrian rebels, but it does not appear to be extensive. Iran, commensurate with its use of proxy warfare, demonstrates the most proliferation, but even its proliferation is greatly lessened compared to the conventional support it offers.

There are a few possible explanations for this. One is that the nature of cyber methods make them difficult to constrain, and so states are less inclined to give them away. Unlike conventional aid - finite, makes for easy bookkeeping, and more restrained by logistics and geography - cyber aid has the potential for unlimited, international use. Militant groups, often unreliable and unpredictable, may in time turn these cyberweapons against the proliferator's allies or even the proliferator itself.

The second is that it may be redundant to offer cyber aid to these groups, when there are pre-existing hacker groups to collaborate with, making for an easier process. An example of this is Russia's collaboration with the Russian Business Network. It is simpler to contract out cyber work rather than teach it to inexperienced militants. However, it may be more costly, and there may be benefits the militants have by the essence of their regionality. The truth is likely a mix of these two explanations.

Implications for Strategic Culture Theory

Perhaps the most significant takeaway from the results of this hypothesis is the relationship between technological development and application and strategic culture theory. As mentioned, there appears to be no link between a strategic culture's attitude towards the nature of war and the quantity of use of cyber methods.

Many modern scholars and public figures suggest that cyber is a new form of warfare, entirely novel and misunderstood. But what is evident is that cyber is not a "new form of warfare", but rather, a new means of waging it. The way in which war is waged is beholden to strategic culture, not to technology.

While this paper concerned the effect of strategic culture on cyberstrategy, it has more general implications for technological usage. A state will use any novel technology to the fullest extent, but they will do so in their own distinct way. American cyberwarfare is distinct from Russian cyberwarfare, though they engage in both to the extent of their capability. This conclusion, though left unstated in strategic culture scholarship, hearkens back to its very origins.

The U.S. and the USSR, strategically distinct, had comparable development of nuclear weapons. And while, unlike cyber methods, their application of nuclear weapons was comparable as well, it was the result of very different reasonings.

Though one may expect new technologies and the amount of their usage in conventional war to be beholden to the rigidity of a strategic culture's perception of war, this has proven untrue. What *is* beholden to the perceived nature of war is the way in which technology is used. We have seen this in the cases of nuclear weaponry, precision strike technology, and cyber methods.

This will likely hold true for future technologies, as well. We may see this come to fruition with artificial intelligence capabilities, an emergent technology with broad application. From this, one might expect the governments' national security application of AI to vary - the U.S. to focus on a tactical advantage on the battlefield, Russia to focus on opinion analysis and information warfare.

While the applications of any novel technology and its effects on international relations can be hard to predict, these findings reinforce the idea that technology does not revolutionize warfare, or introduce a new kind of warfare, it merely amplifies different aspects of it. Indeed, informational warfare did not come about with the advent of the Internet. Espionage did not come about with the advent of hacking capabilities. These aspects of war have been constant throughout human history, though they manifest in different ways, whether it be leaflets dropping

over Europe in 1942, or medieval-era espionage. Technology can change it, make aspects more or less important, but it would be a misnomer to name any technology a “new” form of warfare.

REFERENCES

1. Snyder, J. (1977). The Soviet Strategic Culture: Implications for Limited Nuclear Operations. *RAND.* https://www.rand.org/content/dam/rand/pubs/reports/2005/R2154.pdf
2. Johnston, A. (1995). Thinking about Strategic Culture. *International Security* (pp. 36-37) https://www.jstor.org/stable/2539119
3. Ibid.
4. Johnston, p. 40
5. Klein, B. (1988). Hegemony and Strategic Culture: American Power Projection and Alliance Defence Politics. *Review of International Studies.* http://www.jstor.org/stable/20097137
6. Johnston, pp. 41-42
7. Ibid p. 46
8. Ibid.
9. Gray, C. (1999). Strategic Culture as Context: The First Generation of Theory Strikes Back. *Review of International Studies* http://www.jstor.org/stable/20097575
10. Ibid.
11. Ibid.
12. Hobbes, Thomas, 1588-1679. (1968). Leviathan. *Penguin Books.*

13. Clausewitz, C. ., Howard, M., Paret, P., & Brodie, B. (1984). *On war*. Princeton University Press

14. U.S. Government Accountability Office (2010). Briefing on hybrid warfare. *Committee on Armed Services, House of Representatives.* https://web.archive.org/web/20110923072600/http://www.gao.gov/new.items/d101036r.pdf

15. Botero, G. ., Birely, R. (2017) The Reason of State. *Cambridge University Press.*

16. Hargrove, Paul (2016). Roots of Russian Irregular Warfare. *Naval Postgraduate School*. https://calhoun.nps.edu/handle/10945/51715

17. Reuveny, R. Aseem, P. (1999). The Afghanistan war and the breakdown of the Soviet Union. *Review of International Studies.* http://faculty.washington.edu/aseem/afganwar.pdf

18. Ermarth, Fritz. (2006). "RUSSIA'S STRATEGIC CULTURE: PAST, PRESENT, AND… IN TRANSITION?" Defense Threat Reduction Agency. https://fas.org/irp/agency/dod/dtra/russia.pdf

19. Ibid.

20. Pain, Emil. (2001). From the First Chechen War Towards the Second. *The Brown Journal of World Affairs*, 8(1), 7-19. http://www.jstor.org/stable/24590171

21. Ibid.

22. Ibid.

23. CNN (1999) Russia acknowledges bombing raids in Chechnya. *CNN*. https://web.archive.org/web/20000919000313/http://www.cnn.com/WORLD/europe/9908/26/russia.chechnya/

24. Cockburn, P. (1999) Russian warplanes kill dozens of villagers. *The Independent*. https://web.archive.org/web/20080115001724/http://findarticles.com/p/articles/mi_qn4158/is_19991011/ai_n14278495

25. https://fas.org/nuke/guide/russia/agency/Felg.htm

26. Martti J. Kari & Katri Pynnöniemi (2019) Theory of strategic culture: An analytical framework for Russian cyber threat perception, Journal of Strategic Studies, https://www.tandfonline.com/doi/abs/10.1080/01402390.2019.1663411

27. Aron, Leon. (2008). "The Problematic Pages." The New Republic, newrepublic.com/article/62070/the-problematic-pages.

28. Gerasimov, Valeri, (2013) 'The value of science in anticipation. New challenges require rethinking the forms and methods of conducting military operations', Voenno-Promyshlennyi Kurier (in Russian). https://www.vpk-news.ru/articles/14632

29. Nato, Warsaw, (2016) 'Summit Communiqué of the North Atlantic Council in Warsaw', https://www.nato.int/cps/en/natohq/official_texts_133169.htm and MoD, Military Doctrine of the Russian Federation (2014). https://rg.ru/2014/12/30/doktrina-dok.html.

30. Jonsson, O. (2019). The Russian Understanidng of War: Blurring the Lines Between War and Peace. Georgetown University Press.

31. Keizer, Gregg. “Cyberattacks Knock out Georgia's Internet Presence.” Computerworld, Computerworld, 11 Aug. 2008, www.computerworld.com/article/2532289/cyberattacks-knock-out-georgia-s-internet-presence.html.

32. Goodman, W. (2010). Cyber Deterrence: Tougher in Theory than in Practice? Strategic Studies Quarterly, 4(3), 102-135. Retrieved November 17, 2020, from http://www.jstor.org/stable/26269789

33. Barnard, Anne. (2008) “Georgia and Russia Nearing All-Out War.” The New York Times, The New York Times www.nytimes.com/2008/08/10/world/europe/10georgia.html.

34. The World Bank. Individuals using the Internet (% of population) - Georgia. *World Bank.* https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=GE

35. Conklin, B. (2019). Cybersecurity: The Geospatial Edge. ESRI https://www.esri.com/about/newsroom/blog/german-cybersecurity-experts-use-gis/

36. Satter, Raphael. “Ukraine Soldiers Bombarded by 'Pinpoint Propaganda' Texts.” AP NEWS, Associated Press, 11 May 2017, apnews.com/article/9a564a5f64e847d1a50938035ea64b8f

37. Meyers, Adam, et al. “Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units.” CrowdStrike, 29 Mar. 2019,

www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.

38. Ibid.

39. Siboni, Gabi, and Zvi Magen. The Cyber Attack on the Ukrainian Electrical Infrastructure: Another Warning. Institute for National Security Studies, 2016, www.jstor.org/stable/resrep08283.

40. Ibid.

41. Baezner, M., Robin, P. (2017). The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict. Center for Security Studies. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-05.pdf

42. Apps, P., (2012). Disinformation flies in Syria's growing cyber war. Reuters https://www.reuters.com/article/us-syria-crisis-hacking/disinformation-flies-in-syrias-growing-cyber-war-idUSBRE8760GI20120807

43. Baezner.

44. Ibid.

45. Harding, L. Arthur, C. (2013) Syrian Electronic Army: Assad''S cyber warriors. The Guardian. https://www.theguardian.com/technology/2013/apr/29/hacking-guardian-syria-background

46. Rutherford, E. (2013). Experts assess Syrian Hackers' capabilities. NTI https://www.nti.org/gsn/article/experts-assess-syrian-hackers-targeting-government-sites/

47. GALANTE, LAURA, and SHAUN EE. (2018) Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents. Atlantic Council www.jstor.org/stable/resrep20718.

48. U.S. Senate. (2017). SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf

49. Strohm, C. (2016). “FBI Investigating DNC Hack Some Democrats Blame on Russia.” Bloomberg.com, Bloomberg, www.bloomberg.com/news/articles/2016-07-25/fbi-investigating-dnc-cyber-hack-some-democrats-blame-on-russia.

50. Holland, S. (2016). Exclusive: Trump says Clinton policy on Syria would lead to World War Three. Reuters https://www.reuters.com/article/us-usa-election-trump-exclusive/exclusive-trump-says-clinton-policy-on-syria-would-lead-to-world-war-three-idUSKCN12P2PZ

51. Croft, A., & Vey, J. (2017). French presidential front-runner Macron urges military intervention in Syria. Reuters

52. Ganley, A., Rosa, A. (2017). French far-right chief says Assad is solution to Syrian crisis. Times of Israel https://www.timesofisrael.com/french-far-right-chief-says-assad-solution-to-syrian-crisis/

53. Vilmer, J., & Conley, H. (2018). (Rep.). Center for Strategic and International Studies (CSIS). doi:10.2307/resrep22297

54. Mackinnon, A. (2020). 4 key takeaways from the British report on Russian interference. Foreign Policy https://foreignpolicy.com/2020/07/21/britain-report-russian-interference-brexit/

55. Galante, L., Lee, S. (2018) Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber enabled incidents. Atlantic Council https://www.atlanticcouncil.org/wp-content/uploads/2018/09/Defining_Russian_Election_Interference_web.pdf

56. The Syria Campaign. (n.d.) Killing the Truth. *The Syria Campaign.* https://thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf

57. Alami, Mona. (2018). Russia's disinformation campaign has changed how we see Syria. *Atlantic Council.* https://www.atlanticcouncil.org/blogs/syriasource/russia-s-disinformation-campaign-has-changed-how-we-see-syria/

58. Baezner op. Cit.

59. Baker, P. (2018). White House penalizes Russians over election meddling and cyberattacks. *New York Times.* https://www.nytimes.com/2018/03/15/us/politics/trump-russia-sanctions.html

60. Gray, C. (2005). Another Bloody Century. *Phoenix Press*.

61. Cleveland, C. (2020). The American Way of Irregular War: An Analytical Memoir. *RAND Corporation.* https://www.rand.org/content/dam/rand/pubs/perspectives/PEA300/PEA301-1/RAND_PEA301-1.pdf

62. Fowler, C. (2014). Forgetting Lessons Learned: The United States Army's Inability to Embrace Irregular Warfare. *Air University*. https://apps.dtic.mil/dtic/tr/fulltext/u2/1023604.pdf

63. Ibid.

64. Greentree, T. (2015). America Did Hybrid Warfare Too. *War on the Rocks.* https://warontherocks.com/2015/04/america-did-hybrid-warfare-too/

65. Watts, B. (2013). The Evolution of Precision Strike. Center for Strategic and Budgetary Assessments. https://csbaonline.org/uploads/documents/Evolution-of-Precision-Strike-final-v15.pdf

66. Citino, R. (2004). Blitzkreig to Desert Storm.

67. Gray, C. (2006) Irregular Enemies and the Essence of Strategy: Can the American Way of War Adapt?

68. Fowler op. cit

69. White House. (2010) National Security Strategy

70. Eisenstadt, M. (2015) The Strategic Culture of the Islamic Republic of Iran. *Washington Institute.* https://www.washingtoninstitute.org/policy-analysis/strategic-culture-islamic-republic-iran-religion-expediency-and-soft-power-era

71. Sanger, D. (2016). U.S. Cyberattacks Target ISIS in a New Line of Combat. *The New York Times.* https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=0

72. White House. (2018). National Defense Strategy

73. Clark, C. (2016). CJCS Dunford Calls For Strategic Shifts; 'At Peace Or At War is Insufficient'. *Breaking Defense.* https://breakingdefense.com/2016/09/cjcs-dunford-calls-for-strategic-shifts-at-peace-or-at-war-is-insufficient/

74. Morris, L. (2019). Gaining Competitive Advantage in the Gray Zone. *RAND*. https://www.rand.org/pubs/research_reports/RR2942.html

75. Markham, J., Shanker, T. (2009). Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk. *The New York Times.* https://www.nytimes.com/2009/08/02/us/politics/02cyber.html

76. Smith, Charles R. (2003) "Cyber War Against Iraq." NewsMax.com

77. Markham op. Cit.

78. Smith op. cit.

79. Associated Press. (2012). U.S. general: We hacked the enemy in Afghanistan. *Politico.* https://www.politico.com/story/2012/08/us-general-we-hacked-the-enemy-in-afghanistan-080098

80. The World Bank. Individuals using the Internet (% of population) - Afghanistan. *World Bank.* https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=AF

81. State. (2013). Department of State, "U.S. Government Assistance to Syria— Fact Sheet,"

82. Grohe, E. (2015). The Cyber Dimensions of the Syrian Civil War. *Johns Hopkins.* https://www.jhuapl.edu/Content/documents/TheCyberDimensionsoftheSyrianCivilWar.pdf

83. Sanger, D. (2016). U.S. Cyberattacks Target ISIS in a New Line of Combat. *The New York Times.* https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=0

84. Miller, G., Higham, S. (2015). In a propaganda war against ISIS, the U.S. tried to play by the enemy's rules. *The Washington Post.* https://www.washingtonpost.com/world/national-security/in-a-propaganda-war-us-tried-t

o-play-by-the-enemys-rules/2015/05/08/6eb6b732-e52f-11e4-81ea-0649268f729e_story.html

85. Ibid.

86. Speckhard, A., & Ellenberg, M. (2020). Breaking the ISIS Brand Counter Narrative Facebook Campaigns in Europe. Journal of Strategic Security, 13(3), 120-148. doi:10.2307/26936548 https://www.jstor.org/stable/26936548

87. Sanger, D. (2014). Syria War Stirs New U.S. Debate on Cyberattacks. *The New York Times.* https://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html

88. Temple-Raston, D. (2019). How The U.S. Hacked ISIS. *NPR.* https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis

89. Martinez, L. (2015). US Drops Anti-ISIS Leaflets Over Syria. *ABC News.* https://abcnews.go.com/Politics/us-drops-anti-isis-leaflets-syria/story?id=29930980

90. Zetter, K. (2014). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. *Wired.* https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

91. Sullivan, B. (2020). Iran-USA Cyberwar Has a Long History. *SecureWorldExpo.* https://www.secureworldexpo.com/industry-news/iran-usa-cyberwar-history

92. Hanna, A. (2019) The Invisible U.S.-Iran Cyber War. *United States Institute of Peace*. https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war

93. Ali, I., Stewart, P. (2019). Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials. *Reuters.* https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-idUSKBN1WV0EK

94. Stanley, W. (2006). The Strategic Culture of the Islamic Republic of Iran. Defense Threat Reduction Agency. https://fas.org/irp/agency/dod/dtra/iran.pdf

95. Ibid.

96. Fixler, A., Cilluffo, F. (2018). Iran's USe of Cyber-enabled Economic Warfare. Foundation for Defense of Democracies. https://www.fdd.org/wp-content/uploads/2018/11/REPORT_IranCEEW.pdf

97. Ibid.

98. Dagler, M. (2020). The Iranian Islamic Revolutionary Guard Corps from an Iraq View - a Lost Role or a Bright Future? Center for Strategic and International Studies. https://www.csis.org/analysis/iranian-islamic-revolutionary-guard-corps-irgc-iraqi-view-%E2%80%93-lost-role-or-bright-future

99. Wehrey, F., Thaler, D., Bensahel, N., Cragin, K., Green, J., Kaye, D., . . . Li, J. (2009). Asymmetric Ambition and Conventional Reality: Iran's Evolving Defense Strategy, Doctrine, and Capabilities. RAND Corporation. http://www.jstor.org/stable/10.7249/mg781af.11

100. Cain, A. (2002). Iran's Strategic Culture and Weapons of Mass Destruction: Implications of US Policy. (Rep.). Air University Press. http://www.jstor.org/stable/resrep13692

101. Wehrey op. cit

102. Ziedel, R. (2013). Implications of the Iran-Iraq War. E-International Relations. https://www.e-ir.info/2013/10/07/implications-of-the-iran-iraq-war/

103. Eisenstadt, M. (2015) The Strategic Culture of the Islamic Republic of Iran. *Washington Institute.* https://www.washingtoninstitute.org/policy-analysis/strategic-culture-islamic-republic-iran-religion-expediency-and-soft-power-era

104. Ibid.

105. Findlater, E. (2020) Islamic Republic of Iran's Strategic Culture and National Security Analysis. Small Wars Journal. https://smallwarsjournal.com/jrnl/art/islamic-republic-irans-strategic-culture-and-national-security-analysis

106. Ibid.

107. Wehrey op. cit

108. McChrystal, S. (2019). Iran's deadly puppet master. Foreign Policy. https://foreignpolicy.com/gt-essay/irans-deadly-puppet-master-qassem-suleimani/

109. Wehrey.

110. Ibid.

111. Dagler op. Cit

112. Constantin, L. (2012). Kill timer found in SHAMOON malware suggests possible connection to Saudi ARAMCO ATTACK. Network World. https://www.networkworld.com/article/2190711/kill-timer-found-in-shamoon-malware-suggests-possible-connection-to-saudi-aramco-attack.html

113. Hanna op. cit.

114. Lyngaas, S. (2019). IBM sounds alarm about More data-wiping malware from Iran. Cyberscoop. https://www.cyberscoop.com/iran-destructive-malware-ibm/

115. Ibid.

116. RT (2015) Yemeni group hacks 3,000 Saudi govt computers to Reveal top secret Docs – report. RT. https://www.rt.com/news/261073-yemen-cyber-hack-saudi/

117. Wagenheim, M. (2020). Hezbollah hones expertise in training cyber-warfare. agents. The Jerusalem Post . https://www.jpost.com/middle-east/hezbollah-hones-expertise-in-training-cyber-warfare-agents-638800

118. King, R. (2013). Data Shows No Link Between Syrian Electronic Army and Iran. *Wall Street Journal*. https://www.wsj.com/articles/BL-CIOB-2730

119. Menn, J. (2013). Analysis: Syria, aided by Iran, could strike back at U.S. in cyberspace. Reuters.

https://www.reuters.com/article/us-syria-crisis-cyberspace-analysis/analysis-syria-aided-by-iran-could-strike-back-at-u-s-in-cyberspace-idUSBRE97S04Z20130829

120. Siboni, G, Kronenfeld, S. (2014) Developments in Iranian Cyber Warfare 2013-2014. *Military and Strategic Affairs.* https://www.inss.org.il/wp-content/uploads/systemfiles/SiboniKronenfeld.pdf

121. King op. cit.

122. Grohe op. cit.

123. Duggan, P. (2015). Strategic Development of Special Warfare in Cyberspace. Joint Force Quarterly. https://ndupress.ndu.edu/Media/News/Article/621123/strategic-development-of-special-warfare-in-cyber/

124. Ibid.

125. Scott-Railton, J. (2016) Group5: Syria and the Iranian Connection. The Citizen Lab.

126. Regalado, D., Villeneuve, N., Scott-Railton, J., (2015). Behind the Syrian conflict's digital front lines, Special Report. *FireEye Inc*

127. Gaza (2014) "Occupied Palestinian territory, Gaza Crisis". United Nations Office for the Coordination of Humanitarian Affairs. https://web.archive.org/web/20150725191044/http://www.ochaopt.org/content.aspx?id=1010361

128. Winer, S. (2014). Iranians launched cyber-attack on Israel during Gaza Op. Times of Israel https://www.timesofisrael.com/iranian-cyber-attack-on-israel-during-gaza-op/

129. Vogt, H. (2014). Iran launched major cyberattacks on the Israeli Internet – German Intelligence snooped On Kerry and Clinton – seleznev gets no bail. Politico. https://www.politico.com/tipsheets/morning-cybersecurity/2014/08/iran-launched-major-cyberattacks-on-the-israeli-internet-german-intelligence-snooped-on-kerry-and-clinton-seleznev-gets-no-bail-212543

130. Pleitgen, F., Mullen, J., & Smith-Spark, L. (2014). 29 rockets in 20 minutes: Israel, Hamas Ceasefire breaks down. CNN. https://www.cnn.com/2014/08/19/world/meast/mideast-crisis/index.html

131. Rosen, A. (2014). Israel faced a huge wave of cyber attacks during its war With Hamas - And Iran could be the reason why. Business Insider. https://www.businessinsider.com/israel-faced-a-wave-of-cyber-attacks-2014-8

132. Gwertzman, B. (2009) Iran supports Hamas, but Hamas is No Iranian 'Puppet'. Council on Foreign Relations https://www.cfr.org/interview/iran-supports-hamas-hamas-no-iranian-puppet

133. Koss, M. (2018). Flexible resistance: How Hezbollah and Hamas Are Mending Ties. Carnegie Middle East Center. https://carnegie-mec.org/2018/07/11/flexible-resistance-how-hezbollah-and-hamas-are-mending-ties-pub-76782

134. Sverdlov, L. (2020). Israeli cyber company uncovers Hamas campaign against PA. The Jerusalem Post. https://www.jpost.com/arab-israeli-conflict/gaza-news/israeli-cyber-company-uncovers-hamas-campaign-against-pa-617421

135. Sjoholm, J. (2019). Israel-Hamas cyberwar, when old warfare meets new. Lima Charlie News. https://limacharlienews.com/mena/israel-hamas-cyberwar/

136. Hylton/Austin, H. (2006). How Hizballah hijacks the internet. Time. https://content.time.com/time/world/article/0,8599,1224273,00.html

137. Wege, Carl (2014) Hezbollah's Communication System: A Most Important Weapon, International Journal of Intelligence and CounterIntelligence, 27:2, 240-252, DOI: 10.1080/08850607.2014.872532

138. Natasha Bertrand, "Iran is Building a Non-Nuclear Threat Faster than Experts 'Would Have Ever Imagined,'" Business Insider, March 27, 2015, http://www.businessinsider.com/irans-cyber-army-2015-3.

139. Hanna op. cit.

140. DW. (2020) Israel thwarted attack on water systems: cyber chief. DW. https://www.dw.com/en/israel-thwarted-attack-on-water-systems-cyber-chief/a-53596796

141. Staff, T. (2020). Cyber attacks again hit Israel's water system, shutting agricultural pumps. The Times of Israel.

https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/

142. Sanger, E., Schmitt, E., Bergman, R. (2020). Long-Planned and Bigger Than Thought: Strike on Iran's Nuclear Program. The New York Times. https://www.nytimes.com/2020/07/10/world/middleeast/iran-nuclear-trump.html

143. Kovacs, E. (2020). Iranian hackers access unprotected ICS at Israeli water facility. SecurityWeek. https://www.securityweek.com/iranian-hackers-access-unprotected-ics-israeli-water-facility

144. BBC (2021). Iran says key Natanz nuclear facility hit by 'sabotage'. *BBC.* https://www.bbc.com/news/world-middle-east-56708778