Georgetown Security Studies Review

Volume 8, Issue 2

November 2020

A Publication of the Center for Security Studies at
Georgetown University's Edmund A. Walsh School of Foreign Service

http://gssr.georgetown.edu

Volume 8 || Issue 2

GEORGETOWN SECURITY STUDIES REVIEW

Published by the Center for Security Studies
at Georgetown University's Edmund A. Walsh School of Foreign Service

The Georgetown Security Studies Review is the official academic journal of Georgetown University's Security Studies Program. Founded in 2012, the GSSR has also served as the official publication of the Center for Security Studies and publishes regular columns in its online Forum and occasional special edition reports.

Access the Georgetown Security Studies Review online at http://gssr.georgetown.edu
Connect on Facebook at http://www.facebook.com/GeorgetownUniversityGSSR
Follow the Georgetown Security Studies Review on Twitter at '@gssreview'
Contact the Editor-in-Chief at GSSR@georgetown.edu

Table of Contents

You Can't have Women in Peace without Women in Conflict and Security……5
Kyleanne Hunter and Rebecca Best

Does Democratic Peace Theory Hold in Cyberspace?……19
Samantha Randazzo Childress

Just Robots, Just Collection: The Implications of Lethal Autonomous Weapons Systems for Ethical Intelligence Collection…….34
Ainikki Riikonen

China's Influence in Central and Eastern Europe, European Responses, and Implications for Transatlantic Security……...41
Julia Warshafsky

Five Models of Strategic Relationship in Proxy War……50
Amos C. Fox

The Critical Importance of Brown-Water Operations in the Era of Great Power Competition…59
Hugh Harsono

Endnotes…….67

Endnotes: You Can't have Women in Peace without Women in Conflict and Security……..67

Endnotes: Does Democratic Peace Theory Hold in Cyberspace?.....71

Endnotes: Just Robots, Just Collection: The Implications of Lethal Autonomous Weapons Systems for Ethical Intelligence Collection……73

Endnotes: China's Influence in Central and Eastern Europe, European Responses, and Implications for Transatlantic Security……75

Endnotes: Five Models of Strategic Relationship in Proxy War……79

Endnotes: The Critical Importance of Brown-Water Operations in the Era of Great Power Competition……..82

Letter from the Editor

This November, we are excited to present the *Georgetown Security Studies Review Volume 8, Issue 2*.

This cycle, we received a multitude of excellent pieces. With articles on women in conflict and security, cyberspace norms, the implications of artificial intelligence, China's growing influence, and proxy wars, this issue will address a wide array of national security issues. I want to thank all authors for submitting such high-quality articles. I also want to thank each author for exuding incredible patience amid an incredibly uncertain times due to the coronavirus pandemic. I would also like to thank the GSSR editorial board for dedicating many hours of editing and refining these pieces for publication, while also contending with stresses of the pandemic, finals, and comprehensive exams. Thank you. Moreover, I would also like to thank Dr. Keir Lieber and Annie Kraft for their leadership and support in ensuring GSSR operations run as smoothly as possible amid the uncertainties this year has brought. This publication would not have been possible without the unrelenting dedication of our entire team, so once again, thank you.

I want to emphasize the impact the coronavirus pandemic has had on GSSR operations, and that, in light of the many complications it has brought about for authors, editors, and GSSR operations alike, we were unable to publish in our normal format. However, we have done our best to present the below works in the best possible way. Moreover, I ask that you read the articles in this issue with this in mind, as our authors did not have the usual amount of time to prepare their pieces for submission given the rather unusual nature of this semester's timeline.

I sincerely hope that the ideas presented in this issue allow you to deepen your understanding of some of the most pressing national security issues of our time.

Thank you for reading our work!

I hope you all stay healthy and safe.

All the best,

Caroline C. Nutt
Editor-in-Chief
Georgetown, Washington D.C.

You Can't have Women in Peace without Women in Conflict and Security

Kyleanne Hunter and Rebecca Best

Since the passage of UN Resolution 1325 there has been a call for an increase of women in post-conflict negotiations. Indeed, research shows that the presence of women in these negotiations improves prospects for lasting peace. However, there has yet to be a meaningful increase in women's participation in such negotiations. Similarly, despite an international focus on increasing women's participation at all levels of government, women remain underrepresented in both elected and appointed positions. One area where women are increasingly present is as combatants - both in formal militaries and in rebel groups. In this article, we argue that the social gender norms related to women participating in combat are a key driver/reason of the lack of women's meaningful participation in peace processes and government bodies. We introduce a model of cognitive-institutional reinforcement that shows how institutions designed to give former combatants access to public life undermine women's credibility and result in lost opportunities. We use evidence from Disarmament, Demobilization and Reintegration (DDR) programs and veterans' services to show how this model explains the continued lack of women's participation.

"General Martin Dempsey, USA, Chairman of the Joint Chiefs of Staff, has recognized that we undercut the contributions of women at our own peril. We cannot deny ourselves half the talent, half the resources, and half the potential of the population." – Hillary Rodham Clinton and Leon Panetta 2015[i]

In the 21st century, women are increasingly serving as combatants in state militaries and non-state politically violent groups. Concurrently, against the backdrop of UN Resolution 1325, the social status of women has taken center stage as part of a broader "human security" agenda. Additionally, public opinion about the status of women is optimistic, especially among the younger generation. Yet, despite this trend, gendered perceptions are not shifting to reflect the reality that more women are engaging in combat operations. Both public perception and formal institutions deny this reality, ultimately to the detriment of both women's political and economic equality, and the prospects for peace. Research is increasingly indicating that the involvement of women in governance, peace processes, and public socioeconomic life leads to more peaceful and stable conflict outcomes[i] and official UN Resolutions[ii] have been adopted calling for women's equality in all facets of post-conflict negotiations and governance. Despite this, women are still largely excluded from, or included only as tokens, in peace processes and heavily under-represented in many governments. In 2010, then United States Secretary of State Hillary Rodham Clinton observed, "still, we hear the question: Why should women be part of peace negotiations if they were neither combatants nor government officials?" In response, she noted that while women are rarely included in formal peace negotiations, "More and more, [women] are being recruited into regular armed forces and terrorist groups."[iii] Secretary Clinton's words highlight the fact that women's increasing contributions in combat are not being publicly recognized, which stymies efforts toward women's equality in other arenas such as politics and business, where military service or the perception that one has (or could have) served, improves an individual's prospects of success.[iv] This, in turn, hinders efforts at

conflict resolution and peace building – endeavors in which women are proving valuable, but from which capable women are being excluded due to gendered perceptions. In this article, we present a model of cognitive-institutional reinforcement, showing how the institutions created to reintegrate former combatants into society are based on perceptions of women as peaceful noncombatants. As a result, female combatants' social, political and economic equality is compromised, ultimately hindering their ability to participate in and contribute to public life.

This article offers a way to understand why women continue to be excluded from the negotiating table and post-conflict public socioeconomic engagement. It lays out a model of cognitive-institutional reinforcement that shows how institutions aimed at reintegrating combatants, have significantly hampered women's ability for post-conflict public participation based on misconceptions about women's role in combat. The research shows how this applies to both Disarmament, Demobilization and Reintegration (DDR) programs and veterans' service programs.

This article begins with a review of the literature and policy proposals aimed at increasing women's participation in both public and post-conflict life and a discussion of the (mis)perceptions around women serving as combatants. It then introduces cognitive-institutional reinforcement as an explanation as to why more progress has not been made in achieving this. DDR implementation and Veteran Affairs (VA) services are used as evidence to show this theory at work. The article concludes with testable hypotheses for future research and implications from these findings.

BACKGROUND

How are we trying to get women to the table?

United Nations Security Council (UNSC) resolution 1325, adopted in 2000, calls for greater inclusion of women in decision-making that affects the prevention, management, and resolution of conflict. Between 2008 and 2013, the UNSC adopted three additional resolutions (UNSCRs 1820, 1889, and 2122) pertaining to the involvement of women in conflict prevention and resolution. Academic research indicates that meaningful inclusion of women in peacemaking, peacebuilding, and governance is associated with a greater probability of reaching a peaceful resolution and with greater durability of the peace.[v] Despite the increasing emphasis both in academic work and policy on the importance of women to achieve peace, women are still largely excluded from peace processes and, where they are involved, their roles are often not central and their authority is severely limited.[vi] A United Nations study of 31 peace processes between 1992-2011 found that only 2% of chief mediators, 4% witnesses and signatories, and 9% of negotiators were women.[vii] Only 8 of the 31 cases in the sample took place before the adoption of UNSCR 1325. Of the 23 peace processes that occurred after UNSCR 1325, only 13 included women in any capacity and of those, only 2 had at least 10% of signatories who were women. This mandate alone is not enough to bring women to the table.

Involving women in the negotiation and implementation of peace in a meaningful way requires a process for determining which women to include in the process. For women to be effective in peace processes, the individual women and the process by which they are selected should have legitimacy among all negotiators. This means that the women should be chosen on their own merits and ability to represent broader interests not simply to fill a quota or to take on traditional "women's issues". As Bell and O'Rourke (2011) find, if the women involved in peace

negotiations are viewed as legitimate actors by the parties typically involved in these processes – namely politicians and military elites – there is very little likelihood that any provisions either introduced by or meant to address previous inequalities suffered by women will be meaningfully adopted. To best ensure this, the process through which women are selected to be part of the process should be transparent and fair and avoid the appearance (or reality) that women are used as pawns or puppets. Identifying women to participate in all levels of peace processes therefore necessitates identifying a pool of recognized qualified women who will be respected as peers by all at the negotiating table. There is limited evidence from post-conflict South America as to the benefits of including females who had proved themselves as combatants in conflict. In the recent Colombian Process, participants included many FARC women from a variety of ranks.[viii] In the case of El Salvador, prominent female members of the FMLN were present at the negotiating tables. Their presence helped to cement a place for women in post-conflict politics that went beyond traditional "women's issues.[ix]"

Men are often included in post-conflict negotiations and key decision-making positions based on their positions as combatants and leaders in the conflict. Women, however, are often included to meet a numerical quota, resulting in their meaningful contributions being downplayed.[x] If women are to achieve similar status to men at the negotiating table it requires that the contributions of women to combat, both in support and in fighting, be recognized and respected by their society and outside mediators. In addition to combatants, such a pool of women might be drawn from those who have been elected to public office, or prominent figures in public socioeconomic life. However, this avenue is only available when women are sufficiently well represented in public life. When women are not already serving as elected officials and their involvement as combatants is not recognized, meaningful inclusion of women in peace negotiations is handicapped from the outset. The dilemma posed leads us to question which women should participate in peace talks? How will they be chosen when the usual criteria for evaluating a candidate's record do not apply and none are perceived to have relevant experience or legitimacy as leaders or policymakers? The realization of 1325 and subsequent resolutions have suffered from a chicken-and-egg problem. Women present at the negotiating table and in public office have been shown to increase the socioeconomic status of other women. However, recognizing a large enough pool of women with prominent public status is required to get women to the table and in public life on their merits rather than as a result of tokenism.

Why do we need women at the table anyway?

The effect of women on peace and security goes beyond their inclusion in peace processes. There is evidence to support the positive effect that codified gender equality and women's ability to effectively participate in public life has on national political and economic stability more broadly.[xi] Evidence indicates that higher proportions of female legislators are associated with lower likelihoods of both internal conflict occurrence[xii] and civil war reoccurrence[xiii] as well as a greater probability of peaceful resolution to civil conflict.[xiv] Caprioli (2000) finds that both a longer history of female suffrage and a higher percentage of female parliamentarians are associated with a lower likelihood of a state using military violence to resolve interstate disputes. Higher levels of gender equality have even been shown to increase the chances of success of United Nations peacebuilding efforts.[xv] Despite the many positive effects of women in

government, women's political representation still lags in many areas. The United Nations records that, as of February 2019, less than one quarter of national members of parliament worldwide are women and as of June 2019, there are 11 female Heads of State and 12 female Heads of Government.

A barrier to women in elected office emerges in the ways in which individuals are viewed as citizens worthy of holding elected office or ascending to leadership positions. Individuals are more likely to be elected when they are viewed as full citizens and strong leaders, willing and able to sacrifice for their country. Especially in the Western democratic tradition, acknowledged military service is often critical to achieving both of these ends. The tie of military service to worthy citizenship presents an obstacle to women achieving greater influence in politics. Hudson, et al. (2012, p. 40) argue that women are not seen as full citizens because their sacrifice for society is in the form of childbirth which is not visible as a patriotic sacrifice for their country or society in the way that military service is for men. They note that the Swiss Government's rationale for not granting women suffrage until 1971 was that women did not shed blood for their countries. Likewise, because women are not seen as fighting on behalf of their countries and are sometimes viewed as having pacifist or anti-war sentiments as well as cross-cutting loyalties with the women of the enemy (or being susceptible to manipulation by men of the opposing side), they may be viewed with suspicion as possible traitors at worst or as holding the interests of women and children above the interests of the state.[xvi]

The idea that women do not participate in combat is at the root of the chicken-and-egg problem experienced by women in public life. If this idea was overcome, an avenue for women to more fully participate in public life could emerge. Below we discuss the roots of the (mis)perceptions that have led to women's exclusion from public life and introduce our theory of the cognitive-institutional reinforcement that has kept women in this position.

WOMEN IN COMBAT: PERCEPTIONS AND REALITY

Literature shows why female combatants have been largely ignored or misunderstood. Women have made up a relatively small minority of combatants in recorded history. In his extensive review of the relevant literatures, Goldstein (2001) finds no evidence of a society in which women served as most or even fully half of combatants. However, women have participated in conflict for thousands of years, if in small numbers. This fact is supported not only by the ancient histories recorded by Herodotus, legends of warrior women from Celtic and other traditions, but by more recent anthropological and archeological evidence showing that "warrior women" lived, fought, and died alongside their male counterparts in these ancient societies.[xvii] Perceptions of women's participation in conflict are skewed by the fact that despite this evidence, female participation has historically been recorded as myth or fancy[xviii] while male participation has been viewed as part of a nation's official history. This has given female combatants a mythic quality that has detached them from the civilizations they protected and made them into aberrations, rather than affording them the civic recognition given to their male counterparts.

In Western modernity, there has been an uptick in women's participation as combatants in global conflicts. Women have participated in combat roles in conflicts ranging from the American, French, and Nicaraguan Revolutions to the recent wars in Iraq, Afghanistan, and Syria. In the last two decades, there has been a recognized need for women as part of effective counterinsurgency strategies in nearly every NATO country.[xix]

As of 2017, the average percentage of women in the armed forces of NATO members was 11.1%[xx], with Hungary reporting the highest level of women's participation at 19.3% and Turkey the lowest at 0.8%. At that time, 25 of the 28 member states with active militaries placed no legal restrictions on the engagement of women in combat or in particular roles.[xxixxii]

It is also significant that even when states do restrict women from serving in combat roles, the lines between combat and non-combat roles for deployed troops are often blurred. For example, the United States Secretary of the Army stated in 1994,[xxiii] "the issue at hand is not one of deciding whether or not women will be "in combat." The nature of the modern battlefield is such that we can expect soldiers throughout the breadth and depth of a theater of war to be potentially in combat."[xxiv] Further, even when restrictions are in place, the nature of warfare makes it very difficult for them to be followed. In particular, so called "combat exclusion" policies are nearly impossible to enforce in modern war. Such policies are based on both the types of jobs that women are allowed to have (prohibitions on ground combat), and assignment to units that may find themselves in combat situations. However, as "front lines" increasingly disappear from warfare, the ability to assess combat restrictions becomes difficult. A 2007 RAND study found that in trying to adhere to such policies in Iraq and Afghanistan, the Army fell was unable to comply with its own policies and the spirit of the DoD policies restricting women.[xxv]

Similarly, women have long been a vital part of non-state violent groups. Examples run the gamut from the women of Imperial Russia's Narodnaya Volya (several of whom were members of the group's executive committee and were involved in planning the assassination of Czar Alexander II) to the fighters in the Viet Cong and later in El Salvador, Nicaragua, and Guatemala in the 1970s and 1980s; Eretria in the 1990s; and the Kurdish and Yazidi militia women fighting ISIS today. While it is true that women have not been the majority in any of these groups, they represent a sizable, and important, minority, constituting between a tenth and a third of most fighting forces.[xxvi]

To gauge the significance of women's participation in the Nicaraguan Sandinistas, we can look to their numbers: most estimates put the percentage of female armed combatants above 30 percent in the 1970s, while the Sandinista Popular Army boasted about 40 percent women at its creation in 1980. Similarly, 29 percent of El Salvador's FMLN combatants in the 1980s were women.[xxvii] FMLN women served in many roles, including radio operator, medic, cook, recruiter, and fighter; however, female guerrillas of any role might be called up to fight when needed.[xxviii] Though Viterna concludes that the gender neutrality of the duty assignment and promotion within the FMLN has been exaggerated, she determines that women were a vital component of the FMLN and the increased recruitment of literate women in 1985 helped to turn the tide of the FMLN's decline and bring the organization "back as a powerful contender for state power".

Despite the long history of women as combatants, women are still viewed primarily as victims rather than active participants in the conflict. While only a small minority of women participate in combat (just as a small minority of men participate in combat as well)[xxix], the perception of women as non-combatant victims and of men as combatants is so pervasive it delegitimizes the involvement of women in both combat and peace efforts, and leads to misunderstandings and misreporting of data on civilian victimization.[xxx]

Women have been essential to the combat missions during recent conflicts in Iraq and

Afghanistan.[xxxi] As the character of war has changed, so too have the requirements of the battlefield. The presence of women in infantry units led to more accurate and effective intelligence gathering, and more stable post-conflict societies.[xxxii] The nature of these conflicts has also redefined what it means to serve in combat. As the authors of the RAND study note, "women [comprise] approximately 10 to 20 percent of Army personnel deployed to Iraq and [participate] in almost every kind of unit or subunit open to women within [brigade combat teams]"

The misunderstanding of the true nature of women's participation in violent conflict can be traced to the way in which women have been conceptualized in the study of war. In the study of conflict, women are generally viewed in one of three ways. First, women are seen as civilians who are separate and removed from the conflict.[xxxiii] Women are kept in the domestic, private space while men go off and fight. Second, they are portrayed as victims of war. Whether through sexual violence or forced participation in rebel groups, women are frequently seen as lacking agency and being victimized during armed conflict.[xxxiv] Third, women are thought of as peace-activists.[xxxv] When women's agency during conflict is acknowledged, it is frequently in the form of what they do to stop war.

Despite these generalizations, there have been research focused on women's agency during conflict into both scholarly and practical circles. The increased attention on women in both the recent Global War on Terror and current civil wars have given space for this work. Notably, Sjoberg and Gentry (2007) highlight how it is agency, not victimization, that allows women to choose violence during conflict. Additionally, much attention has been given to the agency of women who fight in the FARC.[xxxvi]

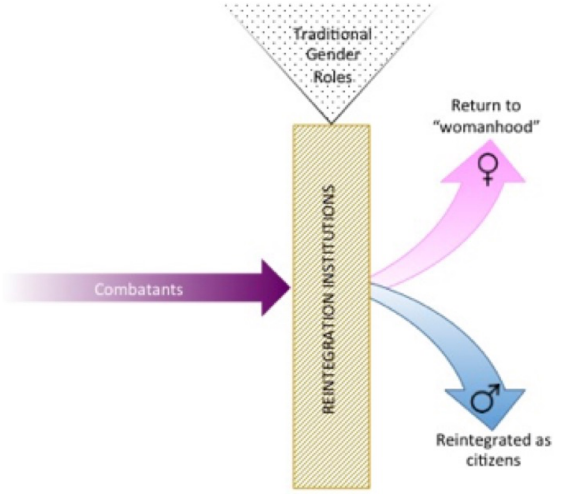
This work has started to turn the tide on our understanding of women during conflict. However, there remains much to be done. As April Carter (1998) argues, the feminist discourse will not be complete until women are given the agency and autonomy to choose violence, just as their male counterparts are. In this article we introduce our model of cognitive-institution to explain why women who choose to engage in combat continue to be marginalized and excluded in ways that their male counterparts have not, and offer solutions towards effectively bringing women to the table.

A MODEL OF COGNITIVE-INSTITUTIONAL REINFORCEMENT

Despite the fact that women do participate in conflict as combatants, they are continually conceptualized as pacific civilians due to cognitive-institutional reinforcement, whereby norms and traditional gender roles shape the societal perceptions of both genders, and the institutions that surround warfare, combat, and armed groups (both state and non-state sanctioned). To understand this phenomenon, we must first understand the purpose and role of institutions in society. Public institutions both reflect the social norms and culture of the societies that create them and reinforce, reproduce, and protect those norms.[xxxvii]. Institutions of violence, such as the military, in particular, reinforce traditional gender roles.[xxxviii] The public face of violence has long been a space occupied by men,[xxxix] and institutions of violence therefore perpetuate the cognitive assumption that women are peaceful, domestic actors. As Louise Chappell (2006) argues, one cannot understand a society's political institutions without first understanding the culturally specific gender-based power dynamics that underlay them. Institutions of political violence act as reinforcement of gendered norms, as acts of violence are frequently the bedrock of social constructions.[xl] It thus follows that the institutions that exist to de-mobilize individuals in the post-conflict

period have been created via this same framework of traditional gender roles. Therefore, despite their participation as combatants, women are reintegrated into society as "women," while their male counterparts are reintegrated as former fighters. Figure 1 illustrates cognitive-institutional reinforcement.

Figure 1: Cognitive – Institutional Reinforcement



As shown, institutions of reintegration (such as DDR programs and veterans services) are informed by traditional gender roles. The result is that institutions act as a filter to reinforce the norms on which they were built. Therefore, while men and women combatants both enter reintegration institutions with largely the same experiences and expectations, after participating in programs designed by gendered institutions, men and women experience drastically different outcomes. This explains why despite women's participation in combat, they are denied the elevated citizen status frequently enjoyed by their male counterparts and the lack of women at post-conflict negotiations and in government, despite the passage of UN Resolution 1325 and its successors. As long as institutions are built on and reinforce traditional gender roles, women will continue to be excluded from public life. Below we highlight how the gendered nature of these institutions provide the groundwork for our theory on cognitive-institutional reinforcement.

THE GENDERED NATURE OF REINTEGRATION INSTITUTIONS

In this section we provide examples of DDR programs as well as results from an original survey of US female veterans to provide evidence for cognitive-institutional reinforcement.

DDR – Re-casting female fighters as women

DDR programs facilitate the transition from periods of armed civil conflict to peace and the reconstruction of civil society and the associated institutions. DDR agreements vary greatly in their specifics, but they all include three main types of provisions. (1) Disarmament provisions include the collection of arms, including sweeping for land mines, and the documentation of fighters. (2) Demobilization provides for the reinsertion of individual fighters, and receive support, which may include stipends for food and job training, as well as access to land. (3) Reintegration includes include long-term provisions such as assistance with employment.[xli]

However, a 2015 assessment of DDR programs concludes that "women's participation in war has often been ignored and excluded in the design and implementation of programmes for former combatants".[xlii] This exclusion of women can have disastrous consequences, as in the case of the failed 1994 Lusaka protocol in Angola. Even though the Lusaka protocol was extolled at the outset for its gender neutrality, in practice women were entirely excluded from the peace talks, which ultimately failed to address issues such as sexual violence and government abuses. Furthermore, the agreement delegated the identification of combatants to military and rebel leaders, who failed to identify female combatants, and the men planning the removal of landmines failed to consider sweeping fields, wells, and forests that women would traverse to do the

work of maintaining their homes and growing crops.[xliii]

Though more than two decades have passed since the failure in Angola, it highlights persistent problems. In the 21st century, both the need for the inclusion of women and the inability of "gender blind" processes to adequately include women or address the needs of women remain. In her examination of DDR programs in Sierra Leone, Megan MacKenzie (2009) finds that the programs were primarily aimed at re-characterizing female combatants as "mothers" or "wives" and stripping them of the authority they had earned in combat, rather than giving them the tools necessary for successful reintegration. While job training options for men included lucrative fields such as masonry and mechanics, women were primarily offered training in traditionally feminine skills such as tailoring and hairdressing, with the choices so limited that the skills were in oversupply and therefore worthless.[xlivxlv] Training women in only a very narrow range of gendered fields means that not only are the women's earning prospects reduced while they are left with obligations toward the children they may have born while in service, but they may also be alienated by the process, causing the DDR, the peace, and the government to lose legitimacy.[xlvi] O'Neill and Vary add that, as in Angola, women were largely excluded from the Sierra Leone DDR by the processes used to identify combatants and gendered requirements to receive benefits, for example the requirement that women who received microcredit through the DDR be accompanied by their husbands (2011). As a result, former female soldiers were largely cut out of the post-conflict government negotiations and economy. MacKenzie goes on to note that both the original DDR process in Sierra Leone and the subsequent attempts by the United Nations and the international community did not incorporate women. This omission means that they failed to consider the lived experiences of the large numbers of women who chose to engage in violence, as opposed to being abductees or camp followers. The case of Sierra Leone is hardly unique; much of Liberia's DDR was copied directly from Sierra Leone's.[xlvii]

Research on gender and DDR programs indicates three pieces of evidence of cognitive-institutional reinforcement: (1) female combatants are often excluded, implicitly or explicitly, from many or all of the benefits extended to former combatants and are often re-cast as camp-followers, wives, whores, or abductees; (2) within the context of DDR programs, at least some of the traditional gender norms shaping these programs are coming from NGOs and IGOs founded on liberal Western values;[xlviii] and (3) the exclusion of women extends beyond former combatants, with women and their perspectives and interests also being excluded from peace talks and post conflict governance, despite evidence that the inclusion of women produces better outcomes.[xlix] As the cases of Angolan women killed by landmines while tending fields and gathering firewood demonstrate, excluding women from peace processes not only makes those processes more likely to fail, it produces unanticipated and sometimes far-reaching consequences.[l]

Data on rebel women is harder to come by than that of women in formal militaries. Therefore, fully quantifying the scope of those touched by the adverse outcomes of cognitive-institutional reinforcement proves difficult. Insurgencies and other non-state fighting forces often rely on a certain degree of secrecy and tend to be less transparent in their record-keeping. Compounding this problem are those eluded to above: some female combatants may not want to be identified for fear of gendered reprisals or ostracization while some male commanders may purposefully not identify the women

who were under their command as combatants. Therefore, while we can get a good idea of the rate of women's participation in DDR, we may not always have accurate figures detailing their participation in armed groups. However, by relying on expert case studies, we can get an approximation of the extent of women's exclusion from DDRs. In Sierra Leone, where estimates of women's participation varies by unit from 10-50%, women made up less than 7% of adult combatants in DDR and girls accounted for 8% of children in DDR.[lilii] In Liberia, women accounted for nearly 22% of those disarmed in the DDR.[liii] Although it is difficult to estimate the percentage of women combatants, women were involved in both integrated units and all women units, and Specht suggests that the number of non-demobilized *girls* may reach 14,000.[liv] In the DRC, girls were estimated to be 40% (12,500) of all children in armed groups as of 2005. However, by 2007, only 2,610 of the 130,000 demobilized DRC fighters were women.[lv]

The exclusion of women from DDR processes is sometimes by design,[lvi] but it is more often the result of preexisting normative frameworks about who can or should be a combatant and about the roles that women can and do play after war. While studies of DDR implementation indicate that individual male commanders and fighters may deliberately exclude eligible women from these programs[lvii] and reintegration programs may turn away women for reasons such as pregnancy,[lviii] in other cases exclusion is the result either of fallacious assumptions about the contributions of women or of normative strictures that made female combatants less likely to participate even where they were eligible. Indeed, MacKenzie (2009) notes that not only were women in Sierra Leone more likely than men to be stigmatized for their involvement with an armed group, but that women, especially those who had children by other rebels, might be stigmatized as probable rape victims[lix] or as violating communal norms regarding the passage from childhood if they self-identified as combatants to participate in the DDR. In other cases, gendered norms, such as women's responsibilities for childcare, were not accounted for in the DDR, meaning that women were simply unable to participate.[lx]

Not only does the exclusion of female combatants from DDR harm the affected women, it harms their families, communities, and, ultimately, the prospects for peace. Individual women suffer as they are unable to access benefits such as education and training, loans and land, even healthcare. Families and communities in turn are harmed both by the resulting loss of income and by the loss of women's perspectives, skills, and leadership. Families and communities are further harmed as women fighters who have born children during conflict are denied DDR resources that would enable them to care for themselves and their children or are stigmatized as prostitutes or victims for having borne children. Women denied access to DDR may be pushed back into the home and away from more lucrative careers making better use of their experience and insight, which is further costly both to the women and the communities that lose out on the benefits of women with experience in leaderships, medicine, radio operation, engineering, or other fields.

As noted in the recent Democratic Progress Institute report, "addressing gender concerns in DDR goes beyond merely considering the role and needs of women in armed conflict" (2015, 18). Indeed, it is clear that societal impressions of gendered conflict behavior are harmful to women who may be infantilized and denied access and agency in post-conflict societies; to men who may be viewed as violent or as willful combatants, regardless of their actual roles; and to societies generally as they are denied the diversity of

perspectives that may allow for more stable and sustainable peace deals and a more prosperous society. While traditional gender norms confer certain political advantages to men, they also make them subject to victimization in war (e.g. Ormhaug 2009) and, evidence suggests, makes the wars that claim the lives of men, women, and children alike more intractable by ensuring the exclusion of women from peace making and peacekeeping.

As DDR programs make it harder for women to access benefits, they also effectively erase female combatants and their war efforts, allowing for the populace to forget or downplay the roles of women in combat and to further entrench common stereotypes.[lxi] MacKenzie writes that through the official DDR programs and even through the efforts of aid organizations attempting to help women in Sierra Leone, rebel women were recast as camp followers or abductees. She observes that even the agencies that aimed to help women never referred to them as soldiers, favoring terms that denied them agency to choose violence (2009). One result of this refusal to view women as agents of violence is that women are less effective as agents of peace (or engines of growth) than they might be. When we consider the great volume of research on the effectiveness of women at producing and maintaining peace,[lxii] we can theorize that the acknowledgement of women's roles in conflict (and therefore their legitimacy to speak about issues of conflict and peace as not only victims or bystanders but as participants and potential spoilers, willing to fight for their causes) might be the missing link to ensuring more equitable and sustainable peace deals and more enduring peace.

Veterans' Reintegration

Members of informal fighting groups are not the only ones suffering from the cognitive-institutional reinforcement of traditional gender norms. Female members of the military also have to engage with reintegration institutions built on reinforcing traditional gender norms. As Melissa Herbert (2000) found, after leaving the military, women often felt "excluded" or "alienated" from the veteran community as a result of their gender. Much of this was a result of the way in which reintegration programs and veteran services engaged with women. Though Herbert's work draws on surveys from many Western nations, most of the work done on women's re-integration is focused on the US. The US has one of the largest militaries, and as a result, one of the largest percentage of women veterans. It also has a vast and extensive Veteran's Administration (VA) as well as dozens of established and active Veterans' Service Organizations (VSOs), making it an accessible case study. These institutions are primarily responsible for handling the transition of veterans from military service into the civilian world.

The Department of Veterans' Affairs states that its purpose is to "care for him who shall have born the battle."[lxiii] "Care" in this instance, refers to far more than physical medical care, as the VA strives to serve the whole veteran. The VA is often the gatekeeper between military service and civilian life. It provides educational, financial, and vocational benefits, as well as a network of past and future veterans/connection to generations of veterans past and future. In addition to the VA, several VSOs are active in the US. Groups such as the American Legion, Veterans of Foreign Wars, and Iraq and Afghanistan Veterans of America provide additional transitional support to veterans transitioning from military into civilian life.

In the context of the VA, evidence of the cognitive-institutional reinforcing nature of veterans' reintegration can be seen in variety of disciplines. The sociological work of

Theda Skocpol (1992) sheds light onto the origins of the gendered nature of veterans' reintegration. Dating back to the Civil War era, public provisions for men were closely tied to military service, while women's provisions were tied to "motherhood." Though these institutions were not intentionally gendered, the tying of men's benefits to soldiering and women's benefits to motherhood, reinforced the cognitive gender stereotypes of the publicly violent men and the private nurturing women. It is out of this system of post-Civil War pensions and educational benefits that the modern-day VA was born. As the VA grew, its facilities and programs were designed to reintegrate male veterans. From the medical services available to the aim of vocational and educational programs, the VA has focused primarily on men and their needs. Even into the 21st Century, when women are an increasing part of the military, the cognitive notion of the male soldier still informs the way in which the VA as an institution operates.

Public health and behavior science research show the impact of the cognitive-institutional reinforcement of the VA. The review of survey data gathered on female veterans found that they did not believe that they received the same level of care, or the same opportunities for participation in reintegration programs as their male counterparts.[lxiv] This perception was largely a result of female veterans believing that the VA was unable to meet their needs, or treated them like spouses or dependents, rather than as service members.[lxv]

Furthermore, exclusion from VA services has both physical and socio-economic impacts. Physically, female veterans are more likely to suffer from depression and chronic illness than their male counterparts due to the fact that they are less likely to seek and/or receive care from the VA.[lxvi] Female veterans are also more likely to experience homelessness and un- or under-employment, resulting in a growing poverty rate among this population. In 2015, female veterans were more than three times as likely to have no income as their male counterparts, and almost twice as likely to be homeless.[lxvii] In exploring this phenomenon, women cite reasons such as "expectations of a return to being a mother/wife," or "expectations that I didn't have to be the primary bread-winner[lxviii]" as reasons why they believed the VA programs did not adequately serve them. Indeed, these gendered expectations provide a real and tangible disservice to female veterans.

In addition to the physical problems faced by female veterans, female veterans often suffer from socio-economic inequities. The social ties formed at the VA and in other VSOs often provide the springboard for veterans to engage in public life. Being associated and identifying as a veteran has helped many veterans engage in careers in politics or other public service. Veterans are seen as more trustworthy, and civic-minded than their civilian counterparts by the American electorate, and therefore enjoy more popular and cross-party support.[lxix] However, female veterans remain under-represented in public office. Only 7 female veterans serve in the 116th US Congress (compared to 89 male veterans). Therefore, while nearly 11% of United States veterans are women[lxx], only 6% of veterans in Congress are women. Much of this disparity can be linked to who enjoys the benefits of association with veteran status. Military service has been associated with a particularly favorable views of candidate ability in the arenas of foreign policy and defense – policy areas that become more important to voters during crises and wars.[lxxi] However, women are rarely associated with these positive characteristics of service.

Women's lack of participation in and involvement with VSOs provides one explanation for the fact that women are less frequently associated with veteran status.

Though there is limited research on the topic, there is early evidence to show that involvement with a VSO heightens identity – both in terms of self-identification and identification by others – as a veteran.[lxxii] Having both an internal and external validation for veteran identity heightens the ability of veterans to gain public citizenship benefits of military service. In an original survey of 165 military veterans (67 men and 97 women), 33% of women indicate strong agreement with the statement that VSOs disproportionately cater to male veterans and 70% indicate that they somewhat agree, agree, or strongly agree. Among male veterans, just over 49% indicate some degree of agreement with that statement, while only 13.4% disagreed.[lxxiii] Women, therefore, do not capture the benefits of this public identity with regards to their service. This lack of formal external identification may contribute to the lack of women veterans gaining public political prominence.

We also asked survey respondents[lxxiv] if they had ever experienced any of a variety of different challenges to their service. These challenges included: having others dismiss/diminish the nature or magnitude of service, having VA employees accuse you of unfairly claiming benefits or challenge your right to access those benefits, had VA employees direct you to spousal services when you sought services as a veteran, had members of a VSO assume you were there for spousal support or activities, been told that you don't look like a veteran, or been accused of lying about your military service. The results of these questions are reported in Table 1.

Table 1. Summary statistics for challenge types by respondent gender.

Challenge	Women (n=97)	Men (n=65)
Service diminished	65.0% (n=63)	47.7% (n=31)
Spousal Services – VSO	44.3% (n=43)	1.5% (n=1)
Spousal Services – VA	24.7% (n=24)	0
Don't Look Like Vet	83.5% (n=81)	44.4% (n=20)
Accused of Lying	9.3% (n=9)	7.7% (n=5)

To evaluate whether women in our sample experience significantly more challenges as compared to men in the sample, controlling for age, officer status, and combat experience, we use a logistic regression model. We first create a single variable that captures the number of different types of challenges reported by each respondent. Men in our sample report an average of .6 types of challenges (std. dev. .8). Women report an average of 1.5 types of challenges (std. dev. 1.3). It is worth noting that this is the number of types of challenges, not a measure of how frequently the challenges are experienced. The results of our regression model are reported in Table 2.

Table 2. Regression of gender on challenges to veterans. N=119

	Challenges
Female	1.259***
	(0.200)
Age	-0.004
	(0.087)
Officer	0.175
	(0.191)
Combat	0.022
	(0.025)

Constant	0.042
	(0.538)
R-squared	0.242

* p<0.05, ** p<0.01, *** p<0.001
Standard errors in parentheses.

HYPOTHESES FOR FUTURE RESEARCH

This article has introduced a model of cognitive-institutional reinforcement of traditional norms in the reintegration of female combatants to civilian society and provided supportive narratives drawn from the contexts of veterans' services in the United States and disarmament, demobilization, and reintegration programs around the world. This model can aid in future research on the two primary communities served by these processes: female veterans of state armed forces and female veterans of armed non-state actors. In particular, it can help to determine how (or if) the gender appropriateness[i] of reintegration programs and services translates into better socio-economic and political outcomes for women. As we have previously argued, better outcomes for women in these areas serve not only the interests of women and their families, but also the cause of peace more generally. Therefore, it is important to test the ways in which women are brought to the peace table and into public life more broadly, to ensure practitioners are engaging women in the best possible way.

An assessment of the model and the connection between the reintegration of women combatants and the status of women in society and politics generally necessitates the development of testable hypotheses. For future research we propose two primary groups of hypotheses:

Hypothesis Group 1: DDR programs that included women in a gender appropriate manner led to more women's participation in peace processes, higher socio-economic status for women, greater representation of women in politics, and a shift in gendered perceptions of women (e.g. perceptions of women as leaders as measured by Pew public opinion polls).

Hypothesis Group 2: Countries with gender appropriate veterans' services have more female participation in government, higher socio-economic status for women, and a shift in gendered perceptions of women.

Each of these hypothesis groups can be broken down into several smaller hypotheses. This allows us to disaggregate "women's participation" into several sub-components and determine the relative weight that each carries. The disaggregation, as well as the focus on gender appropriateness rather than "inclusiveness," will continue to provide valuable contributions to practitioners as well. The more specificity – both in terms of cultural intersectionality and specific outcomes – that can be provided to practitioners, the greater the likelihood for success.

CONCLUSION

Research on the involvement of women in peace and security has been ubiquitous in the wake of the 20-year anniversary of UNSCR 1325. Assessments indicate that meaningful inclusion of women in the peace process and governance produces better outcomes for peace, stability and security writ large. However, despite this women's representation both in peace talks and in governance lags. We argue that the gendered nature of institutions, based on their cognitive underpinnings, is a stumbling block for meaningfully integrating women into peace and security processes as well as government structures. Further, until reintegration institutions incorporate gender in appropriate

ways women will not be able to fully achieve equality in public life more broadly.

We argue that because traditional gender norms have been and are being built into the institutional structures for the reintegration of veterans and non-state combatants, they largely erase the contributions of women and push female combatants back into traditional gender roles, rather than effectively addressing their needs or allowing them the positive externalities of public life afforded by service and sacrifice. This institutional structure, shaped by gender norms, further entrenches a society's cognitive understanding of gender norms, particularly with regards to women's role in public life. As women are erased from combat, their legitimacy as civilian leaders is diminished, and they are seen as weaker options for public leadership.

If institutions took a gender appropriate approach, institutions for reintegration could cast a spotlight on the contributions of women, while keeping them engaged in their communities. For female veterans of both government and non-state armed forces, this could mean more opportunities for leadership in government and business and higher socio-economic status. For women in society generally, this would mean greater recognition of the contributions that women make at all levels of society and of their capabilities, as well as greater representation of the issues that disproportionately affect women.

Through a survey of DDR programs, we illustrate that achieving gender appropriate DDRs is not straightforward. While leaders in the affected states and the international community have attempted to design de-gendered agreements, they have fallen severely short of the target. In part, this is the result of failures to consider local culture and the stickiness of gender norms. In other part, it is the result of failing to reach out to combatant women at an early stage and throughout the DDR process to determine what their needs are and what barriers they face to meeting those needs. The international community has indicated interest in improving the gender inclusiveness of DDRs, doing so will require learning from past mistakes, listening to affected women, and making a conscious effort to appeal to these women.

In our examination of the US Veterans' Administration and survey of a sample of veterans, we highlight how institutions built on the traditional idea of the male soldier have excluded women. Understanding the needs of female veterans and incorporating them in an appropriate and meaningful way is crucial, as female veterans are a fast-growing population. At a time when the international community (including the U.S.) recognizes the importance of women's leadership in public life – both politically and in the broader socioeconomic sphere – it is essential that women who risked their lives to serve their country be included in the institutional benefits of service.

We anticipate that gender appropriate institutions of reintegration of female combatants will lead to an eventual shift in women being able to have a legitimate seat at the table, a step to help codify and entrench the positive benefits of women's leadership. This shift should in turn lead to more positive attitudes toward women in society and in leadership, higher socio-economic status for women, greater gender equality, more meaningful representation of women in government, and greater security and stability worldwide.

Does Democratic Peace Theory Hold in Cyberspace?

Samantha Randazzo Childress

Current international relations scholarship emphasizes cyber conflict, and the debate tends to focus on the use of cyber attacks between authoritarian states and Western democracies. But do democracies attack each other in cyberspace? Exploring such possibilities could challenge current notions about the broad applicability of the democratic peace theory. An examination of cyber incident databases demonstrates that democracies do, in fact, trade cyber attacks, and a qualitative analysis of known cases highlights the conditions under which they choose to do so. This paper indicates trends in democracy-on-democracy cyber attacks that have important implications for US policy while testing the theory of democratic peace in a new context.

The fact that democracies rarely fight each other is one of the most robust findings of international relations scholarship. The theoretical framework that flows from this observation—known as democratic peace theory—has been investigated extensively, and while there are many valid criticisms of it, democratic peace theory is considered by some to be "as close as anything we have to an empirical law in international relations."[i]

Since at least the end of World War II, military conflicts between democratic states have been few and far between. Given that democracies are hesitant to attack each other in the real world, it stands to reason that they may also refrain from attacking each other in the digital world. But I offer that democracies may be willing to attack each other[ii] in cyberspace for several reasons: 1) cyber attacks are generally covert and may not be immediately attributable, giving perpetrators short-term deniability; 2) cyber attacks are arguably easier to execute than attacks in other domains (land, sea, air) in that they require fewer physical resources; 3) no cyber attack thus far has directly caused a loss of life, which may make states less likely to retaliate or escalate. Overall, cyber weapons may present less perceived risk to their user, therefore lowering the threshold of use.

The vast majority of empirical research focuses on cyber actors known to have malicious intentions toward the United States and the West, while few address how or why states we would least expect—those who are not adversaries and, in some cases, even allies—might attempt to undermine us in the cyber domain. This paper endeavors to bridge that gap in the literature. A systematic study of cyber attacks by democracies on other democracies, including when they choose to deploy them, why, and to what effect, will bring us closer to an understanding of the landscape of cyber conflict. Further, it will help us to extend, or perhaps repair, the logic of democratic peace theory and tell us whether the framework might fall apart in the cyber age.

Research Question

This study will seek to answer the following questions: Do democracies perpetrate cyber attacks against each other? If so, under what circumstances? Could any known attack be construed as a violation of democratic peace theory?

The answers to these questions are important to our understanding of how democratic peace theory functions in practice, and there are wide-ranging implications beyond the theoretical. The results will help inform US policy makers about conflict thresholds and norms in cyberspace and whether they differ from thresholds and norms in the physical realm. For example, is it conceivable that another democracy—even an ally—who would not be willing to attack the United

States kinetically may be willing to deploy a cyber attack, especially in the midst of a diplomatic dispute or if the perceivable risk of retaliation is low? Investigating such hypotheticals will reveal much about the types of cyber threats we will face in the future and whether they might come from unexpected places. Policymakers should consider these implications as they decide what information they choose to share with other democracies, what their offensive and defensive cyber strategies should be, and whether to pursue cyber-specific treaties and arms control agreements.

Given there are varying accepted definitions of "war" and "cyber attack," from this point forward, I will define my terms as follows: "cyber attack" refers to any unauthorized incursion into the digital information systems of a given entity—either state or non-state—including acts of espionage (provided that the espionage required unauthorized system access; passive listening does not count). "Cyber warfare" refers to a government engaged in destruction against another within cyberspace—for example the destruction of data, network interruptions, or system shutdowns—per Richard Clarke's definition[iii] with one additional caveat: the destruction itself must be the goal of the cyber action. This excludes attacks that unintentionally cause collateral damage while serving another end, such as espionage operations that attempt simple data exfiltration or interception of network traffic. For the purposes of this paper, all acts of cyber warfare are cyber attacks, but not all cyber attacks are acts of cyber warfare.

II. THE BROADER DEBATE: DEMOCRATIC PEACE THEORY AND THEORIES OF CYBER WAR

This paper investigates instances of cyber attacks between democracies and seeks to understand whether they constitute acts of cyber war, which could be construed as violations of liberal peace. Because this study sits at the nexus of two theoretical disciplines, it draws from two bodies of literature: democratic peace theory (DPT) and the theory of cyber war. The following section discusses the main arguments and applicability of each.

Democratic Peace Theory

The fact that democracies tend not to fight each other is well established in the empirical record.[iv] In his seminal work "Liberalism and World Politics," Doyle argues that the Kantian idea of a "separate peace"—the observable lack of armed conflict between democracies, even as democracies continue to fight non-democracies—exists due to a combination of characteristics that democracies share: republican principles of government, a like-mindedness that engenders understanding, and an interest in the free flow of commerce.[v] While these causal mechanisms are still debated today, more recent scholarship has sought singular explanations for democratic peace rather than accepting Doyle's idea of interdependent causes.

DPT scholarship has thus fractured into multiple schools of thought. As the task of this paper is not to test what causes democratic peace but rather to find out whether democratic peace exists in cyberspace, the discussion of the debate surrounding DPT's causal mechanisms will be brief. According to normative thinkers, democracies share republican values, such as peaceful resolutions to political conflicts and the right to self-determination; this like-mindedness engenders trust and respect between democracies, which makes them less likely to fight.[vi] In contrast, the institutional school holds that leaders' accountability to constituents allows democracies to signal their true intentions, thus making clashes between them less likely.[vii] The capitalist school contends that liberal economic policy, rather than any given feature endemic to democratic

governments, keeps democracies from fighting each other, as they are averse to harming their intertwined economic interests by fighting wars.[viii]

Criticisms of DPT Scholarship

There are several criticisms that call the robustness of DPT into question, and as this paper endeavors to test DPT in a new domain, they are particularly relevant. Mearsheimer points out that liberal democracies have existed for a relatively short period in world history, thus DPT attempts to draw conclusions from a very small sample size.[ix] As noted by Spiro,[x] the existence of zero wars between democracies is not statistically significant and may well be attributable to chance. Spiro further argues that the DPT literature tends to use ill-defined key terms—particularly "democracy" and "war"—that allow researchers to dismiss ad hoc cases that challenge the theory. These terms frequently go undefined in the DPT literature, and when definitions do appear, there is little consensus. Spiro's criticism of the underspecified definitions of DPT is important in the cyber context, because if we do not know what counts as war, how can we know what sorts of cyber operations might be analogous? How can we decide whether the democratic peace holds in the cyber realm if we don't know who counts as a democracy?

Moreover, Forsythe discusses multiple cases in which the U.S. used "forcible covert action" against another elected government in the name of its security interests.[xi] Though he stops short of claiming that covert interventions constitute "war" (and thus a challenge to DPT), Forsythe's findings call the normative logic into question, as democratic values do not prevent democracies from sabotaging other elected governments. The observation that democracies are willing to conduct covert operations against other elected governments maps directly to the subject at hand, as cyber operations are generally covert. Forsythe's research suggests that we can expect democracies to trade cyber attacks, though it does not necessarily mean that we can expect to see democracies *committing acts of cyber warfare* against one another.

Cyber War

The literature surrounding cyber warfare is far less developed than that of DPT. The term "cyberwar" was coined by John Arquilla and David Ronfeldt;[xii] the pair define cyber war as "conducting, and preparing to conduct, military operations according to information-related principles" and warn that cyber war will occur in the future. However, neither Arquilla and Ronfeldt's definition, nor the notion that cyber war is bound to happen, has gained wide acceptance.

Scholars are divided between those who believe that acts of war are possible in cyberspace and those who do not. In his treatise, "Cyber War Will Not Take Place," Rid argues that in order to qualify as an act of war, an act must be violent (which Rid defines as lethal), instrumental, and political; no past cyber attack has met these criteria, and future cyber attacks are unlikely to meet them, so cyber attacks are better understood as acts of "subversion, espionage, or sabotage" than as acts of war.[xiii] In a response to Rid, Stone asserts that acts of war in cyberspace are possible because the use of force need not kill people; violence against objects or systems that achieves a political end can also qualify as an act of war.[xiv] Clarke agrees that cyber war—which he defines as "a government engaged in destruction against another within cyberspace"—has not happened yet, but is possible, and even likely, in the future.[xv]

Discussion

While the scholars cited above all make valid points, for the sake of argument, this paper will assume that democratic peace exists in the physical world and that an act of war in cyberspace is possible. The analysis that follows will use Clarke's definition of cyber

war ("a government engaged in destruction against another within cyberspace") to determine whether any one cyber incident constitutes a violation of the democratic peace.

Proposing a definition of democracy and deciding which nations count as democratic according to that definition would consume more resources than are available to this author, so the tests that follow will use an appropriate index to code nations as democracies or non-democracies; this will be discussed in more detail in the next section. Per Mearsheimer's criticism, it is important to note that this research uses an even smaller data pool than the one available to DPT theorists because cyber operations are newer than democracy. Bearing Spiro's argument in mind, even a finding of zero acts of cyber war between democracies may not be statistically significant due to the relatively short time from which data can be drawn.

Illuminating the causal mechanisms that underpin DPT is not the main task of this paper, but an examination of the test results may inform our understanding of the causes of democratic peace. For example, if the normative explanation is correct, democracies should be as unlikely to commit acts of war against each other in cyberspace as they are in any other domain, because to do so would be a violation of democratic norms. Democracies should also be less likely to use cyber attacks against each other if the capitalist school of DPT is correct, as they could interrupt the conduct of free markets either directly (through interfering with the systems of financial institutions or companies who do business internationally) or indirectly should the target of the operation decide to retaliate in the economic sphere. The institutional view of DPT is somewhat less relevant here, as cyber operations are generally covert, and leaders of democracies are less constrained in their ability to order covert operations than they are in their ability to start wars. However, to analogize an argument made by Bueno de Mesquita, et al.:[xvi] if democracies are afraid to pick fights they cannot win with other democracies, we would only expect them to clash in cyberspace if there is a large disparity in their cyber capabilities.

Hypotheses to be Tested

My working theory is that democracies are willing to use cyber weapons against each other as a means of achieving their ends. I postulate that while democracies may commit cyber attacks against each other, no discrete incident will meet the criteria for cyber warfare under close examination. In all likelihood, the incidents in which democracies attack other democracies will amount to little more than spying, and thus will not constitute a violation of democratic peace theory. However, such incidents will be worth exploring to gain a better understanding of when and why democracies attack each other in cyberspace.

With that said, I test the following hypotheses:

H1: Democracies employ cyber attacks against each other.

H2: Known cyber attacks between democracies do not meet the definition of cyber war.

The following section outlines how I intend to evaluate these hypotheses.

III. METHODOLOGICAL APPROACH

First, using dyads of democracies, I will evaluate whether any state-sponsored cyber attacks[xvii] have been perpetrated by a democracy against another democracy. To do this, I will compile a list of all states that are democracies and another list of democracies that possess offensive cyber capability. I will then create dyads by pairing each democracy that has offensive cyber capability with every other democratic country and code each dyad as having experienced at least one cyber attack (positive) or not (negative). In order to code a dyad as positive, I will not require both

members to have attacked each other; I will only require one member to have attacked the other.

If there are no positive dyads, H1 can be rejected, and H2 will be irrelevant. Such a result could be taken as evidence that DPT holds in the context of cyberspace. But it is critical to note—per Mearsheimer and Spiro's criticisms of DPT—that a result of zero positive dyads (i.e., no known cyber attacks between democracies) may not be statistically significant due to the small sample size. Should I obtain such a result, I would run further tests to determine its statistical significance.

However, based on preliminary research, I assume that there will be at least one positive dyad. In that case, H1 would be proven correct, the validity of DPT in the cyber domain would still be in question, and I would conduct a qualitative analysis of each exchange in order to evaluate H2. These analyses will discuss the type of attack, the independent variables specified below, and the implications for the robustness of democratic peace theory. If any patterns emerge from that analysis—such as the type of attack used or a particularly tense political context—I will discuss those specifically, as they could be important to policymakers in anticipating and defending against future attacks.

If none of the cyber attacks in my sample constitute "a government engaged in destruction against another within cyberspace," this can be taken as evidence that H2 is correct, and that democratic peace theory holds in cyberspace. Here, it is important to make one more distinction: while one could reasonably argue for a broader definition of "destruction," in the interest of parsimony, I operationalize it as "destruction caused to digital information systems" as specified in the introduction. If a cyber attack penetrates a system but leaves it unchanged save for the presence of the malware itself, this will not to meet the definition of cyber war. I make this distinction in order to exclude acts of espionage in cyberspace as potential challenges to DPT, as their real-world analogy—spying—occurs routinely between democracies and is generally not considered to be an act of war. I also exclude operations that delete data that can later be restored (for example, a WIPER attack that deletes files from users' machines while leaving the file server or backups untouched).

If H2 proves to be incorrect and democracies have caused destruction to other democracies' information systems in cyberspace, this would be evidence that DPT's applicability to the cyber domain should be called into question and researched further. Moreover, a true H1 and false H2 would be another data point with which to evaluate DPT's causal mechanisms. If democracies do use cyber weapons against each other for more than espionage purposes, this would imply that the democratic norms explanation for liberal peace is incorrect, as norms should be a constant; they should not change depending on the operational domain, so if there is no norm preventing acts of cyber war against other democracies, this should call into question whether there are norms preventing acts of war against democracies in general (it is possible, though, that norms preventing kinetic conflict with other democracies are more robust and would still hold). The attacks in question are unlikely to lend any evidence to the institutional or capitalist explanations of democratic peace, but they may not invalidate them, either. It is plausible that a democracy seeking to avoid audience costs or unwinnable wars would employ a cyber attack instead of a kinetic one, as it provides the safe haven of plausible deniability; it is also plausible that a democracy would use a cyber attack to achieve its political ends rather than another

type of attack that could damage its economic interests.

I include only examples where attribution appears in a publication by a cybersecurity research organization, in an in-depth journalistic investigation, or where the suspected government sponsor admitted guilt. Attacks rumored to have been committed by a non-democracy were thrown out because I did not wish to run the risk of including irrelevant data points, so attribution to a democracy of any given attack had to be based on more than speculation for that attack to be considered.

Independent and Dependent Variables

Dependent variable. The dependent variable in this study is the existence of cyber attacks between two democracies, because I intend to 1) find out whether they occur, and 2) gain a broad understanding of when and why they happen. In order to do this, I will draw data from two indices of cyber attacks: the Center for Strategic and International Studies (CSIS) Significant Cyber Incidents Index[xviii] and the Dyadic Cyber Incident and Campaign Data Set (DCID).[xix]

These indices serve two different purposes. The CSIS index is a running list of significant cyber incidents across the globe, including state and non-state actors and targets. This provides an overview of the international landscape of cyber conflict, capturing snapshots of incidents that could include any combination of actors that happened at a particular moment in time. The DCID tracks cyber attacks—often ongoing "campaigns" that span many individual incidents—between rival dyads. The DCID documents incidents that range from a single attack to extended exchanges that occurred over a period of years but does not include one-off events between states that have no established rivalry. By using both indices, I hope to create as complete a picture as possible of cyber conflict between democracies.

Independent variables. There are several independent variables at play in this study, which will be discussed in the qualitative analysis of relevant cyber attacks. I will draw evidence from public documents such as media reports and statements by public officials. The independent variables include:

- **Democracy.** Because defining democracy itself is beyond the scope of this paper, I consulted the Economist Intelligence Unit Democracy Index to determine which countries to include. The Democracy Index evaluates countries' levels of democracy based on five categories: "electoral process and pluralism; civil liberties; the functioning of government; political participation; and political culture."[xx] I create dyads using the 75 countries that are rated as either full democracies or flawed democracies; a full list is attached as Appendix A.[xxi] Countries deemed "flawed democracies" have democratic forms of government and are widely accepted to be democracies, but they are less representative, less functional, and less free compared to full democracies.
- **The dyad's relationship.** Are they allies? How closely do they coordinate in other areas? What points of tension exist between them? The democratic dyads in this sample have a high degree of variance in their relationships, ranging from close alliances (for example, the United States and the United Kingdom) to historical strain (such as South Korea and Japan). All other things being equal, it seems logical that dyads with historical rivalries or points of tension in their relationship would be more likely to trade cyber attacks.

- **The government bodies responsible for the country's cyber operations.** For example, is it state security services, the intelligence community, or the military? Is there a civilian body that has oversight? Perhaps certain types of government bodies are more likely to carry out attacks than others.
- **The dyad members' respective cyber capabilities.** Is there a clear imbalance, or are the dyad members' respective cyber programs equally advanced? If, for example, attackers tend to be much more advanced than their targets, this would imply that democracies are willing to deploy cyber attacks against other democracies when they do not fear retaliation or when they are unlikely to suffer large costs should their target choose to retaliate in the cyber realm.
- **The systems targeted in the attack.** Were the targeted systems operated by the government or by private enterprise? Are they considered critical infrastructure? The ownership and uses of breached networks may illuminate the attacker's motivations as well as the perceived level of provocation.

IV. RESULTS AND ANALYSIS

Twenty-two dyads out of a possible 2,775 (75 democratic countries arranged into unique pairs) were found to be positive for cyber attacks. Positive dyads are included as a table in Appendix B. In some cases, multiple dyads are the result of a single incident that included more than one target. The incident that generated each positive result is specified in the table's third column.

There are three perpetrators in this data set—France, the United Kingdom, and South Korea[xxii]—and 20 unique victims. There are also three unique incidents, exactly one for each perpetrator. Each of these incidents is the subject of a case study below.

I note that there are a handful of cyber attacks between South Korea and Japan found in the DCID that I chose not to include here, as I could not find any evidence independent of the DCID itself that presented compelling reasons to believe that they were state-sponsored. Additionally, the Belgacom breach did not appear in either of the data sets I drew from; I happened upon it while researching attacks that did appear in the CSIS and DCID data sets.

Case Studies

1. Animal Farm

The Animal Farm advanced persistent threat (APT) was discovered in 2014 and has targeted governments, journalists, and defense contractors in the U.S., Malaysia, the Netherlands, Germany, the UK, Sweden, Austria, Israel, New Zealand, Canada, Spain, Norway, and Greece.[xxiii] Animal Farm spies on its victims using two primary malware strains, which are referred to as "Babar" and "Casper."[xxiv] While it is thought that Animal Farm's main target was the Iranian nuclear industry when the espionage campaign began circa 2009, Babar and Casper malware have since been used to infect targets in many democracies, and the malware does not appear to cause any damage to infected systems beyond the infection itself.

Researchers long believed Animal Farm to be French, and a rare admission made the attribution certain. Bernard Barbier, former head of signals intelligence for the French Directorate-General for External Security (DGSE), confirmed that the Animal Farm APT was sponsored by the French government in a public speech in 2016,[xxv] but the disclosure attracted little attention.

Independent variables. France, along with four out of the 13 targeted countries, is a flawed democracy. Most victims are France's allies, either through NATO (Canada, the U.S., the Netherlands, Spain, Germany,

Norway, the UK, and Greece) or the European Union (Austria and Sweden). The only non-allied countries that DGSE targeted were Malaysia, Israel, and New Zealand. There are only two countries on the target list with highly sophisticated offensive cyber programs—the U.S. and the UK—and in both, the intelligence community is responsible for cyber operations. Before Animal Farm was discovered, there had never been such a sophisticated cyber campaign launched by a francophone country. So, while France was clearly a capable actor at the time of the attacks with a decisive cyber advantage over most of the targeted countries, the US and UK cyber programs were almost certainly more advanced.

Consequences of the attack. There were no obvious consequences that were borne out publicly despite Barbier's admission of guilt. This study produced no evidence of condemnatory responses or retaliatory actions undertaken by the targeted countries.

2. DarkHotel

Since 2007, the DarkHotel APT has targeted executives in strategic sectors, including the defense industry, while they travel for business.[xxvi] As victims connect to their hotel Wi-Fi, DarkHotel infects their devices with spyware using various attack vectors, including spear phishing and zero-day exploits. The targeting is surgical; DarkHotel appears to know victims' room numbers and expected arrival times and attacks accordingly.[xxvii] DarkHotel has targeted victims in hotels primarily located in Japan as well as in other democracies (India, Indonesia, Hong Kong, Taiwan, the U.S., Germany, and Ireland). I have treated those countries as victims for the purposes of this study, but note one limitation: some individuals may have been traveling internationally when they were attacked. In those cases, it is possible that critical industry in the individual's home country, rather than that of the country where the attack took place, was the intended target.[xxviii]

In an interview with *Wired*, the manager of Kaspersky's Global Research and Analysis Team indicates that the main targets were individuals in North Korea, Japan, and India; "their targeting is nuclear themed, but they also target the defense industry base in the U.S." The campaign is attributed to South Korea because the malware's sophistication indicates a nation-state actor, and the name of a known South Korean coder ("Chpie") appears in the source code.[xxix]

Independent variables. South Korea is a flawed democracy, and DarkHotel has mainly targeted flawed democracies. South Korea and the U.S. are allies, though they are arguably not as closely intertwined as the U.S. is with NATO countries. India-South Korea relations are generally positive, and the two countries are increasing their security cooperation.[xxx] The case of Japan and South Korea is somewhat complicated; they both uphold the East Asian security architecture through hub-and-spoke alliances with the U.S., and though they share intelligence, they are not formal allies in their own right, as relations are often strained due to historical animosities. While the DarkHotel campaign shows that South Korea is a capable actor in cyberspace, it is not a global cyber power and neither are the democracies it targeted, with the exception of the U.S.

Consequences of the attacks. This study found no evidence that South Korea faced diplomatic consequences or retaliation in the wake of DarkHotel attacks.

3. Operation Socialist

In 2013, Proximus, a Belgian state-owned telecommunications company (then known as Belgacom) discovered an extensive breach of its networks by a highly capable actor. The malware used in the attack was made to look like a Microsoft program and ran in the background to exfiltrate data during business hours. After months of searching for the

perpetrator, investigators found that Belgacom was targeted by a British intelligence organization, Government Communications Headquarters (GCHQ), in an attack that GCHQ had dubbed "Operation Socialist."

GCHQ penetrated the network in 2011 through social engineering; they designed fake LinkedIn pages that infected the computers of Belgacom engineers, giving GCHQ wide-ranging network access. From there, GCHQ intercepted traffic sent over "cellphone internet browsing sessions and multimedia messages"[xxxi] to spy on not only Belgacom but also its customers, which included NATO headquarters, the European Parliament, the European Commission, and the European Council. More so, Belgacom maintains subsidiaries and partnerships worldwide allowing GCHQ to intercept communications in South America, Africa, and the Middle East.[xxxii] It is likely that the purpose of the attack was not limited to spying on European institutions, and it is possible that other governments, defense industries, and critical enterprises were targeted.[xxxiii]

According to an investigation by the Intercept, despite the fact that the spyware bore a resemblance to Stuxnet and Flame (both of which are NSA tools), there has been no suggestion that the US government was directly involved. It appears, rather, that the attack was executed using tools shared between the U.S. and the UK, but the UK government has never officially acknowledged its role in the attack.

Independent variables. While the UK is a full democracy, Belgium is a flawed one, and the two countries are close allies; both are members of NATO and both were members of the European Union at the time of the attack. The UK is one of the world's most advanced cyber actors, while Belgium has no known offensive cyber capability to date. It is unlikely that the GCHQ feared retaliation in cyberspace.

Consequences of the attack. Per an investigation by the Intercept, Belgacom "was forced to replace thousands of its computers at a cost of several million euros."[xxxiv] While the attack did evidently cause damage to systems and necessitated an expensive clean-up, it is not evident that damage was the intention. Operation Socialist appears to have been an espionage operation, albeit a destructive one, which is a bit of a gray area; if a spying operation caused extensive damage to physical infrastructure, it would be highly provocative. *The Guardian* reports that "Elio di Rupo, the Belgian prime minister at the time, promised to take 'the appropriate steps' if the 'high-level involvement' of a foreign country was confirmed," but it is unclear that the UK faced any real consequences,[xxxv] while Europol, the law enforcement agency for the European Union, refused to assist Belgium in its investigation.[xxxvi]

Patterns

A few notable patterns emerge in the results of this study. First, all 22 positive dyads involve at least one flawed democracy, and two out of three perpetrators are flawed democracies (France and South Korea). This pattern suggests that 1) flawed democracies may be more willing than unflawed democracies to perpetrate attacks on other democratic states, and 2) unflawed democracies may be more willing to attack flawed ones. (However, flawed democracies are more than twice as numerous as full democracies, so this result was more likely all other things being equal). Further, two out of three perpetrators—France and the UK—are past hegemons, suggesting that they may feel they have a right to interfere in the affairs of others.

All three perpetrators are powerful, capable countries, and each attack mentioned is highly sophisticated, illustrating that

effective cyber attacks are neither cheap nor easy. In fact, they require high capacity and plentiful resources.[xxxvii] Despite being asymmetric, cyber attacks are not frequently deployed by weak states or by states who are not able to marshal resources efficiently; if attacks were easy to perpetrate, then we might expect that to be the case. The future will probably see more of the same—the strong doing what they can and the weak suffering what they must—than a complete reversal of fortunes, where weak countries undermine the strong ones through asymmetric means.

Interestingly, most positive dyads in this study are allied. Both countries that attacked the U.S. are allies; 11 dyads—exactly half—involve a security alliance (10 dyads involve one NATO country attacking another, and South Korea has a security alliance with the U.S.), and eight involve two EU member countries.[xxxviii] However, there is no evidence of Five Eye countries attacking each other. Therefore, although cyber attacks occur even within security alliances, the closest allies have so far avoided them.

Evaluation of Results

There are a few important caveats to consider, which would be true of virtually any study on cyber attacks. First, it is always possible that a given attack was a false flag, whose true origin was cleverly masked by the developer. One could hypothesize that this is the case in any of the incidents I have analyzed above, but the evidence I have used for attribution is strong in that it does not rely on the clues that are easiest to fake (such as IP addresses, which are easily masked by a Virtual Private Network). Further, a false flag hypothesis would not be falsifiable using open-source data, so I have paid little attention to debunking it. Second, in the case of espionage, it is difficult to rule out the possibility that the government of the targeted country gave under-the-table consent to the country doing the spying, especially if the primary target in the attack was a non-government entity. This could be true even in the presence of diplomatic backlash after the discovery of a security breach, as the consenting government would likely have to feign outrage in order to placate its constituents and avoid the appearance of kowtowing to another state. Finally, there is the possibility of contagion—that malware was unintentionally passed on from its intended targets to additional victims who then became collateral damage. This is, quite frankly, an externality for which it would be almost impossible to control. With that said, an evaluation of each of the original hypotheses follows:

H1: Democracies employ cyber attacks against each other.

In light of the three unique instances of democracy-on-democracy cyber attacks found in this study, H1 can be accepted as true. Democracies do attack other democracies in cyberspace, even if it appears that they do so only rarely. However, they may do so more often than this evidence suggests, as there may be other relevant incidents not known in open sources and outside the scope of this research. Additionally, democracies may be responsible for attacks that have been wrongly attributed to other actors or that have not been attributed because the perpetrators successfully obfuscated their identity.

H2: Known cyber attacks between democracies do not meet the definition of cyber war.

As each of the three attacks was motivated by espionage, H2 can also be accepted as true. None of the incidents amount to a government engaged in destruction against another in cyberspace where the destruction was the goal, and thus none of them meets my definition of an act of cyber war. (While the Belgacom breach did cause material damage, the damage was not in itself the goal of the attack.) As none of the studied attacks can be

considered an act of war, it appears that democratic peace does hold in cyberspace. Thus far, democracies have only been willing to use measures short of cyber war against each other.

V. POLICY RECOMMENDATIONS

While the U.S. is on the right trajectory and should double down on its current cyber efforts to defend its systems, the main implications of this study for US cybersecurity policy are the following: 1) the U.S. should continue to share threat intelligence with allied democracies and help to build other democracies' cyber capacity; 2) the U.S. should pursue cyber treaties and arms control with its allies *if and only if* adversary nations are also willing to sign on to those regimes; 3) the U.S. must ensure that government cyber programs are as well-resourced as possible, as it is imperative to stay ahead of both ally and adversary competition in cyberspace; and 4) the US government should consider naming cyber attackers whenever it is reasonable to do so.

Information Sharing and Capacity Building

The 2018 US National Cyber Strategy emphasizes building international capacity and sharing threat information with friendly countries.[xxxix] But is this truly a good idea in light of the fact that democracies—the block of nations with whom we would most likely be building capacity and sharing intelligence—may use that increased capacity and shared intelligence to attack the U.S.? While it may seem logical for the U.S. to protect itself by not sharing information that would help others execute attacks, in practice, *sharing intelligence would preclude the intelligence being weaponized to the U.S.'s detriment.* It would be risky for a country who receives highly classified US cyber intelligence to weaponize that intelligence against the U.S., given that such privileged information is only shared with a small pool of actors, and they could implicate themselves in the attack if they used it. However, it is important to note that this logic only holds if the information is shared with a sufficiently limited number of nations, for example, the Five Eyes or NATO. The wider the pool, the more numerous the potential suspects and the less likely any given country would face consequences for biting the hand that fed them. Still, it is important to bear in mind that any intelligence shared with ally democracies could potentially be used to attack third-party democracies. But the inherent risk of proliferating capable cyber actors may be acceptable if it is deemed more likely that they will act according to the U.S.'s interest than against it.

The question of capacity building is perhaps an easier one to answer. If the goal is to limit the risk cyber attacks pose to the U.S., it seems clear that the U.S. should not work to build the offensive capacity of other nations, as that capacity may then be used to create cyber weapons that could be used against the U.S. Ideally, the U.S. would work to build others' defensive—not offensive—capacity. Whether this is possible in practice is for policymakers to decide.

Cyber Arms Control

If the U.S. faces cyber threats from democracies, it would seem sensible to pursue cyber arms control with allies and other democratic states. But to do so would be misguided unless adversary nations—such as China, Iran, Russia, and North Korea—sign on as well, which is unlikely. The reasoning behind this is simple: if the U.S. and other democracies agree to limit their use of cyber weapons while others continue to pursue them, the countries who have signed on will be at a disadvantage. This is not to say that an all-encompassing arms control treaty for cyberspace, similar to the Treaty on the Non-Proliferation of Nuclear Weapons, is not worth pursuing. On the contrary, it could be a very positive development. However, it seems unlikely that actors who are highly capable in cyberspace but weaker in other

dimensions of state power would be willing to give up such a useful asymmetric tool. It would be prudent for the U.S. to advance a United Nations convention on norms for cyber weapons use in hopes that a control regime that includes our adversaries is possible in the future. But unless and until that moment comes, the U.S. should sign no such treaty.

Maintaining the Advantage

Perhaps the most important implication of these findings is that the U.S. must work to maintain the advantage in cyberspace, both over its adversaries and its allies. Policymakers should expect that other democracies—even friendly ones—will target the U.S. for espionage if they believe they can get away with it or believe it is worth the risk. It is important, then, to deter other countries by making them believe that they *will not* get away with spying on the U.S. and may face repercussions for doing so. To achieve this, the U.S. must continue to have the most advanced cyber program to identify its attackers and retaliate if necessary; having the best offense is an essential defense.

To stay on top, the U.S. must adequately resource its cyber programs, make research and development a priority, and employ the most competent workforce the country can muster. The latter is easier said than done, as there is a large disparity between a cybersecurity professional's expected earnings in the public sector versus the private sector in the U.S. The Department of Homeland Security's initiative to competitively compensate cybersecurity professionals by offering bonuses is a step in the right direction.[xl] Another viable option to attract talent would be to organize a unit of volunteers skilled in cybersecurity and cyber operations, similar to Estonia's volunteer Cyber Defense Unit (CDU). CDU volunteers serve as reservists under the Estonian national guard and commit to a few weeks of active duty each year. If this model were adopted by the U.S., it would allow cybersecurity professionals to serve their country on a part-time basis. As there are likely many cyber experts who would like to serve but cannot justify public sector work when the government will likely not be able to pay them on a scale comparable to that of the private sector, a volunteer unit would be a sensible compromise. This, in conjunction with raising pay caps for cyber experts, would help to fill the government's needs and attract the best talent.

Of course, preserving the advantage while also sharing intelligence and building others' capacity will be a balancing act. US policymakers should want other nations to be competent defenders of their own cyberspace but not so competent that they go on the offensive and develop an ability to evade the U.S.'s own defenses. By diverting necessary resources to the development of cyber tools and attracting a cadre of highly capable professionals, the U.S. can hold its nearest peer competitors at a comfortable distance.

Naming and Shaming

This study has shown that democracies face few consequences when attacking other democracies in cyberspace. They are rarely, if ever, called out by their victims even when attribution is relatively certain. Consequently, many democracies will accept the minimal risk of getting caught and will continue to attack others because the strategic benefits outweigh the potential costs. With that said, is it still reasonable for nations to refuse to admit that they have been compromised when they know who their attackers are? I would argue that it is not. While no country wants to admit that its critical infrastructure has been breached, suffering the short-term pain of naming the attacker could be well worth the long-term deterrence it would achieve. Democracies' legitimacy in the eyes of others rests, to some degree, on the appearance of adhering to the norms they espouse; it stands to reason that

democracies might find the costs of attacking other democracies unacceptable if their targets are willing to name and shame them.

VI. CLOSING THOUGHTS

This paper has systematically examined several examples of democracy-on-democracy cyber attacks, discussed their applicability to international relations theory, and analyzed their practical application for policymakers. In addition to these insights, the results have implications for the intersection of international relations and technology more broadly. If readers take just one idea from this paper, it should be this: democracies may attack each other in cyberspace when they believe they can get away with it, and we should be wary that offensive technology may be employed not only by our enemies but also by our friends.

Still, recalling Mearsheimer and Spiro's valid criticisms of the small sample size used to construct DPT: this study sampled only a small handful of cyber attacks, and its results should not be taken as gospel. While I have attempted to illuminate a small corner of the cyber domain, much work remains to be done. In the future, others might consider expanding on this research by consulting other cyber conflict databases and investigating attacks not covered here.

APPENDIX A: Democratic Countries		
Argentina*	Hong Kong*	Paraguay*
Australia	Hungary*	Peru*
Austria	Iceland	Philippines*
Belgium*	India*	Poland*
Botswana*	Indonesia*	Portugal*
Brazil*	Ireland	Romania*
Bulgaria*	Israel*	Senegal*
Cabo Verde*	Italy*	Serbia*
Canada	Jamaica*	Singapore*
Chile*	Japan*	Slovakia*
Colombia*	Latvia*	Slovenia*
Costa Rica	Lithuania*	South Africa*
Croatia*	Lesotho*	South Korea*
Cyprus*	Luxembourg	Spain
Czech Republic*	Malaysia*	Sri Lanka*
Denmark	Malta	Suriname*
Dominican Republic*	Mauritius	Sweden
Ecuador*	Mexico*	Switzerland
Estonia*	Mongolia*	Taiwan*
Finland	Namibia*	Timor-Leste*
France*	Netherlands	Trinidad and Tobago*
Germany	New Zealand	Tunisia*
Ghana*	Norway	United Kingdom
Greece*	Panama*	United States*
Guyana*	Papua New Guinea*	Uruguay

*=Flawed democracy

APPENDIX B: Dyads Positive for Cyber Attack			
Dyad	Perpetrator	Victim	Incident
France-Canada	France*	Canada	Animal Farm
France-United States	France*	United States*	Animal Farm
France-Netherlands	France*	Netherlands	Animal Farm
France-Spain	France*	Spain	Animal Farm
France-Germany	France*	Germany	Animal Farm
France-Norway	France*	Norway	Animal Farm
France-Malaysia	France*	Malaysia*	Animal Farm
France-United Kingdom	France*	United Kingdom	Animal Farm
France-Greece	France*	Greece*	Animal Farm
France-Sweden	France*	Sweden	Animal Farm
France-Israel	France*	Israel*	Animal Farm
France-Austria	France*	Austria	Animal Farm
France-New Zealand	France*	New Zealand	Animal Farm
South Korea-Japan	South Korea*	Japan*	DarkHotel
South Korea-India	South Korea*	India*	DarkHotel
South Korea-United States	South Korea*	United States*	DarkHotel
South Korea-Indonesia	South Korea*	Indonesia*	DarkHotel
South Korea-Hong Kong	South Korea*	Hong Kong*	DarkHotel
South Korea-Taiwan	South Korea*	Taiwan*	DarkHotel
South Korea-Germany	South Korea*	Germany	DarkHotel
South Korea-Ireland	South Korea*	Ireland	DarkHotel
United Kingdom-Belgium	United Kingdom	Belgium*	Operation Socialist

*=Flawed democracy

Just Robots, Just Collection: The Implications of Lethal Autonomous Weapons Systems for Ethical Intelligence Collection

Ainikki Riikonen

Artificial intelligence has the potential to revolutionize the way nation-states fight wars. However, these emerging advancements come with pressing questions about ethics. One well-studied dilemma is that posed by lethal autonomous weapons systems (LAWS) and how they might behave on the battlefield. A complementary question is what LAWS' targeting systems could mean for the ethical dimensions of data and intelligence collection. This article explores the ethics of collection in support of hypothetical LAWS through a Just War lens. It frames existing targeting practices and technologies as a bellwether for LAWS, targeting, and collection. It concludes that increases in weapons systems precision could paradoxically pose hazards to discrimination and proportionality in collection.

Weapons systems are growing increasingly precise. The precision revolution has prompted stricter standards for warfighters to assess collateral damage and therefore mitigate civilian casualties.[i] Improvements to precision are possible because of the evolution of sensors and because of expansive battle networks that channel diverse information into targeting decisions. Since 2001, the United States has deployed armed drones on the battlefield. These platforms, in addition to delivering munitions, conduct persistent collection. Human teams work with machine-based collection and processing tools to identify, track, and engage targets.

A future step in this evolution could be lethal autonomous weapons systems (LAWS). LAWS are "defined by the ability to complete the engagement cycle—searching for, deciding to engage, and engaging targets—on their own."[ii] Autonomy is defined by freedom in time and space rather than by the sophistication of the system, but increased sophistication will likely involve artificial intelligence (AI) and particularly machine-learning, a data-intensive technique of AI.[iii] The current generation of AI systems is not yet flexible, reliable, or robust enough for deployment on the battlefield, but the possibility of future deployment poses questions not only about the use of force and for the decision-making behind it, but also about potential ethical ramifications for the intelligence processes that support this application of force. This research examines the intelligence collection requirements that could support these LAWS' targeting systems. Rather than explore the limitations of machine-learning as a technology, which has been studied in depth, it focuses on the hypothetical intelligence collection processes that could enable autonomous target identification in the field and the ethical implications for those collection processes.

To assess the implications of LAWS for the ethics of intelligence, this analysis begins by outlining general criteria for ethical intelligence collection according to an intelligence-focused application of the Just War tradition. Following, it turns to existing technologies and practices that may act as bellwethers for LAWS. While not exact indicators for how onboard targeting systems might work, these offer analogous insights that are useful for consideration. These bellwethers include precision-guided weapons (PGWs) which illustrate the relationship between onboard sensors and intelligence requirements. It also includes an

examination of the targeting practices behind drone strikes, especially the collection of signals intelligence (SIGINT) and analysis leveraging machine-learning tools. Finally, it applies these observations to LAWS as they may be employed on the battlefield and assesses the data collection requirements against the Just War criteria. It finds that the robust SIGINT collection and processing capabilities that LAWS would employ cannot displace the human ability to provide context. This context is essential for the lawful application of force. Moreover, while increasing data collection could make LAWS more precise and more discriminate, the increase would paradoxically erode discrimination and proportionality of data collection.

ETHICAL FRAMEWORK

The U.S. Department of Defense regards law of war standards as *minimum* legal standards and applies these standards to its policies on LAWS.[iv] These law of war principles include military necessity, humanity, proportionality, distinction, and honor.[v] With regard to autonomy in weapon systems, it notes that "The law of war does not prohibit the use of autonomy in weapon systems" and that potentially, "the use of autonomy could *enhance* the way law of war principles are implemented in military operations."[vi] It notes that weapons, as "inanimate objects," cannot make legal decisions but that "Law of war obligations of distinction and proportionality apply to persons rather than the weapons themselves." Military commanders are obligated to use weapons that are not "inherently indiscriminate," so if the Department of Defense were to develop LAWS, it would need to develop them accordingly. If LAWS were to be developed with targeting systems rooted in machine-learning, they would require substantial data support. The ethics of deploying LAWS is outside the scope of this research, but the supporting information collection process poses its own questions and challenges.

Scholars of intelligence have pointed to Just War principles as a framework to "tease out the ethical implications of intelligence activity."[vii] The framework includes *jus ad bellum*- and *jus in bello*-derived principles of last resort, right intention, probability of success, regard for human consequences, proportional means, and discrimination.[viii] In a simplified form, these scholars pose that intelligence collection should commit "minimum trespass"; human costs of invasiveness and injustice should not outweigh the outcomes.[ix] The threat of overreach, however, must be balanced with that of under reach. Zehfuss claims that "Many of the spectacular 'mistakes' in recent wars have indeed not been due to weapon failure but—or so it was claimed—to intelligence failure."[x] Overreach risks disproportionate invasions of privacy but, on the battlefield, under reach could also put civilian lives at risk by not providing enough information to discriminate targets. The question, then, is the minimum trespass required to ensure warfighters can deploy LAWS with respect to law of war principles.

CURRENT TECH: HONING AND TARGETING

Current technologies, and the collection processes around them, could indicate what processes would ultimately support LAWS operations. The example of PGWs illustrates the relationship between automated terminal guidance, onboard sensors, and intelligence requirements. The targeting practices behind contemporary drone operations, which rely heavily on SIGINT and use machine-learning tools for analysis, demonstrate the limitations of these methods and highlight the importance of human operators and human judgment in decisions to apply lethal force. Overall, increases in precision capabilities, combined with the information revolution

mean a "move from segregation of ops and intel to integration of ops and intel."[xi] These processes and technologies offer a snapshot of the way the application of force is evolving to require fewer weapons, less time, and more sensors.[xii]

Precision-Guided Weapons

PGWs are "smart" munitions because of the robust intelligence architecture that supports them.[xiii] These weapons home in on human-selected targets and do so with either a "human-in-the-loop" where a person "paints" a target with a laser designator that onboard sensors detect or through an autonomous terminal guidance system.[xiv] A report from RAND describes this autonomous process as follows:

> "To attack a target the PGW first uses its target-imaging sensor to create an image of the target area and then uses its autonomous target-acquisition algorithm to precisely locate the aimpoint within the imaged scene. The algorithm uses a reference template (or sequence of templates), developed during the mission planning process, to identify the aimpoint. The form of the template depends on the type of target-imaging sensor the PGW uses."[xv]

The human decision-makers use a vast array of networked sensor platforms, called a battle network, to accumulate information before carrying out PGW strikes.[xvi] Mission planners could use imagery or measurements and signatures to build the reference template for the aimpoint, depending on the composition of the weapons' sensor array. Planners also include contextual objects, such as terrain features or neighboring structures, to increase accuracy and decrease the likelihood of false positives; a larger combination of features creates a more unique reference point.[xvii] In sum, the targeting process behind PGWs entails humans assessing all-source intelligence to select targets, then compiling information to suit the PGW's sensor requirements. Mission planners include additional data on nearby military and non-military objects to increase the accuracy of PGW terminal guidance systems. The collection and inclusion of additional data decreases false positive rates and mitigates collateral damage.

Drone Operations

Despite the scale of data collection and the sophistication of analytical tools behind targeted drone strikes, the targeting process benefits from human operators to acquire information and human analysts to provide context and judgment. While publicly available information probably only offers only a sliver of visibility into drone targeting practices, open sources illuminate some of the shortcomings of SIGINT and of machine-learning for target selection. Drone strikes generally fall into two categories: "personal strikes," where the identity of the target is known, and "signature strikes" where the target is determined by pattern-of-life but the exact identity may be unknown.[xviii] The amount of information collected for both types of strikes, including by loitering unmanned aerial systems (UAS), is massive but has limitations.

Collection entails a variety of lines of effort. Lt Gen David Deptula, one of the architects of the U.S. Air Force's drone program, said that "ISR [intelligence, surveillance, and reconnaissance] today *is* operations."[xix] UAS collect imagery intelligence (IMINT) by loitering for hours and capturing full motion video. They have collected SIGINT through various means such as the Shenanigans device which, deployed on UAS, "vacuums up all Internet data from computers, routers, and smartphones within reach."[xx] The Gilgamesh system geolocates SIM cards under the premise that a cell phone generally

belongs to one individual. On the ground, the Central Intelligence Agency used biometric sensors to confirm the identity of al-Qaeda members and gained access to computers with the Polarbreeze tool which "wirelessly taps into nearby computers."[xxi] Ninety percent of high value target (HVT) operations were initiated by SIGINT, but human intelligence (HUMINT) operations enable 70 percent of the National Security Agency's (NSA) exploitations.[xxii] Growing sensor-based collection, enabled in part by the ability for a platform to loiter, supersizes data collection and may pose challenges for proportionality and distinction in collection.

The U.S. Intelligence Community is acquiring bigger amounts of data and may be incentivized to do so because of machine-learning systems' reliance on large datasets. The NSA supposedly collects millions of faces daily "for use in a sophisticated facial recognition program."[xxiii] The Skynet program, used for the pattern-of-life analysis behind signature strike decisions, relied on phone location and bulk phone metadata to identify "suspicious" patterns in travel and communications habits.[xxiv] But bulk metadata collection faces a number of ethical challenges. First, bulk collection does not discriminate between persons of interest and innocent bystanders. And even after analyzing the data, HUMINT is important for distinguishing between targets and false positives.[xxv] The U.S. military faced a similar problem when tracking satellite phones in Iraq; the identity of the person holding the phone was not always clear.[xxvi] Second, mass collection may not be proportional if analysts are combing through only to find a small set of targets. The backlash to the Skynet program's exposure following the Snowden leaks suggests that Americans view the program as a violation of privacy.

Pattern-of-life analysis powered in part by machine-learning is a powerful tool for targeting, but mishaps showcase how reliance on machine-made decisions could lead to avoidable civilian casualties. In a famous case, Skynet misidentified Al Jazeera journalist Mouaffaq Zaidan as a terrorist based on his travel and communications patterns.[xxvii] In reality, those patterns reflected his location and phone practices when meeting with sources. The philosopher Chamayou depicts the U.S. government's perception of these targeting practices this way: "Our procedures and practices for identifying lawful targets are extremely robust, and advanced technologies have helped to make our targeting even more precise."[xxviii] In this case however, the targeting was precise—it drew one data point of interest out of an entire collection—but it was inaccurate. It failed to discriminate a lawful target because it lacked context. This case demonstrates the pitfalls of machine-learning, including opposition to mass data collection practices, and emphasizes the importance of human judgment to apply context to ensure discriminate action.

The PGW example demonstrates that machines can identify unique, pre-selected targets if given enough data that is compatible with their sensor payload. In this case, human actors have selected a target based on threats or objectives and have curated a reference template so the munition can guide itself to an aimpoint. In contrast, the targeting processes behind drone strikes demonstrate the capabilities and limitations of signals-focused targeting practices enabled by loitering collection platforms, big data collection, and analysis by machine-learning systems. It also highlights public sensitivities to bulk data collection.

MAKING GOOD CHOICES: STRATEGIC ROBOTS

The U.S. Department of Defense mandates that warfighters deploy LAWS in compliance with law of war principles including military necessity, distinction, and proportionality.[xxix] Intelligence collection in support of these

principles ought to, according to ethical frameworks, exercise minimum trespass. But because machine-learning as the technology stands requires massive amounts of data to train and function—and to do so with precision—that minimum may be high. This following section explores some of the information requirements for ways LAWS may operate. These include strikes against human pre-selected targets and attacks on machine-selected targets.

LAWS may be desirable because they reduce communications demands but reducing communications would likely take humans out of the machine's observe, orient, decide, and act (OODA) loop. Taking a human out of the loop delegates decision-making (although not responsibility). For example, "autonomous onboard planning algorithms can help reduce communications loads…and can potentially automatically detect and track targets using pattern recognition."[xxx]

Detection and tracking of targets could involve specific human-selected targets or a class of targets. Both types of targets have implications for the ethical conduct of intelligence collection, especially when collection must enable discrimination and proportionality. Paradoxically, *an increase in precision for the use of force will likely mean implementing a high threshold for minimum trespass*.

Human-Selected Targets

In the instance of human-selected targets, a human has already determined who is the target and, implicitly, how many there are. Thus, a human actor has delineated discrimination and proportionality already; the LAWS will need to correctly identify that target and exert force without collateral damage to potential bystanders. Like PGWs, the LAWS will need target indicators that are compatible with its sensors. To target personnel, these could be biometric data for facial recognition, gait recognition, voiceprint recognition, or cardiac signature recognition which would likely produce fewer false positives than scanning for cell phones or other auxiliary devices.[xxxi] Acquiring data of someone's face for recognition is generally possible in the open source or with a camera and entails relatively low trespass.[xxxii] Cardiac signatures can be collected in public at range with a laser. Whether the humans have committed overreach in the *selection* of the target is outside the scope of this particular scenario. Once the target is selected, acquiring data for positive identification, due to the availability of sensors and processing for biometric identification, is within the bounds of minimum trespass. This level of specificity and precision of force, if known to adversaries, could create collateral psychological damage, however: "Knowing that an adversary could focus their efforts in such a personalized way could itself inflict psychological trauma."[xxxiii] At a high level of abstraction, non-combatants could take heart at their decreased risk of exposure to violence. But in reality, the fear of heavy surveillance reaps its own psychological costs. Mission planners would need to build this consideration into their operations as they consider costs and benefits.

Machine-Selected Targets

Targeting systems on board LAWS would confront similar challenges to SIGINT-focused and machine-leaning based processes behind drone campaigns: a lack of context despite massive data requirements. This lack of context would impact their ability to behave proportionally, according to commander's intent, even if they can correctly identify combatants.

To target discriminately, LAWS' targeting systems could be modeled after personal strikes. The collection of massive amounts of data, like military personnel databases, could assist discrimination if LAWS can match potential targets to specific identities. Confirmation of specific identities would

mitigate civilian casualties, but such a method would only be practical if the data were expansive enough to cover all combatant individuals within a zone of engagement. If combatants primarily come from non-state groups, such data might not be available. Mission planners would likely use open source information in addition to other information to find identity matches; however, AI-assisted facial recognition would not discriminate between combatant data and bystander data. Some U.S. government groups already use services like Clearview AI that scrape the open source to find matches for pictures.[xxxiv] Some scholars of intelligence ethics assert that open source intelligence (OSINT) is preferable because it is the least invasive approach, but backlash to facial recognition efforts suggests that mass biometric collection from public mediums is qualitatively invasive. Moreover, the ethics imperative for intelligence is not only about right and wrong but about the potential reputational costs of activities. Massive data collection, whether from the Internet or from foreign military databases, for the purpose of training autonomous targeting systems would impose huge reputational costs on the United States. The paradox of precision is that it would "extend the field of fire to take in the entire world," at least in intelligence terms.[xxxv] If it helps to prevent civilian casualties, the outcome would outweigh the costs, but at a severe risk to the United States' reputation.

Alternatively, autonomous targeting systems could use a method akin to the signature strike. The system's engineers could train it on the signature and pattern of activity of a combatant. Indicators could include uniforms and equipment as recognized by computer vision systems or electronic signatures picked up by other sensors, or ideally an expansive combination of factors to mitigate false positives. Nonetheless, false positives are likely, as this method would face similar shortcomings to NSA's Skynet. Without context, this type of system could categorize the journalist as a terrorist in a failure of distinction.[xxxvi] Such a system could identify who *looks* like a combatant but not who *is* a combatant. This method would require human inputs to give context.

Even if a system successfully discriminates combatants, it would struggle to act proportionally without inputs from humans to signal commander's intent and identify military necessity. Heather Roff describes the "strategic robot problem" where LAWS would struggle to know *why* a target would satisfy military objectives.[xxxvii] Machine-learning systems are adept at identifying correlations but have no conception of causation. One solution to this limitation is the manned-unmanned team where LAWS could absorb and fuse diverse sensor data to build battlefield awareness for humans. These human decision-makers can understand intent and objectives and can inform machines' applications of force. Even if they do not choose specific targets, these operators could determine the time and place of kill boxes. Within these kill boxes—originally zones where air assets do not need further authorization from a commander—LAWS can be deployed with proportionality because they are limited to zones designated to satisfy greater contextual objectives. LAWS could better navigate the strategic robot problem with human inputs to guide the way.

CONCLUSION

Advances in technology have introduced concerns about "killer robots." While LAWS could be prized for their ability to operate with little supervision, human operators would need to be confident that they can deploy LAWS in compliance with law of war principles. Training autonomous targeting systems, if they rely on machine-learning, would require extreme amounts of data. Discriminate targeting is paradoxical;

increased precision in targeting could require near-indiscriminate data collection. This scale of data collection poses challenges for the ethical intelligence collection. If the United States were to carry out such a data collection program to train LAWS, it would also need to consider the risk of adverse reputational costs if or when this activity became publicly known. But even if LAWS were trained to exercise discrimination, military necessity and proportionality is key for the use of force, and in this way humans will remain essential.

China's Influence in Central and Eastern Europe, European Responses, and Implications for Transatlantic Security

Julia Warshafsky

This paper examines some of China's primary efforts to influence the economic, political, and civil society landscape in Central and Eastern Europe—a region that has risen in geostrategic importance for China and become increasingly susceptible to Beijing's appeals. It analyzes the impact of China's efforts on transatlantic unity and security, as well as on U.S.-EU cooperation to address the numerous challenges posed by China's rise on the continent and beyond. As competition with China constitutes the chief security priority for the United States, and our European allies and partners will be critical to any U.S. strategy for curbing China's adverse influence activities as this competition evolves, this topic should be of interest to and closely monitored by U.S. policymakers and academics alike.

China has expanded its economic and political influence in Europe in recent years, as it seeks to boost both its economic growth and soft power abroad.[i] One region Beijing has prioritized within this context is Central and Eastern Europe, which it views as a key entrance to Western European markets—one offering a more favorable regulatory environment than that of Western Europe—and as providing auspicious political conditions for promoting its policy agendas and political-economic model.[ii] China's influence in this region is a timely issue with important implications for transatlantic security, as Europe, the United States, and now NATO seek to grapple with the strategic challenges China poses to their individual and collective interests.

This paper examines a selection of China's efforts in Central and Eastern Europe over the last decade, focusing on the "17+1" initiative; China's economic activities in Central and Eastern European (CEE) countries, particularly its investments related to major Belt and Road Initiative (BRI) infrastructure projects; and its use of civil society, academia, and the media to shape regional narratives in its favor. It also reviews European responses to China's activities to date, including CEE and European Union (EU) attitudes toward Beijing, analyzes what China's growing footprint in this part of Europe means for transatlantic relations and security, and considers opportunities for enhanced transatlantic cooperation to address and mitigate negative influence in the region.

The 17+1 (Formerly 16+1)

In 2012, China's Ministry of Foreign Affairs initiated the Cooperation Between China and Central and Eastern European Countries, or "16+1," to promote and strengthen China-CEE relations in areas spanning investment, trade, infrastructure, education, and culture.[iii] The initiative initially included China, 11 EU member states (Bulgaria, Croatia, the Czech Republic, Estonia, Greece, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia, and Slovenia), and five Balkan countries (Albania, Bosnia and Herzegovina, North Macedonia, Montenegro, and Serbia).[iv] After becoming increasingly involved in the group and a major beneficiary of Chinese investment, Greece officially joined in 2019, and the initiative was relabeled the "17+1."[v] All but three CEE members are in NATO, four are candidates to become EU member states (Albania, North Macedonia, Montenegro, and Serbia), and one is a potential candidate for membership (Bosnia and Herzegovina). All members' heads of

state have met in annual summits in Europe and once in China since 2012.[vi] China was set to host the forum's ninth summit in April 2020, but postponed the gathering indefinitely in the wake of the coronavirus pandemic.[vii]

Originally founded as the 16+1, these states became a key platform for Beijing to promote the BRI in Europe. By investing in infrastructure in CEE countries, China sees profit-earning business opportunities as a means to build support for its government and gain credibility on the European stage. CEE nations largely welcomed the formation of the 16+1 with enthusiasm, as well as the investment offers that followed.[viii] All 17 CEE countries now in the format have formally endorsed the BRI through memoranda of understanding with Beijing, and a number have signed on to infrastructure projects as part of the initiative.[ix] As many are struggling economically and are disillusioned with the continuation of unequal development across Europe, the 16+1 sparked hope for meeting acute infrastructure needs and addressing other ongoing economic challenges.[x] It also created a way for CEE nations, which had seen consistent underrepresentation in prior EU-China summits, to engage China's leaders directly and command a stronger voice in Europe-China policy discussions.[xi]

EU officials and larger member states, particularly Germany, have become increasingly critical of the 17+1, arguing that the format dilutes EU unity and prevents Europe from speaking with "one voice" on China.[xii] These leaders, as well as senior U.S. national security analysts, have warned that Beijing uses the 17+1 and related investments in CEE countries to garner support for policy agendas that challenge Western interests and values and market its political-economic model to illiberal-leaning governments.[xiii] These concerns are justified. On at least four occasions, China's influence and lobbying efforts have translated into direct political leverage in Brussels. In 2016, Greece, Hungary, and Croatia opposed direct reference to China and any non-neutral language in a joint EU statement addressing a Hague tribunal ruling that struck down Beijing's territorial claims in the South China Sea.[xiv] In 2017, Hungary refused to sign a joint letter denouncing the torture of detained lawyers in China, and Greece blocked an EU statement condemning China's human rights record at the UN Human Rights Council.[xv] This marked the first time the EU failed to make a joint statement at the UN body. Later in 2017, Greece, the Czech Republic, and several Western European countries sought less targeted language in an EU policy creating a centralized framework to screen foreign direct investment (FDI), with Greece specifically citing Chinese investment as a justification for its position.[xvi]

In response, the EU has stated that member states' bilateral relations with China, including in group settings such as the 17+1, should be coordinated with the EU to ensure activities align with EU laws and policies and benefit the bloc as a whole.[xvii]

Evidently, China has become more sensitive to the EU's criticisms. In 2017, Beijing directed Chinese think tank scholars to survey EU and European attitudes toward the 17+1, requesting particular focus on German perceptions.[xviii] China recently has also sought to accommodate certain EU demands, such as granting it observer status in future 17+1 meetings, and to stress that it respects EU rules and standards.[xix] Many CEE nations, however, decry the hypocrisy of some larger Western members—especially France and Germany—in condemning bilateral China-CEE ties, pointing out that these countries enjoy privileged "1+1" relations and frequent high-level engagements with Beijing.[xx]

Economic Activities in CEE Countries

To date, the highest levels of Chinese investment in Europe have remained concentrated in Western countries, in particular the EU's four largest economies: United Kingdom, Germany, France, and Italy.[xxi] However, CEE nations have seen an increasing share in recent years, even as total Chinese FDI in Europe has declined from its peak of about $41 billion (€37 billion) in 2016.[xxii] Investment in Central and Eastern Europe is also concentrated in a handful of countries: Hungary, Poland, Bulgaria, the Czech Republic, and Slovakia have received nearly 95% of Chinese FDI in the region.[xxiii] These nations and others saw steep increases between 2017 and 2018, with investment growing by 162% in Poland, 185% in Hungary, 355% in Croatia, and over 1,000% in Slovenia.[xxiv] Trade flows between the CEE region and China have also increased considerably, rising from $32 billion in 2009 to $58 billion in 2016.[xxv] This figure, however, fell well short of a China-CEE objective to reach $100 billion in trade by 2016.[xxvi] Similar to investment patterns, the majority of trade is concentrated in five countries, with Poland, the Czech Republic, Hungary, Slovakia, and Romania accounting for nearly 80% of the total.[xxvii] Although CEE exports to China have increased, the balance is decidedly tilted in Beijing's favor, as trade and market access barriers continue to restrict CEE firms' opportunities in China.[xxviii] As Beijing had pledged to help CEE states reduce these deficits, the rising imbalances are a growing source of disillusionment in the region.[xxix]

Since the 16+1 was established, China has vowed to contribute over $15 billion toward infrastructure and other investment in CEE states, in areas including energy, transportation, manufacturing, real estate, information and communication technology, and mergers and acquisition.[xxx] Investment deals increased significantly amid tightening European austerity measures adopted after the 2008 global financial crisis; these deals promised to compensate for the EU's limited financing options to support CEE development after the crisis and to provide an alternative means for CEE countries to recover from recession.[xxxi]

The largest Chinese investments announced within the 17+1 format are set to fund major BRI infrastructure projects, including a $1 billion highway in Montenegro, slated to form part of a longer corridor stretching from Bari, Italy to Bucharest, Romania[xxxii]; a $1.4 billion highway in Bosnia and Herzegovina[xxxiii]; and a $1.1 billion high-speed railway from Budapest, Hungary to Belgrade, Serbia.[xxxiv] The Budapest-Belgrade line would eventually connect with North Macedonia and the Port of Piraeus, ultimately serving as a transit route for Chinese goods to reach CEE markets.[xxxv] In 2016, the state-owned China Ocean Shipping Company (COSC) bought a 51% majority stake in Piraeus, now the Mediterranean's busiest and Europe's sixth-largest container port.[xxxvi] More recently, COSC and Greece's Prime Minister Kyriakos Mitsotakis announced a plan to invest $660 million more in the port to transform it into the largest commercial harbor in Europe.[xxxvii] Beyond BRI-related financing, in previous 16+1 summits, Beijing had announced plans to invest heavily in Romania's energy sector, to include pledging in 2013 to commit $8 billion to construct two reactors at the Cernavodă nuclear power plant and $2 billion for hydro and thermal power plant projects.[xxxviii]

Several smaller projects announced by China and CEE countries are now complete. In 2014, China finished construction of the Sino-Serbia Friendship Bridge (or Pupin Bridge) across the Danube in Belgrade, marking its first notable infrastructure project in Europe and a symbol of its deepening partnership with Serbia.[xxxix] However, according to a MERICS BRI database, only a fraction of the investment figures announced

at the 16+1 summits has yet been put toward actual infrastructure projects and only a fraction of projects has been completed, indicating that the results of China's investments have so far fallen short of its public rhetoric.[xl] The data show that, since 2013, Beijing has invested $715 million in now-complete infrastructure projects in the 16+1 region, over $3 million is tied to projects currently under construction, and the remainder of the announced figures are connected to planned projects that have not yet commenced.[xli]

A few major plans advertised at early 16+1 summits have now been canceled, and more remain delayed or stalled indefinitely as negative implications of working with China have become more apparent.[xlii] Many CEE states have learned that Chinese "investment" most often refers to loans issued by state-owned banks, which must eventually be paid back with interest.[xliii] The EU, United States, and economic experts have warned that such loans expose already indebted CEE economies to potentially unsustainable debt accumulation and financial instability, and that there may be no realistic prospect of economic return for these receiving states..[xliv] The International Monetary Fund (IMF) reported that continued construction of the highway in Montenegro, for example, will "again endanger debt sustainability," as the country's debt level has risen to 78% of gross domestic product (GDP) in 2019 when it otherwise would have fallen to 59% of GDP had the project not commenced.[xlv] In addition, as these loans are typically conditioned on the use of Chinese labor to complete the projects, the work often does not help recipient countries to mitigate systemic unemployment challenges.[xlvi] EU leaders also worry about Chinese companies' markedly weaker environmental standards and the effects that CEE infrastructure and energy projects will have on the bloc's efforts to address climate change.[xlvii]

In a serious blow to Beijing, Poland, a "strategic partner" of China per a 2011 agreement, cancelled a contract for a leading Chinese construction company to build a highly anticipated road from Warsaw to Germany after the firm gravely mismanaged the project and failed to work within EU regulations.[xlviii] Construction on the Budapest–Belgrade railway has not yet started, and updated designs show the line will be far slower than initially envisioned.[xlix] Approval for a loan to finance the highway in Bosnia and Herzegovina is pending; Beijing–Bucharest talks on the hydropower plant are still ongoing, with the project requiring a new bidding process before work can proceed; and Romania recently announced it would exit the deal with China to build the Cernavodă nuclear reactors.[l] Construction on the thermal power plant also has yet to begin.[li] Although the turbulent Romanian political environment has contributed significantly to these delays and cancelations, EU concerns about Chinese competition, subsidy, and environmental practices have also played a leading role.

Shaping Narratives in Civil Society, Academia, and the Media

China's influence in the CEE region also extends to non-economic arenas, such as civil society, academia, and the media. Beijing uses these avenues to promulgate its official views, enhance its regional soft power, create a more positive perception of its model of governance, and favorably foster expert opinion on China and China-led initiatives in Central and Eastern Europe. In civil society and academia in particular, Beijing seeks to sway analytical agendas and policy recommendations to shape CEE government decision making.[lii]

In 2015, China's Premier Li Keqiang proposed development of a 16+1 think tank network to augment the "High-Level Symposium of Chinese and Central and Eastern European Think Tanks" created in

2013.[liii] Beijing directed the Chinese Academy of Social Sciences (CASS), an academic organization affiliated with the State Council, to serve as the consortium's secretariat. The network includes a Sino-Czech Center for Cooperation on the BRI, a Sino-European Foundation in Hungary with the mission to "bring China closer to Europe while introducing China's achievements to the region," and a new China-CEE Institute in Budapest, opened by CASS and constituting China's first think tank in Europe.[liv] CASS-led programs arranged within the network are becoming more frequent, acting as Track 1.5 dialogues convening senior-level government officials, business leaders, and scholars to promote China's activities on the continent.[lv]

More positive media reporting on these activities has emerged in a number of CEE states. In the Czech Republic, another strategic partner per a 2016 agreement, China Energy Company Limited (CEFC) has invested in several news outlets, prompting a significant uptick in favorable coverage on China, the BRI, and 17+1.[lvi] Analysis by ChinfluenCE, a project examining Chinese influence in the region, found that neutral and negative reporting on China vanished from outlets acquired by the company.[lvii] Czech media often portrayed China not only as a key economic partner, but also as a normative model.[lviii] Analysis of Serbian reporting showed similar trends.[lix] Recently, CEFC made a bid to acquire Central European Media Enterprises, a conglomerate operating in Bulgaria, the Czech Republic, Romania, and Slovakia.[lx] Beijing also exposes CEE populations to its views through paid inserts produced by Chinese state media, and often signed by local reporters, in major CEE newspapers.[lxi] European scholars highlight that such practices can mislead readers and create financial dependencies for print publications struggling to compete with online media.[lxii]

In recent months, Beijing initiated a coordinated, region-wide effort to shift the CEE media's narrative in on the ongoing protests in Hong Kong. From August to October, Chinese embassy officials approached local news outlets with offers to write op-eds or give interviews to disseminate the Chinese Communist Party's (CCP) version of events.[lxiii] Later, articles criticizing the protests and signed by China's ambassadors emerged in widely read mainstream and alternative media in Lithuania, Latvia, Estonia, Poland, Slovakia, the Czech Republic, Bosnia and Herzegovina, and Montenegro.[lxiv] One op-ed published in Estonia appeared in *Postimees*, the country's most widely circulated and read daily newspaper, the country's most widely circulated and read daily newspaper.[lxv] Several articles discussed the "real factors" behind the incidents in Hong Kong, explaining that foreign forces led by the United States fomented the unrest to undermine China.[lxvi] This campaign demonstrates both China's growing political reach in CEE nations and its capacity to manipulate regional narratives.

Implications for Transatlantic Relations and Security

What does China's rising influence in Central and Eastern Europe mean for transatlantic security? It is evident that Chinese power in this region presents intricate challenges for the EU and United States to navigate, and that, barring some major shift on the international stage, these challenges are likely to only intensify over time as Beijing continues to pursue its long-term goals on the European continent. These interrelated goals include: challenging Western influence, ideals, and the Western alliance system in Europe, which China views as in decline and having monopolized rule-setting in the international order for too long; building tacit or active support among governments, academia, media, and businesses for Chinese

interests and policy issues important to the CCP; countering U.S. efforts to influence European policy toward China; cultivating positive perceptions of China in European public opinion; and increasing economic opportunities as Beijing wrestles with slowing growth rates and structural weaknesses in its economy.[lxvii] In sum, Beijing seeks to "make the world safer" for China's rise under the leadership of Xi Jinping by confronting, and eventually altering, some of the norms and rules of the current order in Europe.[lxviii] These goals are geared toward elevating China's role in regional and international affairs, ensuring the CCP remains in power and in control of China, and ultimately achieving the "great rejuvenation of the Chinese nation."[lxix]

Beijing's outreach to CEE states, specifically, helps to fulfill these objectives.[lxx] First, it focuses on a region ripe for economic opportunities given Central and Eastern Europe's geographic position and need for external investment. By undertaking BRI projects in the region in particular, China can redirect its excess national industrial output to building infrastructure that will make it easier to export goods throughout Europe and continue to grow its economy.[lxxi] In doing so, it can advertise its activities as "win-win" opportunities both for CEE countries and China.[lxxii] It also targets several state leaders and governments—such as those of President Miloš Zeman of the Czech Republic, Prime Minister Victor Orbán of Hungary, and President Aleksandar Vučić of Serbia—that exhibit illiberal-authoritarian behavior and are more likely than Western European nations to empathize with Beijing's views on issues from human rights to non-independent media to surveillance.[lxxiii] Third, China's outreach exploits already existing, underlying fractures in EU and wider European and Western cohesion—such as uneven development and access to financing, perceived underrepresentation in multilateral and international forums, and Euroscepticism—to its advantage.[lxxiv] The cases in 2016 and 2017 of multiple 17+1 members refusing to speak against Beijing in EU statements and at the UN indicate the possible risks for not only European unity, but also upholding the liberal democratic values that underpin the transatlantic relationship. The potential for strengthening these values and norms across a wider swath of the continent could diminish if the depth and breadth of China's activities in the CEE region expand, and if 17+1 countries increasingly feel more pressure or more empowered to contradict broader Western positions as a result.

Even as a number of CEE countries begin to recognize the risks in accepting Beijing's economic outreach, the difficulty in turning away enticing opportunities for growth means that China will continue to become more integrated in the economic foundations of the United States' poorer and institutionally weaker allies and partners. These countries, which have less capacity or motivation to resist this influence due to grievances with the EU, will likely continue to question the West's commitment to their development and EU rules that appear to constrict their prosperity. As demonstrated by the lack of unity in several EU attempts to release joint statements criticizing China's actions, Chinese influence and pressure will place susceptible CEE governments in a position where they are reluctant to publicly align with EU and U.S. positions on critical issues. Alternatively, this influence provides increasingly undemocratic CEE nations critical of Western liberalism and EU norms and standards a valuable bargaining chip when dealing with Brussels. Prime Minister Orbán, who has openly denounced EU integration and praised Beijing's role in Europe, has stated that if the EU will not provide Central Europeans enough capital to build necessary infrastructure, they will

simply turn to China instead.[lxxv] This behavior deepens divisions within Europe and forces the EU to wrestle with the choice between withholding structural funds from member states that do not abide by EU values or rewarding bad behavior in pursuit of preventing stronger ties between CEE states and China.

Similarly, China's influence in Balkan EU candidate countries could exacerbate challenges such as corruption and adherence to the rule of law that are at issue in ongoing accession negotiations and future Euro-Atlantic integration. Whereas reducing corruption and adherence to EU rules regarding competition, for example, are prerequisites for candidate states' ascension to the EU and access to EU financing options, Chinese funding is not contingent on CEE governments' anti-corruption efforts or other major changes in state behavior. Allegations of corruption linked to BRI projects have so far been raised in North Macedonia, Serbia, and Hungary.[lxxvi]

Further, unfavorable EU decisions regarding enlargement, such as its recent refusal to begin negotiations with Albania and North Macedonia, could improve Beijing's standing among CEE states. These tensions, combined with China's promotion of pro-Beijing and anti-U.S. propaganda in Europe, contribute to a diluted transatlantic front in exposing and addressing harmful Chinese activities.

With respect to NATO, the issues of CEE allies partnering with Huawei Technologies to build 5G networks and participating in the BRI have already prompted debate within the alliance.[lxxvii] Despite NATO agreement that China does not present a direct military threat to the alliance, Chinese control of CEE critical infrastructure—including the Port of Piraeus and a rising number of telecommunications networks—has implications for NATO security in peacetime, as well as for NATO mobilization, mobility, and operations in a crisis or conflict. U.S. and EU concerns include the potential for enhanced cyber and human intelligence collection in NATO-member CEE countries involved in BRI projects, or where China has ownership of key infrastructure; the ability of Beijing to gain access to, and hold at risk through the threat of offensive cyber operations, critical infrastructure networks on which NATO relies, such as industrial control systems; and even the ability of Chinese-constructed rail lines to safely transfer heavy NATO equipment.[lxxviii] These concerns will worsen if or when major BRI transportation projects in the CEE region are completed, but the divisions they create may translate into weaker NATO effectiveness beforehand. As China-CEE ties deepen, NATO may also need to prepare for Chinese proposals regarding arms sales or military diplomacy with CEE allies. In September, Beijing sold armed unmanned aerial vehicles and other supplies to Serbia, in what is believed to be its largest export of military equipment to Europe in decades.[lxxix] The move signals China's willingness to increase its arms footprint in the CEE region, despite concerns that this action could contribute to instability. Finally, growing debt-to-GDP ratios in smaller allied nations resulting from Chinese investment could impact their ability to sustain defense spending levels and achieve future NATO expenditure commitments.

Opportunities for Transatlantic Cooperation to Address Adverse Chinese Influence

Despite the complexity of the "China challenge" and differences in view on specific policy solutions, the United States and EU have new opportunities to engage CEE countries in the near term, both to address economic and political vulnerabilities that have allowed China to gain greater influence in the region and to confront Beijing's influence efforts head on.

The EU has already toughened its stance toward the 17+1 and China in general, labeling it a "systemic rival promoting alternative models of governance."[lxxx] For the first time, NATO recognized that China's "growing influence and international policies" present strategic "challenges" at the December Leaders' Meeting in London, and CEE nations are signaling disenchantment with Beijing for failing to fulfill economic promises, including infrastructure goals, transparency, market reciprocity, and trade deficit reduction.[lxxxi] This shift in attitude was on display during the previous two 17+1 summits and was underscored by the absence of Poland and Romania's prime ministers from the events.[lxxxii] In January, President Zeman—previously one of Xi Jinping's closest and most outspoken supporters—announced that he will not attend this year's 17+1 event.[lxxxiii]

The United States and EU could work with the Three Seas Initiative—a forum of 12 CEE countries focused on stimulating investment for cross-border energy and infrastructure projects—to develop alternatives to Chinese investment and infrastructure in Central and Eastern Europe. The Trump administration has voiced support for the Three Seas Initiative as an opportunity to bolster allied economies and lessen their dependence on Russia.[lxxxiv] However, engagement could expand to cultivating economic assistance in vulnerable CEE nations to offset their need for Chinese financing. The EU should also strongly consider ways to make funds available to support capacity building in EU candidate countries, including enabling them to evaluate and monitor China's investments. Similarly, EU and U.S. leaders might partner to advise CEE governments courting China's assistance on the hidden economic costs of some of Beijing's practices and the risks these could pose to their countries' long-term development and stability.

Further, the EU and U.S. should invest in protecting and growing the number of democratic institutions—including independent media, civil services, election commissions, and checks on government authority—in EU and EU candidate countries whose current leaders find elements of China's authoritarian model attractive, especially Hungary, the Czech Republic, and Serbia. This will require financial as well as human capital resources working on the ground in CEE states. Efforts to restore and strengthen the democratic foundations of CEE nations should simultaneously involve a conversation around banning foreign donations to European political parties or campaigns, using Australia's 2018 decision to do so as a recent example.[lxxxv] The United States could also propose NATO dialogues with allies in the 17+1 to discuss security concerns regarding Chinese investment in critical infrastructure in their countries. Finally, Germany's virtually-hosted EU-China Summit in September 2020 should have illuminated opportunities for U.S. officials to enhance cooperation with Berlin, the EU, and CEE member states to ensure CEE concerns are captured at similar future forums, seek consensus on China-related issues, and reaffirm their commitment to helping the CEE region achieve economic goals. This particular EU-China summit was the first to include heads of government from all EU member states—a positive development intended to address frustration from smaller CEE countries regarding their marginalization in past summits and to demonstrate European unity in confronting China.[lxxxvi] With this and future engagements, the transatlantic alliance has opportunities to make the 17+1 look less attractive to its CEE partners. However, the EU and United States especially must be cautious of exerting undue pressure on CEE

countries and of demanding binary "us or China" decisions. Such pressure could easily backfire, while tightening Chinese pressure on CEE nations, and continued economic shortcomings in the region could ultimately serve to inspire more unified transatlantic stances and bolster security vis-à-vis China.

Five Models of Strategic Relationship in Proxy War

Amos C. Fox

In the past six years, proxy wars have subtly assumed a position of dominance in contemporary war. Yet, as proxy wars have voraciously marched into the future it has become apparent that they are not well understood, which is the byproduct of insufficient strategic theory on the subject. Within this dynamic, five basic relationship models exist – exploitative, transactional, cultural, coerced, and contractual. Proxy wars will remain relevant for years to come. Understanding the contours of strategic relationships amongst partners is important for the policymaker and practitioner because it allows them to better navigate the waters of proxy war. Understanding the type of relationship that exists between a proxy and its partner is the first step.

In recent years, many thinkers have addressed proxy war, but they have done so in isolation from a strategic theoretical framework. Beyond offering a cursory definitions of proxy war, the strategic studies is bereft of a framework to understand proxy war. To be sure, analysts at American think tank *New America*, posit that, "All of these analytical approaches offer a window onto the variegated nature of proxy strategies but there is nothing in the way of a unified theory on what drives proxy wars."[i] While the strategic studies community is absent theoretical models that illuminate proxy war, American military doctrine also fails to appropriately account for proxy war. Instead, it stands fast with its shibboleths, security force assistance and foreign internal defense, while mentioning proxies or proxy war in passing. Further, Department of Defense joint force doctrine incorrectly captures the role of proxies in modern war, stating that when state-actors employ proxies in pursuit of their objectives, they (the state actor) are operating outside of armed conflict, while their proxies are operating within the realm of armed conflict.[ii] This paper clearly demonstrates that actors employing proxies are often deeply immersed in armed conflict, right alongside their proxy, operating within one of five types of proxy relationships.

Although proxy war is coming back into vogue, it is not a new phenomenon. Flipping back through the pages of military and political history, proxies jump off the page at almost every turn. For example, historian Geoffrey Parker calls attention to the pivotal role of Italian condottieri and Swedish companies for hire in the Middle Ages, as well as the Hessians of eighteenth and nineteenth century Germany working on behalf of a principal agent.[iii] Meanwhile, historian John Keegan contends that surrogates have long, rich role in war, noting that, "During the eighteenth century the expansion of such forces – Cossacks, 'hunters,' Highlanders, 'borders,' Hussars – had been one of the most noted contemporary military developments."[iv]

Reality drives the need for a theory of proxy war. The increasing use of proxies in war, most recently sparked by Russia's 2014 invasion of eastern Ukraine through culturally aligned proxies, demands a fresh look at the phenomena. Further, legislative testimony from U.S. military combatant commanders finds that all geographic combatant commands, apart from U.S. Northern Command, argue that proxies play a critical role within their respective area of responsibility. Despite the dominant position proxies play in modern armed conflict, few theories exist to illuminate the contours and relationship dynamics that make the phenomena unique and worthy of discussion.

Theory and theoretical frameworks are useful because they provide a common language for the phenomenon being analyzed. Next, theories provide a framework for developing models in which to analyze the environment. Lastly, theory allow one to unpack and trace the consequences of how one or more actor operates in an environment.[v] In turn, a sound theory facilitates environmental understanding and what drives relationships within that environment. Therefore, given the increasing frequency of proxies in contemporary armed conflict, it follows to offer a theory regarding proxy relationships and proxy employment in proxy war.

This work does not argue that proxy war is a new phenomenon, but instead it is a strategic approach to war that requires a fresh assessment because today's proxy environment is insufficiently defined. This work builds upon existing the existing body of knowledge that currently frames proxy war. To do so, this paper contends that five basic relationship models guide strategic interaction within proxy war. These relationships are representative of the problems of agency and risk-sharing, which are the defining features in proxy war partnerships. Before discussing the relationship models a brief review of definitions and terms of reference is required.

Framing Proxy Relationships

Because academia, the strategic studies community, and the defense community have not agreed on a common lexicon, the following definitions are used as terms of reference herein. A proxy war is one in which two or more actors, working against a common adversary, strive to achieve a common objective. Borrowing from economics and political science fields, relationships in this environment are governed by a principal-agent dynamic that fuses the partners into a nested package. The relationship between the actors is tiered. The principal actor works indirectly through its agent, or proxy, to accomplish its strategic objective or curate its strategic interests. By extension, the principal's objective becomes the proxy's objective.[vi] However, this generates problems associated with risk-sharing and agency, neither of which are new concepts. For example, Prussian military theorist Carl von Clausewitz contends that, "One country may support another's cause, but will never take it as serious as it takes its own."[vii] Meanwhile British military theorist B.H. Liddell Hart posits that, "No agreement between governments has had any stability beyond their recognition that it is in their own interest to adhere to it."[viii]

With Clausewitz and Liddell Hart as back drops, contemporary theory suggests that problem of agency surfaces in situations when the ambitions or aims of the two actors (i.e. the principal and the agent) are no longer aligned or come into conflict with one another.[ix] On the other hand, the problem of risk-sharing arises when the two parties' attitudes toward risk are misaligned, which then results in divergent action as contact with risk continues.[x]

As with most other partnerships, proxy relationships are either tight or loosely coupled. The relationship's coupling results from environmental and internal conditions. Two types of tight-coupled relationships exist within proxy relationships. The first type is a relationship in which both parties possess numerous commonalities. The second type is a relationship in which the partners possess a small number of variables in common, but those variables are vital to both actors. Those variables could be things like shared religious virtues and customs, ethnic ties, or geographic commonalities. Conversely, in loose coupled relationships the bond between the principal and agent is wanting because the actors have few commonalities or because those commonalities not indispensable to both actors.[xi]

Proxy wars are not exclusive to one type of warfighting. Therefore, they must not be equated with insurgencies, guerrilla warfare, counterinsurgencies, or any other specific type of operational or tactical approach. The way combatants face off with one another is subject to each actors' political narratives, objectives, resources. For the principal, the method of warfighting is also subject to the narratives, objectives, resources limitations of its respective agent, and the strength of bond with that proxy. To be sure, the bludgeoning conventional battles of Russia's proxy war against Ukraine has resulted in over 13,000 Ukrainian dead and 30,000 wounded since the spring of 2014.[xii] This is a clear indication that today's proxy wars are far from just state-sponsored insurgencies in banana republics or political backwaters, but instead often manifest in large-scale land wars in modern nation-states.

Previous work on proxy war theory contends that two primary models—transactional and exploitative models—dominate proxy war.[xiii] Further research indicates that these two models insufficiently capture the breadth of proxy relationships. Instead, analyzing the sinew of proxy relationships along the lines of investment cost and commitment towards a common goal yields five relationship models—transactional, exploitative, coercive, cultural, and contractual. These models provide a useful tool for analyzing proxy wars, understanding how partners operate within a proxy relationship, and understanding how risk can be manipulated in proxy relationships to accelerate or decelerate divergence between principals and agents.

The Exploitative Model

The exploitative model is characterized by a proxy that is dependent on its principal for survival—the relationship could almost be viewed as one between a parasite and a host. The principal provides the animus for the parasitic proxy to survive. Yet, the proxy is important to the principal. When existential threat arises, the principal ensures that its proxy remains intact. Russia's relief of its overwhelmed proxies during multiple battels in the Donbas demonstrates this point.[xiv] This reliance creates a strong bond between the proxy and the partner, resulting in the partner possessing near boundless power and influence over the proxy.

This model is often the result of a stronger actor looking for an instrument, or proxy force, to do its fighting for it. As a result, the proxy is as useful to the principal as is its ability to make progress towards the principal's ends. Therefore, an exploitative relationship is temporary—once the principal's ends have been achieved, or the proxy is unable to maintain momentum towards the principal's ends then the principal tends to discontinue the relationship. Furthermore, if the principal actor feels that the proxy is growing too strong or if its influence with the proxy is waning, it (the principal) will often eliminate political, strategic, or other influential proxy leaders in order to maintain order and control within the relationship.

The assassination of Donetsk People's Republic prime minister Alexander Zakharchenko in August 2018, might well fall into this category.[xv] Zakharchenko's death came on the heels of the assassination of military commander's Mikhail Tolstykh and Arseny Pavlov in February 2017 and October 2016, respectively.[xvi] Attribution is far from certain, however. Some sources contend that Ukrainian forces killed Zakharchenko, Tolstykh, and Arseny in a deliberate effort to counter the Russian proxy movement. Meanwhile, other sources offer that Russian special forces eliminated those leaders to keep their proxies weak and subservient to Moscow.[xvii]

Beyond Russian proxies in Ukraine, a similar dynamic exists between the United States and its proxies along Syria's Euphrates River

valley and expansive eastern deserts. The Syrian Democratic Forces (SDF), an American manufactured proxy force, grew out of amalgamating Syrian Kurdish militias, most notable of which is the People's Protection Units, or YPG.[xviii] The SDF, the United States' proxy for fighting ISIS in Syria, established a political wing—the Syrian Democratic Council (SDC)—in the wake of their early success against ISIS.[xix] In doing so, the SDF and SDC intended to implement Kurdish self-rule in Syria's Western Kurdistan region, or Rojava.[xx]

At the same time, proxies like the SDF and the idea of self-rule, present a unique problem for principal actors locked in formal politico-military alliances such as NATO. Kurdish nationalism has proven a non-starter time and again for Turkey, a formal military ally of the United States. On several occasions, most notably 2018's Operation Olive Branch, Turkey militarily intervened in Syria to stamp out growing Kurdish national and military strength.[xxi] On more than one occasions Turkey's intervention in Western Kurdistan resulted in a strategic and operational pause in the campaign to defeat ISIS in Syria as the SDF split from its American counterpart to defend its homeland in northern Syria.[xxii]

What makes this problem unique is that instead of coming to the help of the SDF, the U.S. military stands idly by as its counter-ISIS proxy in Syria fights for survival against its NATO ally, Turkey.[xxiii] As the SDF battled against the Turks, its force was battered into a shell of the 60,000-strong proxy army that battled ISIS for several years.[xxiv]

The U.S.-SDF relationship also demonstrates how quickly a principal will suspend or eliminate the relationship with its proxy when the unifying military strategy is no longer aligned with policy. America's schizophrenic policy attitude towards the SDF, which has lost over 11,000 fighters on behalf of the U.S.-led counter-ISIS campaign in Syria, illustrates the point that a proxy is only useful so long as military strategy and policy are in harmony with each other.[xxv] As the Russian proxies in the Donbas and the SDF in Syria demonstrate, an agent is vitally dependent on its principal.

However, success can change the power relationship between partners. In certain instances, successful proxies can generate enough legitimacy that it outgrows the principal-agent relationship and is no longer dependent on its principal. If, through battlefield success, political wrangling, or the intervention of other actors, the proxy can transition into the second relational variation, the transactional model. Further, if the principal assesses that the proxy is more useful with more strategic autonomy, it might elect to allow the proxy to gain more power and political independence.

The Transactional Model

The transactional model is proxy war's second relational variation. Prussian military theorist Carl von Clausewitz provides an insightful starting point for understanding this model. He contends:

> But even when both states are in earnest about making war upon the third, they do not always say, "we must treat this country as our common enemy and destroy it, or we shall be destroyed ourselves." Far from it: The affair is more often like a business deal.[xxvi]

One finds that an exchange of services and goods which benefits both the principal and the proxy are at the heart of the transactional model.

This model is also paradoxical because most often the tactical proxy is the strategic powerbroker in the relationship. In many cases, the proxy force's government is independent but looking for assistance in defeating an adversary. For example, in 2014 the government Iraq sought international help

from the United States, among others, to combat ISIS.[xxvii] Strategically, the government of Iraq and the Iraqi military were in charge, but at the tactical level American forces fought a proxy war against ISIS through Iraqi regular and irregular land forces.

Strategically, the proxy possesses the power in the relationship because its association with the principal is wholly transactional. Given the 'business deal' character of the relationship, the clock starts ticking on the duration of the relationship when the first shot fired. As a result, the agent's interest in the principal recedes at a comparable rate to the attainment of the two actors' common goal. Following ISIS's defeat at the battle of Mosul in July 2017 and its unwillingness or inability to stand and fight at the subsequent battle of Tal A'far in August 2017, the United States began to lose influence with the government of Iraq and Iraqi land forces.[xxviii] To be sure, the Iraqi campaign to quell Kurdish independence in October 2017 was a key indicator of this loss of influence. The Iraqi campaign against the Kurds was levied against the recommendations of the United States.[xxix] Further, the subsequent calls for the departure of American forces in Iraq in the wake of Prime Minister Haider Abadi's formal declaration of victory over ISIS in December 2017 illustrate this point.[xxx]

Think of this model as one in which the proxy is in the lead, while the principal follows and supports the proxy. Unlike the exploitative model, this model sees the proxy force's government request support from other nation(s) to defeat a given threat. In doing so, the proxy force's government places parameters on the principal and on the duration of the mission. The proxy government issues parameters to align the principal with its own political and military objectives. It is also important to note that the proxy has fixed political and social interest in the principal, therefore it attempts to terminate the partnership upon attainment of its goals.

Lastly, this model is extremely vulnerable to external influence. It is vulnerable because the proxy's commitment to the principal is based self-interest on more than survival, meaning it can divorce itself from the principal whenever it no longer profits from the relationship, or if it sees danger in its partner. In either situation, cynical self-interest regulates the commitment between partners in the transactional model.

The Coercive Model

The remaining three models are new relational variations being introduced into proxy war theory. The first of these is the coercive model. The coercive model resembles the exploitative model but differs in that the proxy isn't necessarily manufactured, and because the proxy is either an unwilling or reluctant partner. Instead, the proxy is a pre-existing agent that is coerced into a principal-agent proxy relationship. Because of the relationship's coercive nature, the proxy possesses low willingness to share the principal's risk. The principal's physical presence is often the only factor that keeps the agent working on behalf of the principal, resulting in loosely coupled partnership. This also results in a low level of autonomy for the proxy because the principal understands the tenuous bond between the two partners. The proxy's reluctance often manifests as insider attacks by the proxy against the principal. As a result, a principal often must employ an internal security force while working alongside its proxy, much in the way American forces use security forces to protect themselves in Afghanistan when working with their Afghan proxies.[xxxi]

The coerced proxy is often the byproduct of a situation in which a principal has come into an area and defeated the existing ruling body and its security forces. Following that defeat, the principal coopts trusted elements from the defeated regime's security forces as well as

other forces the principal deems necessary. The proxy, either indifferent to the occupying power, or concerned about the effect of cooperating with the principal, displays little motivation for working with the occupier and displays limited capability, whether that be in the form of governance or security.

The most noticeable example of this model is the United States' relationship with the government of Afghanistan and the Afghan security forces. In this relationship the U.S. is the principal actor and the Afghans are the coerced proxy in the fight against the Taliban, Al Qaeda, and various other actors over the course of twenty years of armed conflict. Following the Taliban's initial defeat in Afghanistan in late 2001 and early 2002, U.S. forces created the Afghan army and its security apparatus from scratch.[xxxii]

For the duration of the nineteen-year relationship the Afghan security forces demonstrated reluctance to work with U.S. forces and limited ability to effectively combat the Taliban and other security threats. Reports vary, but one notable report states that the Afghan government and security forces only control 54 percent of the country, while 13 percent of the country is controlled by the Taliban, and the remaining territory is contested.[xxxiii] The Taliban, on the other hand, contend that they control 70 percent of the country.[xxxiv] The inability or unwillingness of the government of Afghanistan and its security forces to systematically root out and eliminate the Taliban, especially when factoring in the 18 years of dedicated train, advise, and assist support from the United States and NATO, infers a coerced agent that is not interested in the same objectives as the principal. Further, this also infers a partner that is unwilling to burden the risk associated with meeting the principal's goal. Lastly, the high number of insider attacks on United States and Afghan forces further indicates a reluctant and coerced relationship.[xxxv]

The Cultural Model

The cultural model is the fourth model of relationship within the proxy wars. Historian John Keegan provides an instructive starting point for understanding the cultural model. Speaking of cultural factor in war, Keegan contends that, "War embraces much more than politics: that it is always an expression of cultural, often a determinant of cultural form, in some societies the cultural itself."[xxxvi] The cultural model appears to share some of the same characteristics as the transactional model, but due to the cultural bond between the principal and the agent, the two are tightly coupled, and thus the proxy is willing to go to the razors edge of strategic and tactical risk with the principal.

Not unlike parts of the American southwest, many countries across the world have cultural lines that do not neatly align with the political map. The most common cultural leverage points are religion, ethnicity, language, and historical geographic precedence. Cultural proxies tend to be found in areas of conflict where culture bleeds across political boundaries. In this model the principal manipulates one or more cultural ties in a location in which they have political or strategic interest to gain power and influence over a malleable group of culturally similar individuals. Although also an example of an exploitative proxy, Russian proxies in eastern Ukraine are a good example of a cultural proxy.

Ukraine's Donbas is a region in which Russian culture and the imperial legacy of the czar's extends well into Ukraine's borders. As a result, the Donbas contains a high number of ethnic Russians, Russophones, and Eastern Orthodox Christians. This differs from central and western Ukraine, which is predominately Catholic and ethnically Ukrainian.

Further, Ukraine, either in part or in whole, has often been part of Russia. To be sure, under the czar's Ukraine constituted a

significant part of what the Romanov's stylized as "All Russias." Appealing to historical precedent, Russian president Vladimir Putin used the "All Russias" concept to legitimize his political and military activity in the Donbas.[xxxvii] Indeed, in the early days of the current Russo-Ukrainian war, Putin and foreign minister Sergey Lavrov were often found using the term Novorossiya and its historical pedigree within the 'All Russias' framework to justify Russian aggression in Ukraine.[xxxviii] Further, protecting ethnic Russians and Russophones was also regularly used to justify aggressive Russian behavior in the Ukraine.[xxxix]

Iranian proxies throughout the Shia Crescent are another exemplar of this model. Iran uses cultural ties, generally the Shite branch of Islam, to build strong-bonded proxies throughout the Middle East. Today, Iran's most notable proxies are Lebanon's Hezbollah and Iraq's Kata'ib Hezbollah. However, as analyst Jack Watling notes, Iran also supports Houthi rebels in Yemen, Hamas in throughout the Middle East, Shia militia groups in Syria and Iraq, just to name a few.[xl] These proxy forces are primarily supported, funded, and advised by Iran's elite Quds Force, a pillar of the Islamic Revolutionary Guard Corps (IRGC).[xli]

The tight cultural bond between principal and agent results in a stalwart proxy that will often stand by the principal agent, sharing high degrees of risk.[xlii] Kata'ib Hezbollah's steadfastness in spite of American targeting through the winter of 2019 and early 2020, in which its headquarters was attacked multiple time, it had droves of its operatives and senior leaders killed, and its primary principal support, Iranian Major General Qasem Soleimani, was killed alongside a number of its leaders highlights this point. Kata'ib Hezbollah's continued rocket strikes through 2020 on American bases in Iraq demonstrates its unwavering commitment to its principal and their unified aims against American interests in Iraq.

The Contractual Model

The contractual model is the final relationship within proxy wars. The contractual model is perhaps one of the oldest relational models between principal and agent. As noted earlier, the pages of history are littered with contractual proxies. In fact, contractual proxies played such an important role war that Italian political theorist Niccolò Machiavelli discussed their utility, or lack thereof, in his classic political and military treatise, *The Prince*.[xliii]

In this model, the principal outsources the pursuit of military objectives to a corporation that has the military means to accomplish those objectives. The benefit of employing contractual proxies is that it increases the distance between one's own population from a war and thereby decreasing the principal's potential for political risk. Further, because the principal's domestic audience does not see large formations of uniformed soldiers deploying from their home stations, this model increases the principal's operational secrecy and deniability. For principal agents not concerned with either of the two previous points, a contractual proxy is also a quick, easy way to increase one's tactical options through the leasing of forces, much like the British use of Hessians during the American Revolution.[xliv]

The wars in the Middle East provide an instructive look at the use of contractual proxies. During the dizzying years of Operation Iraqi Freedom, companies like such as *Blackwater*, *Aegis*, and *Triple Canopy* became household names to those following the conflict. Indeed, in many instances, contractual proxies like *Blackwater* fought alongside American land forces and were occasionally responsible for, and participated, in some of the war's biggest battles. For example, operatives from *Blackwater* fought alongside U.S. Army and

Marine units during 2004's battle of Najaf, helping turn the tide of the battle to an American victory.[xlv]

Furthermore, the killing of several *Blackwater* contractors in March 2004 was directly responsible for the First and Second Battles of Fallujah which raged through the remainder of 2004.[xlvi] Meanwhile, *Blackwater's* role in the indiscriminate killing of over 20 Iraqis in Baghdad's Mansour district in 2007 fanned the flames of a growing insurgency which exacerbated the increasing problems facing the American mission in Iraq.[xlvii] *Blackwater* has since rebranded itself many times, but its head, Erik Prince, continues to offer contractual proxy solutions to stated-based problems in armed conflict, as his 2018 push to privatize the war in Afghanistan illustrates.[xlviii]

Russian contractual proxy, the *Wagner Group*, is the most notable example of this relationship model today. The *Wagner Group* came to prominence following a brief battle near Deir ez-Zor, Syria. During the battle it fought against American special operations forces, resulting in the death of over 200 *Wagner* contractors.[xlix] Moreover, the group has been operating in Ukraine, Syria, South America, and Africa. However, its reach is likely broader than that.[l] These contractual proxies roughly follow the model laid out by *Executive Outcomes*, the South African contractual proxy that gain notoriety in the 1990s for its role in wars across southern Africa.[li]

From the standpoint or risk-sharing, the bond between principal and agent is high because the proxy would not accept the contract if it were not comfortable with the contract's inherent risk. However, a principal and contractual proxy's decoupling point is associated with strategic risk reaching ruinous proportions for the proxy, or a situation in which the proxy's presence cuts against the principal's strategic ambition. For example, tactical risk, like the *Wagner Group's* defeat at Deir ez-Zor, are within a contractual proxy's capacity to absorb.[lii] On the other hand, situations like *Blackwater's* misstep in Baghdad's Mansour Square in September 2007, where it killed over 20 Iraqi civilians, result in strategic loss because situations such as that increase the strategic between actors risk to the point that the principal-agent relationship becomes deleterious for both parties.[liii]

To close the discussion on proxy relationships, risk, regardless of the type of relationship is fundamental to the duration of any proxy relationship. Tactical and strategic risk each affect the relationship in different ways, depending on the strength and character of bond between principal and agent. While not scientific because it is nearly impossible to measure intangibles such as commitment, it is useful to identify the relatively strength and weakness of a proxy partnerships based upon their tolerance for tactical and strategic risk. Doing so provides a useful model for further examining and forecasting proxy wars.

Conclusion

Proxy war's frequency and pervasiveness in modern armed conflict reveals its political and strategic relevance. Because of this it is important to frame proxy wars in order to develop useful models to help guide understanding about proxy war. Proxy relationships are governed by a principal-agent dynamic. Two types of problems are inherent in this type of relationship. The first is the problem of agency, or who owns the problem. But more important is the problem of risk-sharing. Risk-sharing, from a broader perspective, is the defining component of principal-proxy relationships because it is the lubricating substance between two cooperating parties. In most cases risk-sharing is what determines the duration of any principal-agent relationship and the tight or looseness of the bond between partners.

Building upon the principal-agent dynamic, analyzing risk as it relates to a proxy war principal-agent interaction is central to understanding proxy relationships. International relations theorist Thomas Schelling's comments on risk are helpful when analyzing risk-sharing in proxy relationships. Schelling contends that, "The questions that do arise involve degrees of risk – what risk is worth taking, and how to evaluate risk involved in a course of action…It adds an entire dimension to military relations: the manipulation of risk."[liv] Integrating Schelling's thoughts on strategic risk into proxy environments and the bond between principal and agent, one finds risk that strategic risk is the priority cleavage point between actors. This, in essences, results in five models of relationship in proxy war—exploitative, transactional, coercive, cultural, or contractual.

For exploited proxies, the relationship's duration is protracted and the bond between parties is durable. However, for transactional partners, the duration of their partnership lasts as long as their mutual interests serve both parties. In turn, the bond between partners in a transactional relationship is relatively weak, given that it is contingent upon accomplishing strategic and operational objectives. For coerced proxies, their commitment is weak and almost exclusively linked to the physical presence and direct interaction of an occupying force. In cultural relationships, the duration of the relationship is prodigious because of the steadfast cultural bond between principal and agent.

Contractual relationships are firm because the profit motive is a great motivator and because the agent knowingly accepts the strategic and tactical risk before entering a principal-agent relationship. While the partners are tightly coupled at the tactical level, that bond loosens towards the strategic level. It loosens because a principal will sever the relationship if the agent does something that brings about existential threat to the principal's strategic aims or objective. Likewise, the agent will find an out if it approaches strategic collapse. It is also important to emphasize that contractual proxyism dominates the global proxy phenomena today. To be sure, companies like *Aegis*, *Blackwater,* and the *Wagner Group* operate globally and often transparent to the public.[lv] As war continues to push further into the Grey Zone through hybrid means, one should expect to find increasing demand for contractual agents.

The discussion of proxies is far from clean. Proxy relationships coexist within a world rife with paradox. For instance, a sensible argument can be made that transactional relationships fall under the umbrella of several other concepts, to include coalition warfare or alliances. The counterbalance to this point is found within the definition outlined earlier in this work. Coalitions and alliances work toward a common goal, but in proxy relationships one actor is often exploiting another for self-serving ends. Most contractual proxies, on the other hand, can easily be classified as mercenaries. Regardless of how one feels about the morals and ethics surrounding the employment of mercenaries, they have always been and continue to be proxies, or intermediaries.

As to the future, proxy wars are here to stay. They will continue to dominate war so long as the specter of nuclear weapons continues to shadow great power and regional power competition. Further, proxy wars will continue to dominate conflict so long as governments want to decrease their political risks associated with war. Proxy wars do so by obscuring involvement and by deferring the butchers bill of war to intermediaries, thereby making war more palatable to a domestic audience, and thus, more pervasive tool for policy makers and strategists.

The Critical Importance of Brown-Water Operations in the Era of Great Power Competition

Hugh Harsono

The United States' National Defense Strategy has seen a marked shift from focusing on countering violent extremist organizations during the Global War on Terror (GWOT) to one emphasizing Great Power Competition against both China and Russia. This shift in military mentality must also come with an acknowledgement of the critically important battlefield domain of so-called brown-water operations, which comprise operations in river or littoral environments. This topic is noticeably absent from the vast majority of the GWOT. As such, the era of Great Power Competition necessitates a revitalization of American brown-water capabilities led by Special Operations Forces (SOF), a notion that must be understood in order for the United States to regain the competitive advantage against China and Russia.

The American focus on brown-water operations is a topic that has seemingly faded into obscurity in the last several decades. The Vietnam War represented the true pinnacle of American brown-water operations, with robust development of riverine forces capable of conducting, advising, and assisting in brown-water operations, though these capabilities have since been significantly reduced. Although initiatives have been started demonstrating a desire to revitalize American riverine capabilities, the fact remains that the Global War on Terror's land-based emphasis on warfare has led to a significant reduction in U.S. brown-water abilities. Brown-water capabilities are vital to ensuring America's place in today's era of Great Power Competition by supporting developing nations in military and civil capabilities, with the current lack of American brown-water abilities being particularly concerning.

The Age of Great Power Competition

The age of Great Power Competition has seen China, Russia, and the United States vying for increasing amounts of influence throughout the globe. This new era of conflict has resulted in the creation of a more holistic model of competition through the combination of multiple different domains into a select few. For example, the military is no longer solely utilized in a force-on-force capacity. Rather, the military is now seen as a tool to augment national security objectives for a variety of different scenarios, in combination with economic, political, and potentially civil tools. Through this understanding, brown-water operations have become increasingly important for the American military to processes, particularly given the military's changing role in the era of Great Power Competition.

Often a source of political, economic, and social importance within their respective communities, rivers provide immense support for the populations that surround them. This makes controlling and safeguarding these waterways critical to developing nations. China and Russia have also recognized this fact, emplacing themselves through infrastructure investment projects in areas such as rivers and waterways as a way to strengthen local relationships and compete with one another as well as with the United States. China has initiated the *Belt and Road Initiative*, an ambitious global development strategy that aims to link trade between Asia, Europe, and Africa, with expansion potential to the Americas.[i] On a similar note, Ellyat describes how Russia's reach also extends globally through infrastructure and foreign investment to

include many formerly-Communist regions in Latin America, developing nations in Africa, and even the Middle East.[ii] This influence through infrastructure investment creates a distinct necessity for brown-water operations in the modern era, with rivers playing a significant influence on much of the developing world's populations.

With this in mind, the purpose of revitalizing American military brown-water operations would be to further enable the growth of corresponding partner nation force capabilities. The critical importance of rivers as a source of political, economic, and social importance in developing nations necessitates the use of those specific nation's forces in brown-water operations. Some actions that a partner nation might conduct in a riverine environment could include drug interdiction, civil patrol, and humanitarian response operations. Therefore, it is critical for the American military to understand the need for brown-water operations in the modern day. It is also important to understand the context of Great Power Competition in order to grasp the critical importance of brown-water operations. The nature of Great Power Competition emphasizes more on partner nation capacity-building, in direct contrast to more traditional symmetrical views of warfare. Keeping this in mind, it is easy to understand the critical nature and importance of brown-water operations in the modern era.

The requirement for riverine capabilities: why SOF?

The requirement for riverine capabilities during the GWOT era was limited greatly by the overwhelming nature of ground-based conflicts during this time. However, the era of Great Power Competition necessitates the requirement of brown-water forces within the American military's force construct. This is particularly vital due to the asymmetric nature of conflicts today, with much emphasis being placed on partner force development in contrast to a more symmetric view of protracted military conflict.

Simply put, Great Power Competition is not warfare in its most literal and traditional sense. Instead, Great Power Competition emphasizes the People's Republic of China (PRC), Russia, and the United States competing for influence in other countries as preferred partner-of-choice. Infrastructure investment is one way that the PRC and Russia have been able to extend significant influence. However, riverine operations remain an outlet that provides America with the potential to hold more influence in developing nations.

Riverine operations are by no means a strictly military-exclusive effort. Instead, brown-water actions require forces from all over the Department of Defense (DoD) construct, with heavy emphasis from the Special Operations Forces (SOF) community. Gray describes how SOF elements represent a "favorable disproportionate return on military investment," making these forces the perfect fit for riverine operations.[iii] Additionally, SOF units tend to work in a joint manner, thereby facilitating interoperability within the DoD construct, with the Department of the Army's ATP 3-18.12 citing that riverine operations can be "joint operations undertaken primarily by Army and USN forces," with these joint command organizations having the ability to "centrally direct the detailed action of a large number of commands or individuals and common doctrine among the involved forces."[iv] This joint force construct enables the sharing of best tactics and procedures while enabling a cumulative level of knowledge rarely seen in a singular DoD service component. The SOF community's noted flexibility, combined with their already-developed abilities in applicable brown-water skills ranging from direct-action to civil affairs, makes SOF the best choice to further revitalize American brown-

water capabilities. Therefore, in light of the asymmetric nature of warfare in the context of Great Power Competition, combined with a dynamic ability coupled with an already-desirable set of skills, SOF units represent the United States' best opportunity to revitalize America's brown-water operational abilities.

Initiatives with a riverine focus during the GWOT era

The United States military's focus on riverine units was greatly reduced following the Vietnam War, which only presented itself as a conflict domain due to the Viet Cong's use of the Mekong River. Since that time, the American military has not supported the widespread development of riverine-specific units, much less those with a SOF-affiliation, or ones specifically created to participate in Great Power Competition. This analysis considers several past and current riverine-focused units in the era of the Global War on Terror (GWOT) and explains why these initiatives fall short in regard to utilization within the context of today's era of Great Power Competition.

The United States Marine Corps' Small Craft Company (SCC) emerged in 1991, and Scheffer details how these units were created to provide a "riverine transport capability to Marine Expeditionary Units and Brigades."[v] Of note, one of the key developments by the Small Craft Company was the creation of the Small Unit Riverine Craft (SURC). This purpose-built vessel was designed to insert "thirteen fully-equipped Marines in addition to the crew of five", and even featured a bow ramp for easy troop access.[vi] Deploying in 2004, the Small Craft Company played an integral part in ad-hoc combat operations on Iraqi rivers, "bearing a striking resemblance" to American riverine forces in the Vietnam War.[vii] In spite of its relative success in advancing the riverine force through craft development and several successful deployments, the SCC was ultimately disbanded in 2005.[viii] In any case, the Small Craft Company's primary purpose of transportation would preclude it from being an effective part of any American effort in Great Power Competition. Such a singular focus would prevent the Small Craft Company from being truly utilized in multi-function military and civil efforts to develop partner nation capabilities in the riverine realm, negating the primarily American-internal lessons learned from this formerly dynamic organization.

The United States Navy Expeditionary Combat Command established its Coastal Riverine Force by merging its own Riverine Group1 with the Marine Expeditionary Security Force's Groups 1 and 2 in 2012, as described by Burke.[ix] The Coastal Riverine Force has prioritized use of the MK-VI patrol boat, with Rosamond detailing how the Coastal Riverine Force helped pioneer the development of the MK-VI's Coastal Command Boat variant.[x] While in theory an ideal force to enable brown-water operations, Brunson describes how the Coastal Riverine Force's primary functions revolve around "force protection type missions,"[xi] a fact further confirmed by the Department of the Navy in NTTP 3-10.1, where it is stated that the Coastal Riverine Force is "not capable of providing tactical insertion and extraction of forces in the 'brown water' riverine environment."[xii] This lack of any semblance of offensive ability, combined with the fact that "all riverine craft transferred to inactive status" as of late 2016,[xiii] makes the title of the Coastal Riverine Force a significant misnomer. Therefore, the Coastal Riverine Force's ability to carry out, much less empower partner nations to establish such brown-water operations capabilities, is limited in this respect. Additionally, Harrison details how the lack of a selection process for individuals within the Coastal Riverine Force denigrates the professional potential of the Coastal Riverine Force,[xiv] a notion compounded by incidents such as the 2016

U.S.-Iran naval incident in the Persian Gulf. In short, the Coastal Riverine Force is simply not the best force to enable American brown-water operations in the era of Great Power Competition.

Special Boat Team (SBT) 22 is one of the best examples of the American focus on riverine capability development. Already part of the SOF enterprise, SBT-22 operates the Navy's Special Operations Craft – Riverine (SOC-R), a purpose-built vessel for SOF riverine capabilities, as presented by Dutton and Parker.[xv] Dutton and Parker go on to detail how the SOC-R is capable of holding eight personnel in addition to its crew of four and is transportable via C-130, making the SOC-R ideal for a variety of missions.[xvi] However, even with an already-integrated SOF focus and obvious riverine capabilities, SBT-22 still falls short in regards to ensuring a holistic survival of brown-water operations within the U.S. military. While SBT-22 represents the closest development to an ideal riverine-focused force construct, it does have its specific limitations. Firstly, the consolidation of all DoD brown-water operations into a singular unit is a haphazard construct, with the distinct possibility of reduced DoD interoperability, information sharing, and interagency cooperation as a whole. Secondly, the relatively limited number of SWCC personnel as a whole further limits the abilities of SBT-22, with Sofge detailing how there are only several hundred operators spread throughout three boat teams,[xvii] further hampering a widened knowledge base for brown-water operations. Lastly, while the SOC-R represents an unprecedented leap in brown-water capability, the fact that SBT-22 possesses the only individuals with the technical knowledge to operate the SOC-R also hampers any sort of brown-water operations construct within the military. Therefore, while SBT-22 represents the premiere, and arguably, the best notion of the U.S. military to participate in brown-water operations, its small size and relatively niche specialty are not conducive to ensuring the continuity of brown-water operations in the era of Great Power Competition.

America's brown-water capabilities have seen significant decline since the Vietnam War. While there have been some efforts to revitalize these abilities, with SBT-22 being the best among these efforts, the United States military must recognize the importance of brown-water operations, particularly in this era of Great Power Competition.

Case Study 1: The Philippines

The Philippines is currently torn in the era of Great Power Competition, with China, Russia, and the United States increasingly vying for Filipino favor. This makes the Philippines an excellent example showcasing the importance and necessity of brown-water operations in the era of Great Power Competition, particularly given the Philippines' history with internally-based violent extremist organizations (VEOs).

The Mindanao region in the Southern Philippines has historically been a hotbed of major conflict, primarily due to violent extremist organizations, as described by Murphy.[xviii] As a result, Murphy describes how a significant portion of all Philippine SOF actions occur directly in the Mindanao region.[xix] Cragin et. al. goes on to detail the numerous VEOs in the region, to include "Jemaah Islamiyah (JI); the Misuari Breakaway Group (MBG) of the Moro National Liberation Front (MNLF); the Abu Sayyaf Group (ASG); the Moro Islamic Liberation Front (MILF); and the Rajah Soliaman Revolutionary Movement (RSRM),"[xx] in addition to groups such as the Islamic State's East Asia affiliate (ISIS-EA) and the New People's Army (NPA). These VEO's have utilized the river-dense Mindanao region for a variety of actions, with Cragin et. al. describing several of these

items, ranging from the domestic and international movement of fighters to direct-action operations against Filipinos.[xxi] The overwhelming number of VEOs, combined with the large number of waterways in Mindanao, has created an environment necessitating a riverine force to conduct counter-terror and counter-VEO operations.

The Filipino government recognized the necessity of a riverine force, originally standing up a Philippine "Seaborne Brigade," and later, the 1st and 2nd Special Forces Riverine Battalions, in the Mindanao area in the late 1970s, as described by Ambrum.[xxii] However, both these Battalions were deactivated in 2004 due to reorganization within Philippines Special Operations Command (SOCOM), only to be re-activated into three companies in 2006 and 2007. Therefore, one can conclude that brown-water operations remain at the forefront of Philippine SOCOM's priorities.

The necessity of brown-water operations has been particularly recognized by both Chinese and American forces. The Chinese coast guard has most recently sent one of its vessels to the Philippines in January 2020 as described by Robles,[xxiii] ostensibly to discuss further bi-lateral training engagements focused on maritime security. The Chinese have also provided military material aid to the Philippines for counter-terror operations, with Viray describing "four planeloads of rifles" being delivered for such a purpose.[xxiv] Similarly, the U.S. already provides episodic training to Filipino forces on brown-water operations, to include conducting bilateral training such as Balikatan and Joint Combined Exchange Training (JCET) events, as detailed by Sanchez,[xxv] albeit on an extremely limited basis. The U.S. also provides riverine-specific aid to the Philippines, something that can be seen through LaGrone's description of the American provisioning of six SURCs,[xxvi] 25 combat rubber raiding craft with 30 outboard motors,[xxvii] and even a maritime radar system to Filipino partner forces.[xxviii]

While military involvement from both China and the U.S. can be seen in the Philippines, the common theme of a lack of dedicated brown-water focus is quite apparent by both China and America. Livieratos describes how bilateral training events have overwhelmingly focused on direct-action capabilities,[xxix] rather than a more immeasurable, but sustainable, approach to partner-nation capabilities. This presents specific opportunities for an American brown-water specific unit, particularly one capable of conducting regularly scheduled training to support the relatively young riverine companies within the Filipino SOCOM infrastructure.

Case Study 2: Columbia

South America provides another excellent example to highlight the importance of brown-water operations in the era of Great Power Competition. This is especially apparent with the Amazon River, among many other waterways that flow through a variety of countries in South America having a significant presence in Columbia.

Columbia has been a region plagued by both guerilla and narco-terrorism in the last several decades, initially emerging from *La Violencia* in the 1950s. These vicious movements, combined with the fact that there are more navigable waterways than paved roads in the region, have resulted in rivers facilitating everything from fighter movement to the growth and transportation of "legal goods and illicit products," says Willey.[xxx] Willey goes on to describe the importance of riverine operations for Columbian-based forces, saying how "maintaining an active presence in key strategic areas or choke points along the rivers" is vital to Columbia's national sovereignty, counter-insurgency, and counter-narcotics efforts.[xxxi]

Columbia's riverine force has successfully developed into a robust one owing to the many waterways that dominate this nation. Columbia's 1st, 2nd, 3rd, 4th Marine Brigades, River Infantry Brigades, River Battalions, River Assault Marine Battalions, and riverine Combat Elements,[xxxii] comprising a formidable force, as also described by Munson.[xxxiii] Additionally, Columbia's Marine Brigades possess more than 10 of their Columbian-made *Nodriza* Riverine Support Patrol Craft, with additional Riverine Support Patrol Craft-Light and Fast Patrol Boats to support any specific brown-water movements. In fact, Columbia's brown-water capabilities are so well-known that Columbia has even manufactured Fast Patrol Boats for countries such as Brazil, South Korea, and Honduras, reports Norman.[xxxiv] Columbia's riverine force's effectiveness has no doubt been a primary factor in the 50% decline in opium poppy cultivation and cocaine production, with the United States' Government Accountability Office directly crediting coastal and river interdiction efforts to account for over half of total cocaine seizures in Columbia.[xxxv] Columbia's riverine force has also been credited with playing a part in an estimated 50% reduction of guerilla violence, with these forces playing a pivotal role in counter-terrorism.

However, none of these capabilities and results would be remotely possible without assistance from the American government. With a relationship spanning decades, America has provided more than $7 billion dollars' worth of military equipment and support to Columbian partner forces,[xxxvi] with some estimates marking Columbia as the third-largest recipient of U.S. foreign aid.[xxxvii] The U.S. has provided Columbia with significant support for infrastructure development,[xxxviii] providing boats, weapons, and other pieces of invaluable equipment to enable riverine forces. The key to such robust riverine capability development can be seen primarily through regularly scheduled U.S.-led programming to Columbian partner forces. With assistance from Naval Special Warfare (NSW) and USMC forces, the United States actually conducted frequent Mobile Training Teams (MTTs) with Columbian forces in the 1990s.[xxxix] While these MTTs have since faded away, American engagement in Columbia persists through episodic engagements, to include JCETs where SBT-22 directly trained forces to include the 1st Marine Brigade and Marine Riverine Battalion 70.[xl]

The case study of Columbia presents a specific example where U.S. involvement in brown-water operations enabled the flourishing of an associated partner nation's riverine capabilities. While originally an ad-hoc program put together by NSW and USMC forces, while also benefiting from significant amounts of foreign aid, the American military was able to successfully grow Columbia's brown-water capabilities, as noted by Munson.[xli] This specific example showcases the benefits of understanding the critical importance of brown-water operations, particularly in developing nations.

Emergent Opportunities in the era of Great Power Competition

The examples of both the Philippines and Columbia present a clear case for the importance of American brown-water capabilities. These capabilities are ones that do not exist in a sufficient state in the DoD's current force structure, to include the now-defunct USMC Small Craft Company, the Navy's Coastal Riverine Force, and even Special Boat Team 22. With this in mind, it is evident that an expansion and reemergence of brown-water operations remains a persistently important capability even in the modern era of Great Power Competition. This notion is especially apparent given the critical importance of rivers and waterways

in developing nations, with two specific examples being the Mekong River and the Nile River.

The Mekong River's nearly-3,000-mile length spans China, Vietnam, Thailand, Laos, Cambodia, and Myanmar, all countries that encompass a significant part of China's Belt and Road Initiative (BRI). As a result, the Mekong River presents a particularly interesting operational environment, particularly given the development of the Golden Triangle Special Economic Zone (SEZ), as described by Strangio.[xlii] Sitting on the borders of Thailand, Laos, and Myanmar, the Golden Triangle SEZ clearly demonstrates significant Chinese influence through foreign direct investment. However, specific issues within this SEZ have clearly presented themselves since the establishment of this SEZ in the mid-2000s.[xliii] Sullivan describes how the area is rife with drug trafficking and crime,[xliv] while Strangio details hostile and monopolistic business practices of Chinese-backed organizations such as the King Romans' Casino.[xlv] Incidents such as the 2011 Mekong River massacre have even resulted in Chinese boats patrolling the Mekong at certain points,[xlvi] with no end in sight to what many call a violation of foreign sovereignty. The high rate of illegal acts in the area, in conjunction of both soft and hard power projection by China, showcases the importance of brown-water operations on the Mekong River.

Riverine forces belonging to Thailand, Laos, and Myanmar all deserve a right to govern their specific territories along the Mekong, a feat that could be made possible through a robust effort by American forces with brown-water capabilities. The notion of an American brown-water operational ability would enable these nations to have the opportunity of developing a riverine capability rivaling that of even Columbia. However, it is important to remember that the riverine capability does not solely entail direct-action offensive functions. Instead, a riverine capability must be robust enough to conduct civil-military engagements, to include humanitarian efforts, as emphasized by the Joint Chiefs of Staff in JP 3-32.[xlvii] Therefore, it is important for an American effort to revitalize brown-water operations to also encompass civil operations into their planning framework.

The Nile River is another prime example showcasing the necessity of brown-water operations within the context of Great Power Competition. The Nile River's impressive 4,132-mile length runs from the Mediterranean to Africa, flowing through nations including Egypt, Sudan, Ethiopia, and Kenya. The Nile has also seen significant amounts of both Russian and Chinese-backed investment, with both of these strategic competitors seeing the influence the Nile possesses on populations through which it flows, as described by the Congressional Research Service and Max Security.[xlviiixlix] These influences primarily revolve around infrastructure investment and foreign direct investment, to include things such as hydropower-specific dam projects,[l] water purification initiatives,[li] and even gas extraction facilities.[lii] Additionally, the Nile River also plays an important role in facilitating movement of violent extremist organizations, with the terrorist landscape in the region including deadly groups such as the Islamic State's Sinai Province affiliate (ISIS-SP). This factor is also compounded by the fact that the Nile River provides the countries it flows through with hydroelectricity, agriculture, and for some, over 90% of all domestic water needs.[liii] The importance of brown-water operations on the Nile River can be seen due to burgeoning foreign investment efforts, VEO's, and the very fact that the Nile is a source of life for many countries that it flows through.

Riverine forces native to countries such as Egypt, Sudan, and Ethiopia necessitate the

ability to govern their specific sections of the Nile River. While larger and more prosperous nations such as Egypt have naval capabilities, smaller countries such as Sudan and Ethiopia have little to no naval-specific forces at all. Therefore, this type of requirement presents significant opportunities for brown-water American units. Growing these specific nation's riverine abilities, among others, would greatly help these specific countries ensure their foreign sovereignty against unwanted intrusions by foreign powers in the era of Great Power Competition. Additionally, the possession of such forces could help participate in countering violent extremists through interdiction efforts. Lastly, riverine forces could help protect the Nile River in the long-term, contributing to civil engagements that might have sustainability, environmental, or even agricultural impacts.

Therefore, the examples of both the Mekong and Nile Rivers present a significant case for the revitalization of American brown-water operational capabilities. Whether these capabilities be developed through the establishment of a joint command, or if such an effort expanded training and funding lines for partner nations, the Mekong and Nile Rivers showcase immense potential for America to win influence in the era of Great Power Competition.

Conclusion

American brown-water capability has been an afterthought during the Global War on Terror. This capability has been significantly diminished, most notably through the shuttering of the USMC Small Craft Company and the craft divestment of the Coastal Riverine Force. Therefore, there is no doubt that SBT-22 leads the American military in terms of brown-water capabilities. With this being said, it is obvious that specific limitations do exist within the current American riverine force construct model, mostly owing to size and unit constraints. In the modern day, it is simply a necessity to expand and ensure the sustainability of brown-water capabilities within the American DoD construct as a whole, with the goal of increasing American influence through the enabling of partner nation riverine capabilities. As such, it would greatly benefit the United States to establish some SOF-specific effort to prioritize riverine capabilities, ensuring the combination of best practices from the all SOF forces throughout the DoD enterprise, with specific emphasis from the Army's Special Forces, Army's Civil Affairs, Special Boat Team 22, and Marine Raiders. In this era of Great Power Competition, the possession of robust brown-water capabilities must be realized in order to capture the full potential of such efforts for the United States military and America as a whole.

Endnotes: You Can't have Women in Peace without Women in Conflict and Security

[i] Excerpt from *Women on the Front Lines of Peace and Security.* National Defense University 2016 available at: http://ndupress.ndu.edu/Portals/68/Documents/Books/women-on-the-frontlines.pdf

[i] Valerie M. Hudson, Bonnie Ballif-Spanvill, Mary Caprioli, and Chad Emmet. *Sex and world peace*. (Columbia University Press, 2013); Mary Caprioli, "Gender equality and state aggression: The impact of domestic gender equality on state first use of force." *International Interactions* 29.3 (2003): 195-214.; Erik Melander, "Gender Equality and Intrastate Armed Conflict." *International Studies Quarterly* 49(4): (2005): 695-714.
; Rebecca H. Best, Sarah Shair-Rosenfield, and Reed M. Wood. "Legislative Gender Diversity and the Resolution of Civil Conflict." *Political Research Quarterly* 72(1), (2019): 315-228

[ii] UN Resolution 1325 is the most comprehensive, and the watershed resolution, however others, such as 1820, 1888, 1889, 1960, 2106 and 2122 also apply to women's inclusion in public life and government. Complete texts of these resolutions can be found at: http://www.un.org/en/peacekeeping/issues/women/wps.shtml

[iii] https://www.state.gov/secretary/20092013clinton/rm/2010/10/150128.htm

[iv] Efraim Benmelech, and Carola Frydman. "Military CEOs." *Journal of Financial Economics* 117.1 (2015): 43-59.; Jennifer L. Lawless, "Women, war, and winning elections: Gender stereotyping in the post-September 11th era." *Political Research Quarterly* 57.3 (2004): 479-490.

[v] Marie O'Reilly, Andrea Ó Súilleabháin, and Thania Paffenholz.. "Reimagining Peacemaking: Women's Roles in Peace Processes." (International Peace Institute, 2015). https://www.ipinst.org/wp-content/uploads/2015/06/IPI-E-pub-Reimagining-Peacemaking-rev.pdfwe ; Sanam Anderlini, 2007. *Women Building Peace: What They Do and Why it Matters*. Boulder, CO: (Lynne Reinner Publishers, 2007); Theodora Ismene-Gizelis, "Gender empowerment and United Nations peacebuilding." *Journal of Peace Research* 46, (2009): 505-523.; Theodora Ismene-Gizelis, "Gender empowerment and United Nations peacebuilding." *Journal of Peace Research* 46, (2009): 505-523.; Sarah Shair-Rosenfield, and Reed Wood.. "Governing Well After War: How improving female representation prolongs post-conflict peace." *Journal of Politics* 79(3), (2017): 995-1009.; Rebecca H. Best, Sarah Shair-Rosenfield, and Reed M. Wood. "Legislative Gender Diversity and the Resolution of Civil Conflict." *Political Research Quarterly* 72(1), (2019): 315-228

[vi] Marie O'Reilly, Andrea Ó Súilleabháin, and Thania Paffenholz.. "Reimagining Peacemaking: Women's Roles in Peace Processes." (International Peace Institute, 2015). https://www.ipinst.org/wp-content/uploads/2015/06/IPI-E-pub-Reimagining-Peacemaking-rev.pdfwe ; Elizabeth Brannon and Rebecca H. Best. "Which Women Get a Seat at the Table: Evaluating Women's Inclusion in the Colombian Peace Process." Working Paper, 2020

[vii] Pablo Castillo Diaz, and Simon Tordjman. 2012. "Women's Participation in Peace Negotations: Connections between Presence and Influence." UN Women. Available from http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2012/10/wpssourcebook-03a-womenpeacenegotiations-en.pdf

[viii] Elizabeth Brannon and Rebecca H. Best. "Which Women Get a Seat at the Table: Evaluating Women's Inclusion in the Colombian Peace Process." Working Paper. (2020)

[ix] Patrica Hipsher. "Right and Left-Wing Women in Post-Revolutionary El Salvador: Feminist Autonomy and Cross-Political Alliance Building for Gender Equality" in *Radical Women in Latin America: Left and Right.* Victoria Gonzalez and Karen Kampwirth, (Pennsylvania State University Press, 2001), 133-164

[x] Irene Tinker. "Quotas for women in elected legislatures: do they really empower women?." *Women's Studies International Forum*. Vol. 27. No. 5-6. (Pergamon, 2004).

[xi] Valerie Hudson, M., Ballif-Spanvill, Bonnie, Caprioli, Mary, and Emmet, Chad *Sex and world peace*. (Columbia University Press, 2013).

[xii] Erik Melander, "Gender Equality and Intrastate Armed Conflict." *International Studies Quarterly* 49(4): (2005): 695-714.

[xiii] Jacqueline H.R. DeMerrit, Angela D. Nichols, and Eliza G. Kelly. "Female Participation in Civil War Relapse." *Civil Wars* 16(3); (2014): 346-368.

[xiv] Rebecca H. Best, Sarah Shair-Rosenfield, and Reed M. Wood.. "Legislative Gender Diversity and the Resolution of Civil Conflict." *Political Research Quarterly* 72(1) (2014): 315-228.

[xv] Theodora Ismene-Gizelis, "Gender empowerment and United Nations peacebuilding." *Journal of Peace Research* 46, (2009): 505-523.

[xvi] Jaroslav Tir and Maureen Bailey, "Painting too "Rosie" a picture: The impact of external threat on women's economic welfare." *Conflict Management and Peace Science* 35, (2018): 248-262

[xvii] Mona Behan, and Jeannine Davis-Kimball. "Warrior Women: An Archeologist's Search for History's Hidden Heroines." *Wisconsin: Rutgers University* (2002).
[xviii] Sharon Macdonald, Pat Holden, and Shirley Ardener. *Images of women in peace and war: cross-cultural and historical perspectives*. (Univ of Wisconsin Press, 1988).
[xix] NATO HQ. 2019. "Summary of the National Reports of NATO Members and Partner Nations, 2016-2018." Office of the Gender Advisor, International Military Staff.
[xx] Note that this is not the percentage of women in each NATO member force, but the average percentage of women across all member states' forces.
[xxi] Iceland does not have a military.
[xxii] NATO HQ. 2019. "Summary of the National Reports of NATO Members and Partner Nations, 2016-2018." Office of the Gender Advisor, International Military Staff.
[xxiii] The United States removed combat restrictions in 2016
[xxiv] Togo D. West, Jr., Secretary of the Army, "Increasing Opportunities for Women in the Army," memorandum to the Under Secretary of Defense, Personnel and Readiness, July 27, 1994. Qtd in Harrell et al. 2007.
[xxv] Margaret C. Harrell, Laura Werber Castaneda, Peter Schirmer, Bryan W. Hallmark, Jennifer Kavanagh, Daniel Gershwin, and Paul Steinberg., "Assessing the Assignment Policy for Army Women." RAND: National Defense Research Institute. Available from http://www.rand.org/content/dam/rand/pubs/monographs/2007/RAND_MG590-1.pdf (2007)
[xxvi] Jacqueline O'Neill and Jarad Vary. 2011. "Allies and Assets: Strengthening DDR and SSR Through Women's Inclusion." In *Monopoly of Force: The Nexus of DDR and SSR.* (2011): 84
[xxvii] Margaret Power. In *Women and War: A Historical Encyclopedia from Antiquity to the Present, Vol 1*, (ed. Bernard Cook, 2006). ABC-CLIO
[xxviii] Jocelyn Viterna. *Women in War: The Micro-Processes of Mobilization in El Salvador*. (Oxford University Press, 2013),144.
[xxix] In the countries that have all-volunteer militaries, an average of 2% of the male population is actively participating in the military (NATO 2019). While it is more difficult to get hard numbers on nonstate groups, research suggests that far fewer men actively fight in rebel group than are involved in supporting functions (Gurr 2015).
[xxx] Charli Carpenter, ""Women, Children and Other Vulnerable Groups": Gender, Strategic Frames and the Protection of Civilians as a Transnational Issue." *International Studies Quarterly* 49(2), (2005): 295-334.
[xxxi] Stephanie K. Erwin, *The Veil of Kevlar: an Analysis of the Female Engagement Teams in Afghanistan.* (Monterey, CA: Naval Postgraduate School, 2012); Tyra Harding, *Women in Combat Roles: Case Study of Female Engagement Teams.* (United States Army War College, 2012).
[xxxii] Laleh Khalili, "Gendered practices of counterinsurgency." *Review of International Studies* 37.04 (2011): 1471-1491
[xxxiii] Joshua S. Goldstein, *War and gender*. (Springer US, 2003) ; Charli Carpenter, ""Women, Children and Other Vulnerable Groups": Gender, Strategic Frames and the Protection of Civilians as a Transnational Issue." *International Studies Quarterly* 49(2), (2005): 295-334.
[xxxiv] Susan Brownmiller, *Against our will: Men, women and rape*. (Open Road Media, 2013); Sharon Macdonald, Pat Holden, and Shirley Ardener. *Images of women in peace and war: cross-cultural and historical perspectives*. (Univ of Wisconsin Press, 1988).
[xxxv] Nicola Pratt, and Sophie Richter-Devroe.. "Critically examining UNSCR 1325 on women, peace and security." *International Feminist Journal of Politics* 13(4), (2011): 489-503; Swanee Hunt, and Cristina Posa. "Women waging peace." *Foreign Policy* (2001): 38-47.
[xxxvi] Keith Stanski, "Terrorism, Gender, and Ideology: A Case Study of Women Who Join the Revolutionary Armed Forces of Colombia (FARC)." *The Making of a Terrorist: Recruitment, Training, and Root Causes* (2006): 136.; Natalia Herrera, and Douglas Porch. "'Like going to a fiesta'–the role of female fighters in Colombia's FARC-EP." *Small Wars & Insurgencies* 19.4 (2008): 609-634.
[xxxvii] However, institutions can also affect the evolution of social norms. As we discuss in greater detail below, change in the institutions of reintegration of female combatants may lead to an eventual shift in the content of gender norms and a weakening of traditional gender norms.
[xxxviii] Paul R Higate, "Traditional gendered identities: National service and the all volunteer force." *Comparative Social Research* 20 (2002): 229-236.

[xxxix] Jean Bethke Elshtain. "Public man, private women." *Women in Social and Political Thought. (*Princeton, NJ: Princeton Univ. Pr, 1981).
[xl] Annica Kronsell, "Gendered practices in institutions of hegemonic masculinity: Reflections from feminist standpoint theory." *International Feminist Journal of Politics* 7.2 (2005): 280-298.
[xli] http://www.unddr.org/what-is-ddr/introduction_1.aspx
[xlii] Democratic Progress Institute. "DDR and Former Female Combatants." Available from http://www.democraticprogress.org/wp-content/uploads/2016/03/DDR-and-female-combatants-paper.pdf (2015): 18.
[xliii] Jacqueline O'Neill., "Engaging Women in Disarmament, Demobilization, and Reintegration: Insights from Colombia" The Institute of Inclusive Security, 2015. Available from https://www.inclusivesecurity.org/publication/engaging-women-in-disarmament-demobilizaton-and-reintegration-ddr-insights-for-colombia/; Jacqueline O'Neill and Jarad Vary. 2011. "Allies and Assets: Strengthening DDR and SSR Through Women's Inclusion." In *Monopoly of Force: The Nexus of DDR and SSR.* (2011): 84.
[xliv] MacKenzie (2015) notes that DDR coordinators admitted to having done no market assessments and adds that some of the reintegration programs offered training in only one skill, meaning both that other skills might be undersupplied and that women who completed the training would face intense competition for work.
[xlv] Megan MacKenzie, "Securitization and desecuritization: Female soldiers and the reconstruction of women in post-conflict Sierra Leone." *Security Studies* 18.2 (2009): 241-261.
[xlvi] Helen S. A. Basini, "Gender Mainstreaming Unraveled: The Case of DDRR in Liberia." *International Interactions* 39(4), (2013): 535-557.
[xlvii] Helen S. A. Basini, "Gender Mainstreaming Unraveled: The Case of DDRR in Liberia." *International Interactions* 39(4), (2013): 535-557. ; April O'Neill, and Leona Ward.. *Mainstreaming or Maneuvering? Gender and Peacekeeping in West Africa*. (Accra: Kofi Annan International Peacekeeping Training Center, 2005). Available from http://www.eldis.org/go/home&id=72092&type=Document#.WG1V58eg8o8.
[xlviii] For example, MacKenzie writes of the DDR process in Sierra Leone, "The World Bank and the UN—two organizations claiming to be "gender mainstreaming," inclusive, and concerned with "the local"—dictated that women soldiers should be trained as *gara* tie-dyers, seamstresses, caterers, soap makers, and weavers" (2015, 82).
[xlix] Sanam Anderlini, 2007. *Women Building Peace: What They Do and Why it Matters*. Boulder, CO: (Lynne Reinner Publishers, 2007); Theodora Ismene-Gizelis, "Gender empowerment and United Nations peacebuilding." *Journal of Peace Research* 46, (2009): 505-523.
[l] Jacqueline O'Neill., "Engaging Women in Disarmament, Demobilization, and Reintegration: Insights from Colombia" The Institute of Inclusive Security, 2015. Available from https://www.inclusivesecurity.org/publication/engaging-women-in-disarmament-demobilizaton-and-reintegration-ddr-insights-for-colombia/; Jacqueline O'Neill and Jarad Vary. 2011. "Allies and Assets: Strengthening DDR and SSR Through Women's Inclusion." In *Monopoly of Force: The Nexus of DDR and SSR.* (2011): 84
[li] Specht's report notes that as of April 2005, UNICEF statistics indicated that 11,780 Children Associated with Fighting Forces (CAFF) had formally demobilized, 23% of whom were girls (2006, 82).
[lii] Megan MacKenzie, "Securitization and desecuritization: Female soldiers and the reconstruction of women in post-conflict Sierra Leone." *Security Studies* 18.2 (2009): 241-261.
[liii] Helen S. A. Basini, "Gender Mainstreaming Unraveled: The Case of DDRR in Liberia." *International Interactions* 39(4), (2013): 541)
[liv] Specht's report is primarily concerned with female former combatants under 24.
[lv] Coulter, Chris, Mariam Persson, and Mats Utas. *Young female fighters in African wars: conflict and its consequences*. (Nordiska Afrikainstitutet, 2008).
[lvi] Kathleen M. Jennings, "The Political Economy of DDR in Liberia: A Gendered Critique." *Conflict, Security, and Development* 9(4), (2009): 475-494.
[lvii] For example, MacKenzie (2009) and Specht (2006) document cases in which commanders took actions (threats, confiscation of weapons which could be used to prove status as a combatant, etc.) to prevent female combatants from participating. O'Neill and Vary (2011) and Specht (2006) document cases of commanders excluding the names of female combatants from lists provided for DDR. Specht adds that some commanders added the names of men not involved in their forces to their lists for a price (2006, 82-83). Basini (2013) finds that 76.4% of former female combatants surveyed in Liberia who did not participate in DDR did not do so because they had been misinformed (often by their commanders) about the benefits, criteria, or process of the DDR.

[lviii] See MacKenzie (2015, 77).
[lix] Interestingly, Specht finds through interviews with female former Liberian combatants that many say they joined to protect themselves and other women from rape and to avenge rape (2006, 11). She adds however that an estimated 75% of children demobilized in 204 were believed to have been sexually abused or exploited (16).
[lx] Helen S. A. Basini, "Gender Mainstreaming Unraveled: The Case of DDRR in Liberia." *International Interactions* 39(4), (2013): 541)
[lxi] For examples of such stereotypes of female combatants, see Colekessian (2009).
[lxii] Rebecca H. Best, Sarah Shair-Rosenfield, and Reed M. Wood. "Legislative Gender Diversity and the Resolution of Civil Conflict." *Political Research Quarterly* 72(1), (2019): 315-228.; Jacqueline O'Neill., "Engaging Women in Disarmament, Demobilization, and Reintegration: Insights from Colombia" The Institute of Inclusive Security, 2015. Available from https://www.inclusivesecurity.org/publication/engaging-women-in-disarmament-demobilizaton-and-reintegration-ddr-insights-for-colombia/
[lxiii] From the Department of Veterans' Affairs mission statement at: https://www.va.gov/about_va/mission.asp
[lxiv] Donna L. Washington, et al. "Women veterans' perceptions and decision-making about Veterans Affairs health care." *Military Medicine* 172.8 (2007): 812-817
[lxv] National Research Council. *Returning home from Iraq and Afghanistan: assessment of readjustment needs of veterans, service members, and their families. (*2013)
[lxvi] Kate Hendricks Thomas, Lori W. Turner, & Emily Kaufman, Angelia Paschal, Adam P. Knowlden, David A. Birch, James D. "Predictors of depression diagnoses and symptoms in veterans: Results from a national survey". *Military Behavioral Health*, *3*(4), (2015): 255-265
[lxvii] Veterans' Administration *Profile of Women Veterans: 2015* National Center for Veterans' Analysis and Statistics. Access at: https://www.va.gov/vetdata/docs/SpecialReports/Women_Veterans_Profile_12_22_2016.pdf
[lxviii] Donna L. Washington, et al. "Women veterans' perceptions and decision-making about Veterans Affairs health care." *Military Medicine* 172.8 (2007): 812-817
[lxix] Rebecca Burgess, "Second Service: Military Veterans and Public Office." *AEI Paper & Studies* (2016)
[lxx] It is worth noting that 19% of veterans under the age of 50 are women.
[lxxi] Jeremy M. Teigen, "Military Experience in Elections and Perceptions of Issue Competence: An Experimental Study with Television Ads." *Armed Forces & Society* 39(3), (2012): 415-433.
[lxxii] Susan V. Iverson, and Rachel Anderson. "The complexity of veteran identity: Understanding the role of gender, race, and sexuality." (2013).
[lxxiii] 21.7% of women and 37.3% of men selected "neither agree nor disagree."
[lxxiv] We developed the survey in Qualtrics and deployed it via social media outlets to a convenience sample of veterans.
[i] We use the term gender appropriate as an alternative to "gender neutral," a term that has been used in the context of DDR agreements with good intentions, but poor results. "Gender neutral" has been used to refer to DDRs, such as the one in Angola, that do not directly reference women or do not place any restrictions on women. However, it has been noted through the failures of gender neutral agreements that neglecting to mention women, or to mention gender at all, leads to unintended consequences including a lack of representation of the interests of women in negotiations, lack of preparation to enable women to participate in DDR programs when they have other traditional care obligations or familial restrictions on their activities, and lack of attention to the particular gendered ways in which war may affect women (including unwanted pregnancies, sexual abuses that extend beyond the resolution of the conflict as women are forcibly married, local restrictions on the activities of women, biases about women who have engaged in violence, the use of threats or force to prevent women from accessing services, etc.). By gender appropriate, we refer to not only actively seek to ensure there is no discrimination against women, but that proactively include women in ways that account for the preexisting cultural and institutional context. This means that not only should fighters not be referred to using gendered pronouns, but reintegration services should also account for the ways in which the needs and environments of former female combatants differ from those of their male counterparts.

Endnotes: Does Democratic Peace Theory Hold in Cyberspace?

[i] Jack S. Levy, "Domestic Politics and War." *The Journal of Interdisciplinary History* 18, no. 4 (Spring 1988): 662.
[ii] To give one example: In 2014, researchers uncovered a malware campaign, which they dubbed DarkHotel, that had originated in South Korea. The threat actor was highly advanced and widely believed to be state-sponsored. Its primary targets included Japan and India's militaries, as well as the US defense industry.
[iii] Richard Clarke, "The Risk of Cyber War and Cyber Terrorism: Interview with Richard A. Clarke." *Journal of International Affairs* 70, no. 1 (Winter 2016): 179–81.
[iv] R.J. Rummel, "Libertarianism and International Violence." *The Journal of Conflict Resolution* 27, no. 1 (March 1983): 27-71.
[v] Michael Doyle, "Liberalism and World Politics." *American Political Science Review* 80, no. 4 (December 1986): 1151–69.
[vi] William J. Dixon, "Democracy and the Peaceful Settlement of International Conflict." *The American Political Science Review* 88, no. 1 (March 1994): 14–32.
[vii] James D. Fearon, "Domestic Political Audiences and the Escalation of International Disputes." *American Political Science Review* 88, no. 3 (September 1994): 577-592.
[viii] Erik Gartzke, "The Capitalist Peace." *American Journal of Political Science* 51, no. 1 (January 2007): 166–191.
[ix] John J. Mearsheimer, "Back to the Future: Instability in Europe After the Cold War." *International Security* 15, no. 1 (Summer 1990): 5–56.
[x] David E. Spiro, "The Insignificance of the Liberal Peace." *International Security* 19, no. 2 (September 1994): 50–86.
[xi] David P. Forsythe, "Democracy, War, and Covert Action." *Journal of Peace Research* 29, no. 4 (November 1992): 385–395.
[xii] John Arquilla and David Ronfeldt, "Cyber War Is Coming!" in *In Athena's Camp: Preparing for Conflict in the Information Age*. (Santa Monica, CA: RAND Corporation, 1997). https://www.rand.org/pubs/reprints/RP223.html.
[xiii] Thomas Rid, "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 5–32.
[xiv] John Stone, "Cyber War WILL Take Place!" *Journal of Strategic Studies* 36, no. 1 (February 2013): 101–108.
[xv] Richard Clarke, "The Risk of Cyber War and Cyber Terrorism."
[xvi] Bruce Bueno de Mesquita et al., "An Institutional Explanation of the Democratic Peace." *The American Political Science Review* 93, no. 4 (December 1999): 791–807.
[xvii] From this point forward, I use "attack" to denote any cyber incident that I have yet to classify as a simple attack or as an act of cyber war. Recall that "attack" is defined here as an unauthorized penetration of a system, where "war" must be an act of destruction; destruction necessitates a penetration, but a penetration does not necessarily entail destruction. All acts of cyber war are cyber attacks, but not all cyber attacks are acts of cyber war.
[xviii] "Significant Cyber Incidents," *Center for Strategic and International Studies*, September 2019. Accessed October 10, 2019. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.
[xix] Ryan C. Maness et al., "Dyadic Cyber Incident and Dispute Data, Version 1.5." https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset.
[xx] "Democracy Index 2018: Me Too? Political Participation, Protest and Democracy." *The Economist Intelligence Unit* (2019): 2. http://www.eiu.com/Handlers/WhitepaperHandler.ashx?fi=Democracy_Index_2018.pdf&mode=wp&campaignid=Democracy2018.
[xxi] Per the Democracy Index, countries are scored for each of the five factors on a 1-10 scale, and the five scores are then averaged. Countries whose final scores fall between 8.0 and 10.0 are rated as "full democracies," with countries scoring from 6.0 to 8.0 rated as "flawed democracies." Rather embarrassingly, the U.S. scored as a "flawed democracy" with a 7.96. Several US allies, which are widely considered to be democracies, scored in the same category. If I were to test only those countries that scored as full democracies, thus excluding the U.S. and many allies, this study would be of limited use to American policymakers, hence the decision to include flawed democracies.
[xxii] A critical reader might point out that the U.S. is conspicuously missing from the perpetrator list. This is not because the U.S. has never acted questionably vis-à-vis other democracies in the cyber domain. It is because, to my knowledge, no one incident perpetrated by the U.S. against another democracy was a true network intrusion or amounted to more than passive intelligence collection, and thus none met my definition of a cyber attack.

[xxiii] Sean Gallagher, "Researchers Expose Dino, Espionage Malware With a French Connection." *Ars Technica*, June 30, 2015. https://arstechnica.com/information-technology/2015/06/researchers-expose-dino-espionage-malware-with-a-french-connection/
[xxiv] "Animals in the APT Farm," *Kaspersky SecureList*, March 5, 2016. https://securelist.com/animals-in-the-apt-farm/69114/.
[xxv] Alex Grigsby, "Shouting at Americans: A Peek Into French Signals Intelligence." *Council on Foreign Relations*, September 15, 2016. https://www.cfr.org/blog/shouting-americans-peek-french-signals-intelligence.
[xxvi] Dan Goodin, "'DarkHotel' Uses Bogus Crypto Certificates to Snare Wi-Fi-Connected Execs." *Ars Technica*, November 10, 2014. https://arstechnica.com/information-technology/2014/11/darkhotel-uses-bogus-crypto-certificates-to-snare-wi-fi-connected-execs/.
[xxvii] "The DarkHotel APT: A Story of Unusual Hospitality," *Kaspersky SecureList*, November 10, 2014. https://securelist.com/the-darkhotel-apt/66779/.
[xxviii] Ibid.
[xxix] Kim Zetter, "Darkhotel: A Sophisticated New Hacking Attack Targets High-Profile Hotel Guests." *Wired*, November 10, 2014. https://www.wired.com/2014/11/darkhotel-malware/.
[xxx] Rajeswari Pillai Rajagopalan, "Growing India-South Korea Strategic Synergy: The Defense Domain." *The Diplomat*, September 13, 2019. https://thediplomat.com/2019/09/growing-india-south-korea-strategic-synergy-the-defense-domain/.
[xxxi] Ryan Gallagher, "How UK Spies Hacked a European Ally and Got Away With It." *The Intercept*, February 17, 2018. https://theintercept.com/2018/02/17/gchq-belgacom-investigation-europe-hack/.
[xxxii] Ibid.
[xxxiii] I have been conservative and counted Belgium as the only victim, though one could argue that it would be fair to include other EU member states. However, with only open-source information, it is impossible to parse who else was affected and to what extent.
[xxxiv] Ibid.
[xxxv] Daniel Boffey. "British Spies 'Hacked Into Belgian Telecoms Firms on Ministers' Orders'." *The Guardian*, September 21, 2018. https://www.theguardian.com/uk-news/2018/sep/21/british-spies-hacked-into-belgacom-on-ministers-orders-claims-report.
[xxxvi] Ryan Gallagher, "How UK Spies Hacked a European Ally and Got Away With It."
[xxxvii] Or, at the very least, the ability to divert a disproportionate amount of resources, as is the case with capable authoritarian actors (who are outside the scope of this study).
[xxxviii] As of this writing, the UK was still an EU member.
[xxxix] "National Cyber Strategy of the United States of America." *The White House* (September 2018): 26. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
[xl] Jared Serbu, "DHS Sweetens Cyber Workforce Recruiting With New Bonuses." *Federal News Network*, May 3, 2016. https://federalnewsnetwork.com/cybersecurity/2016/05/dhs-sweetens-cyber-workforce-recruiting-new-bonuses/.

Endnotes: Just Robots, Just Collection: The Implications of Lethal Autonomous Weapons Systems for Ethical Intelligence Collection

[i] Larry Lundy, Alexa O'Brien, Christine Solis, Aaron Sowers, and Jeffrey Turner, "The Ethics of Applied Intelligence in Modern Conflict," *International Journal of Intelligence and* Counterintelligence 32, no. 3 (2019): 593.
[ii] Paul Scharre, *Army of None* (New York: W. W. Norton & Company, 2018), 52.
[iii] Heather M. Roff, "The Strategic Robot Problem: Lethal Autonomous Weapons in War," *Journal of Military Ethics* 13, no. 3 (2014): 212-213.
[iv] General Counsel of the Department of Defense, *Department of Defense Law of War Manual,* Washington, DC: U.S. Department of Defense, 2016, https://ogc.osd.mil/images/law_war_manual_december_16.pdf, 71.
[v] Ibid., 50.
[vi] Ibid.*,* 353.
[vii] David Omand and Mark Phythian, "Secret Agents and Covert Human Sources," in *Principled Spying: The Ethics of Secret Intelligence* (Washington, DC: Georgetown, 2018), 122.
[viii] Angela Gendron, "Just War, Just Intelligence: An Ethical Framework for Foreign Espionage," *International Journal of Intelligence and CounterIntelligence* 18, no. 3 (2005): 417.
[ix] R.V. Jones, "Intelligence Ethics" in Jan Goldman, ed. *Ethics of Spying: A Reader for the Intelligence Professional* (Lanham, MD: Scarecrow Press, 2006), 37.
[x] Maja Zehfuss, "Targeting: Precision and the production of ethics," *European Journal of International Relations* 17, no. 3 (2010): 549.
[xi] Shane P. Hamilton and Michael P. Kreuzer, "The Big Data Imperative: Air Force Intelligence for the Information Age," *Air & Space Power Journal* 32, no. 1 (2018): 9.
[xii] Ibid., 9.
[xiii] Scharre, *Army of None,* 44.
[xiv] Myron Hura and Gary W. McLeod, *Intelligence Support and Mission Planning Requirements for Autonomous Precision Guided Weapons: Implications for Intelligence Support Plan Development* (Santa Monica, CA: RAND Corporation, 1993), 1.
[xv] Hura and McLeod, Intelligence Support and Mission Planning Requirements for Autonomous Precision Guided Weapons, 19.
[xvi] Scharre, *Army of None,* 44.
[xvii] Hura and McLeod, Intelligence Support and Mission Planning Requirements for Autonomous Precision Guided Weapons, 18.
[xviii] Nina Franz, "Targeted killing and pattern-of-life analysis: weaponized media," *Media, Culture & Society* 39, no. 1 (2017): 112-114.
[xix] Ibid., 114.
[xx] Levi Maxey, "The Reassertion of Human Intelligence in the Digital Era," *Georgetown Security Studies Review*, 5, no. 1 (December 2016): 40.
[xxi] Ibid., 40.
[xxii] Ibid., 41.
[xxiii] Charles J. Dunlap, Jr., "The Hyper-Personalization of War: Cyber, Big Data, and the Changing Face of Conflict," *Georgetown Journal of International Affairs* (2014): 110.
[xxiv] Kim Zetter, "So, the NSA Has an Actual Skynet Program," *WIRED*, May 8, 2015, https://www.wired.com/2015/05/nsa-actual-skynet-program.
[xxv] Maxey, "The Reassertion of Human Intelligence in the Digital Era," 38; Grégoire Chamayou, *A Theory of the Drone,* trans. Janet Lloyd (New York: The New Press, 2015), 50.
[xxvi] Zehfuss, "Targeting: Precision and the production of ethics," 549.
[xxvii] Zetter, "So, the NSA Has an Actual Skynet Program."
[xxviii] Chamayou, *A Theory of the Drone*, 46.
[xxix] *Department of Defense Law of War Manual*, 50.
[xxx] Dan Gonzales and Sarah Harting, Designing Unmanned Systems with Greater Autonomy: Using a Federated, Partially Open Systems Architecture Approach (Santa Monica, CA: RAND Corporation, 2014), https://www.rand.org/pubs/research_reports/RR626.html, xii.

[xxxi] Rachel England, "The Pentagon has a laser that identifies people by their heartbeat," *Engadget,* June 27, 2019, https://www.engadget.com/2019/06/27/the-pentagon-has-a-laser-that-identifies-people-by-their-heartbe. Note: Machine-learning, including computer vision, generally has some ways to go in terms of accuracy such as minimization of biases.
[xxxii] Gendron, "Just War, Just Intelligence," 418.
[xxxiii] Dunlap, "The Hyper-Personalization of War," 113.
[xxxiv] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times*, February 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.
[xxxv] Chamayou, *A Theory of the Drone,* 56.
[xxxvi] For a deeper exploration of limitations in computer vision for identifying civilians or persons *hors de combat*, see Rebecca Crootof, "The Killer Robots Are Here: Legal and Policy Implications," *Cardozo Law Review* 36, no. 5 (2015): 1837-1915.
[xxxvii] Roff, "The Strategic Robot Problem," 212.

Endnotes: China's Influence in Central and Eastern Europe, European Responses, and Implications for Transatlantic Security

[i] Andrea Kendall-Taylor, "Prepared Statement Before the US House Subcommittee on Europe, Eurasia, Energy, and the Environment, 'China's Expanding Influence in Europe and Eurasia,'" May 9, 2019, https://s3.amazonaws.com/files.cnas.org/documents/Kendall-Taylor-Testimony 5.9.2019_final2.pdf?mtime=20190509075240.
[ii] Erik Brattberg, "Testimony before the US-China Economic and Security Review Commission, Hearing on 'China's Relations with US Allies and Partners in Europe and the Asia Pacific,'" April 5, 2018, https://www.uscc.gov/sites/default/files/USCC%20Hearing_Erik%20Brattberg_Written%20Statement_April%205% 202018.pdf.
[iii] Jonathan E. Hillman and Maesea McCalpin, "Will China's '16+1' Format Divide Europe?," Center for Strategic and International Studies, April 11, 2019, https://www.csis.org/analysis/will-chinas-161-format-divide-europe and "Five-Year Outcome List of Cooperation Between China and Central and Eastern European Countries," Ministry of Foreign Affairs of the People's Republic of China, November 28, 2017.
[iv] "16+1 Cooperation and China-EU Relationship," China-CEE Institute, November 2018, https://china-cee.eu/wp-content/uploads/2018/11/161-cooperation.pdf.
[v] Phillip Le Corre, "China's Rise as a Geoeconomic Influencer: Four European Case Studies," *Carnegie Endowment for International Peace*, October 15, 2018, https://carnegieendowment.org/2018/10/15/china-s-rise-as-geoeconomic-influencer-four-european-case-studies-pub-77462.
[vi] "The 16+1 Cooperation," Government of the Republic of Croatia, 2019, https://www.ceec-china-croatia.org/en/about-cooperation/.
[vii] Ivana Karásková, "Engaging China in 17+1: Time for the ACT Strategy," *The Diplomat*, April 7, 2020, https://thediplomat.com/2020/04/engaging-china-in-171-time-for-the-act-strategy/.
[viii] Brattberg, Testimony, April 5, 2018 and Valbona Zeneli, "What Has China Accomplished in Central and Eastern Europe," *The Diplomat*, November 25, 2017, https://thediplomat.com/2017/11/what-has-china-accomplished-in-central-and-eastern-europe/.
[ix] "Countries of the Belt and Road Initiative (BRI)," The Green Belt and Road Initiative Center, updated March 2020, https://green-bri.org/countries-of-the-belt-and-road-initiative-bri?cookie-state-change=1592171611745.
[x] Kendall-Taylor, Prepared Statement, May 9, 2019.
[xi] Andrew Small, "Why Europe Is Getting Tough on China, And What It Means for Washington, *Foreign Affairs*, April 3, 2019, https://www.foreignaffairs.com/articles/china/2019-04-03/why-europe-getting-tough-china.
[xii] Thorsten Benner and Thomas Wright, "Testimony to US China Economic and Security Review Commission, Hearing on 'China's Relations with US Allies and Partners in Europe and the Asia Pacific,'" April 5, 2018, https://www.brookings.edu/wp content/uploads/2018/04/wrightbennerchinatransatlanticrelations.pdf and John Van Oudenaren, "Why China Is Wooing Eastern and Central Europe," *The National Interest*, September 4, 2018, https://nationalinterest.org/feature/why-china-wooing-eastern-and-central-europe-30492.
[xiii] Benner and Wright, Testimony, April 5, 2018 and Kendall-Taylor, Prepared Statement, May 9, 2019.
[xiv] Brattberg, Testimony, April 5, 2018 and Theresa Fallon, "The EU, the South China Sea, and China's Successful Wedge Strategy," Center for Strategic and International Studies, October 13, 2016, https://amti.csis.org/eu-south-china-sea-chinas-successful-wedge-strategy/.
[xv] Brattberg, Testimony, April 5, 2018.
[xvi] Thorsten Benner, Jan Gaspers, Mareike Ohlberg, Lucrezia Poggetti, and Kristin Shi-Kupfer, "Authoritarian Advance: Responding to China's Growing Political Influence in Europe," Global Public Policy Institute and Mercator Institute for China Studies, February 2018, https://www.merics.org/sites/default/files/2018-02/GPPi_MERICS_Authoritarian_Advance_2018_1.pdf.
[xvii] Hillman and McCalpin, "Will China's '16+1' Format Divide Europe?," April 11, 2019.
[xviii] Benner et al., "Authoritarian Advance," February 2018.
[xix] Brattberg, Testimony, April 5, 2018.
[xx] Benner et al., "Authoritarian Advance," February 2018 and Oudenaren, "Why China is Wooing Eastern and Central Europe," September 4, 2018.

[xxi] Thilo Hanemann, Mikko Huotari, Agatha Kratz, Joseph Percy, "Chinese FDI in the EU's Top 4 Economies," *China Briefing*, Dezan Shira & Associates, May 8, 2019, https://www.china-briefing.com/news/chinese-fdi-eu-top-4-economies/.
[xxii] Thilo Hanemann, Mikko Huotari, and Agatha Kratz, "Chinese FDI in Europe: 2018 Trends and Impact of New Screening Policies," Mercator Institute for China Studies, March 2019, https://www.merics.org/en/papers-on-china/chinese-fdi-in-europe-2018.
[xxiii] Zeneli, "What Has China Accomplished in Central and Eastern Europe," November 25, 2017.
[xxiv] "Chinese FDI into North America and Europe in 2018 Falls 73% to Six-Year Low of $30 Billion," Baker McKenzie, January 14, 2019, https://www.bakermckenzie.com/en/newsroom/2019/01/chinese-fdi.
[xxv] Zeneli, "What Has China Accomplished in Central and Eastern Europe," November 25, 2017.
[xxvi] Ibid.
[xxvii] Ibid.
[xxviii] Ibid.
[xxix] Ibid.
[xxx] Hillman and McCalpin, "Will China's '16+1' Format Divide Europe?" April 11, 2019.
[xxxi] Benner et al., "Authoritarian Advance," February 2018.
[xxxii] "16+1 Cooperation and China-EU Relationship," 2018 and "Montenegro, China's Exim Bank agree $1 billion highway deal," *Reuters*, October 30, 2014, https://www.reuters.com/article/montenegro-highway-idUSL5N0SP4BI20141030.
[xxxiii] Thomas S. Eder and Jacob Mardell, "Belt and Road Reality Check: How to Assess China's Investment in Eastern Europe," Mercator Institute for China Studies, July 10, 2018, https://www.merics.org/en/blog/belt-and-road-reality-check-how-assess-chinas-investment-eastern-europe.
[xxxiv] Erik Brattberg and Etienne Soula, "Europe's Emerging Approach to China's Belt and Road Initiative," Carnegie Endowment for International Peace, October 19, 2018, https://carnegieendowment.org/2018/10/19/europe-s-emerging-approach-to-china-s-belt-and-road-initiative-pub-77536.
[xxxv] Flora Rencz, "The BRI in Europe and the Budapest-Belgrade Railway Link," European Institute for Asian Studies, October 2019, http://www.eias.org/wp-content/uploads/2019/07/EIAS-Briefing-Paper-The-BRI-in-Europe-and-the-Budapest-Belgrade-Railway-Link-Final.pdf.
[xxxvi] Ilias Bellos, "Piraeus becomes the biggest port in the Med in terms of container traffic," https://www.ekathimerini.com/246605/article/ekathimerini/business/piraeus-becomes-the-biggest-port-in-the-med-in-terms-of-container-traffic and "China, Greece agree to push ahead with COSCO's Piraeus Port investment," *Reuters*, November 11, 2019, https://www.reuters.com/article/us-greece-china/china-greece-agree-to-push-ahead-with-coscos-piraeus-port-investment idUSKBN1XL1KC#:~:text=ATHENS%20(Reuters)%20%2D%20China%20and,trade%20between%20Asia%20and%20Europe.
[xxxvii] "China, Greece agree to push ahead with COSCO's Piraeus Port investment," *Reuters*, November 11, 2019.
[xxxviii] Andreea Brinza, "How China Blew Its Chance in Eastern Europe," *Foreign Policy*, April 11, 2019.
[xxxix] Vuk Vuksanovic, "Light Touch, Tight Grip: China's Influence and The Corrosion Of Serbian Democracy," *War on the Rocks*, September 24, 2019, https://warontherocks.com/2019/09/light-touch-tight-grip-chinas-influence-and-the-corrosion-of-serbian-democracy/.
[xl] Eder and Mardell, "Belt and Road Reality Check," July 10, 2018.
[xli] Ibid.
[xlii] Brinza, "How China Blew Its Chance in Eastern Europe," April 11, 2019.
[xliii] Eder and Mardell, "Belt and Road Reality Check," July 10, 2018.
[xliv] Brattberg, Testimony, April 5, 2018 and Alan Riley, "Beware of Chinese Gifts: A Warning for Central and Eastern Europe," International Centre for Defence and Security (Estonia), September 20, 2018, https://icds.ee/beware-of-chinese-gifts-a-warning-for-central-and-eastern-europe/.
[xlv] Eder and Mardell, "Belt and Road Reality Check," July 10, 2018.
[xlvi] Ethan Kapstein and Jacob Shapiro, "Catching China by the Belt (and Road)," *Foreign Policy*, April 20, 2019, https://foreignpolicy.com/2019/04/20/catching-china-by-the-belt-and-road-international-development-finance-corp-beijing-united-states/ and Nyshka Chandran, "China can make its Belt and Road project more successful if it taps locals, experts say," *CNBC*, September 14, 2018, https://www.cnbc.com/2018/09/14/china-must-do-more-to-tap-locals-in-belt-and-road-initiative-panel.html.

[xlvii] Brattberg and Soula, "Europe's Emerging Approach to China's Belt and Road Initiative," October 19, 2018 and Robin Hicks, "China's Belt and Road Initiative could lead to 3°C global warming, report warns," Eco-Business, September 2, 2019, https://www.eco-business.com/news/chinas-belt-and-road-initiative-could-lead-to-3c-global-warming-report-warns/.
[xlviii] "Poland and China sign strategic partnership declaration," Polish Ministry of Foreign Affairs, June 21, 2016, https://poland.pl/economy/investments-projects/poland-and-china-sign-strategic-partnership-declaration/ and Adam Grzeszak, "The motorway that China couldn't build," *VoxEurop*, June 16, 2011, https://voxeurop.eu/en/the-motorway-that-china-couldnt-build/.
[xlix] Brinza, "How China Blew Its Chance in Eastern Europe," April 11, 2019.
[l] Ibid.
[li] Ibid.
[lii] Benner et al., "Authoritarian Advance," February 2018.
[liii] Ibid.
[liv] Ibid.
[lv] Ibid and François Godement and Abigaël Vasselier, "China at the Gates: A New Power Audit of EU-China Relations," European Council on Foreign Relations, December 2017, https://www.ecfr.eu/page/-/China_Power_Audit.pdf.
[lvi] Ivana Karásková, "How China Influences Media in Central and Eastern Europe," *China Observers in Central and Eastern Europe*, November 25, 2019, https://chinaobservers.eu/how-china-influences-media-in-central-and-eastern-europe/ and "China's Influence in Balkans and Central and Eastern Europe," Warsaw Institute, April 19, 2019, https://warsawinstitute.org/chinas-influence-balkans-central-eastern-europe/.
[lvii] Karásková, "How China Influences Media in Central and Eastern Europe," November 25, 2019.
[lviii] Ibid.
[lix] Le Corre, "China's Rise as a Geoeconomic Influencer," October 15, 2018.
[lx] Benner et al., "Authoritarian Advance," February 2018.
[lxi] Benner et al., "Authoritarian Advance," February 2018 and Karásková, "How China Influences Media in Central and Eastern Europe," November 25, 2019.
[lxii] Karásková, "How China Influences Media in Central and Eastern Europe," November 25, 2019.
[lxiii] Ibid.
[lxiv] Ibid.
[lxv] Ibid.
[lxvi] Ibid.
[lxvii] Benner and Wright, Testimony, April 5, 2018 and Kendall-Taylor, Prepared Statement, May 9, 2019.
[lxviii] Ibid.
[lxix] Elizabeth Economy, *The Third Revolution: Xi Jinping and the New Chinese State* (Oxford: Oxford University Press, 2018).
[lxx] Oudenaren, "Why China Is Wooing Eastern and Central Europe," September 4, 2018.
[lxxi] Joshua Meltzer, "China's One Belt One Road initiative: A view from the United States," Brookings Institution, June 19, 2017, https://www.brookings.edu/research/chinas-one-belt-one-road-initiative-a-view-from-the-united-states/.
[lxxii] Brinza, "How China Blew Its Chance in Eastern Europe," April 11, 2019.
[lxxiii] Benner and Wright, Testimony, April 5, 2018.
[lxxiv] James Kynge and Michael Peel, "Brussels rattled as China reaches out to eastern Europe," *Financial Times*, November 27, 2017, https://www.ft.com/content/16abbf2a-cf9b-11e7-9dbb-291a884dd8c6.
[lxxv] Benner et al., "Authoritarian Advance," February 2018.
[lxxvi] Godement and Vasselier, "China at the Gates," December 2017.
[lxxvii] Aime Williams, James Shotter, Monika Pronczuk, and Michael Peel, "U.S. warns of Huawei's growing influence over eastern Europe," *Financial Times*, February 10, 2019, https://www.ft.com/content/09928e84-2be0-11e9-a5ab-ff8ef2b976c7; Lesley Wroughton and Gergely Szakacs, "Pompeo warns allies Huawei presence complicates partnership with U.S.," *Reuters*, February 10, 2019, https://www.reuters.com/article/us-usa-pompeo-hungary/pompeo-warns-allies-huawei-presence-complicates-partnership-with-u-s-idUSKCN1Q0007; and "China's spreading influence in Eastern Europe worries West," *Associated Press*, April 10, 2019,

https://federalnewsnetwork.com/government-news/2019/04/chinas-spreading-influence-in-eastern-europe-worries-west/.
[lxxviii] Kendall-Taylor, Prepared Statement, May 9, 2019.
[lxxix] Slobodan Lekic, "In a first for Beijing in Europe, Serbia to receive Chinese armed drones," *Stars and Stripes*, September 10, 2019, https://www.stripes.com/news/europe/in-a-first-for-beijing-in-europe-serbia-to-receive-chinese-armed-drones-1.598166.
[lxxx] European Commission, Joint Communication to the European Parliament, the European Council and the Council, "EU-China – A strategic outlook," March 12, 2019, https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf.
[lxxxi] North Atlantic Council, "London Declaration," December 4, 2019, https://www.nato.int/cps/en/natohq/official_texts_171584.htm.
[lxxxii] Eder and Mardell, "Belt and Road Reality Check," July 10, 2018.
[lxxxiii] Stuart Lau, "Czech president to skip Beijing summit over China 'investment letdown,'" *South China Morning Post,* https://www.scmp.com/news/china/diplomacy/article/3045917/czech-president-skip-beijing-summit-over-china-investment.
[lxxxiv] David Wemer, "The Three Seas Initiative explained," The Atlantic Council, February 11, 2019, https://www.atlanticcouncil.org/blogs/new-atlanticist/the-three-seas-initiative-explained-2/.
[lxxxv] Benner and Wright, Testimony, April 5, 2018.
[lxxxvi] Small, "Why Europe Is Getting Tough on China," April 3, 2019.

Endnotes: Five Models of Strategic Relationship in Proxy War

[i] Candace Rondeaux and David Sterman, "Twenty-First Century Proxy Warfare: Confronting Strategic Innovation in a Multipolar World Since the 2011 NATO Intervention," *New America*, February 2019, 15.
[ii] *Joint Integrated Campaigning* (Washington, DC: Government Printing Office, 2018), 8.
[iii] Keegan, 329; Geoffrey Parker, "Dynastic War," in Geoffrey Parked ed., *The Cambridge History of Warfare*, (Cambridge: Cambridge University Press, 2005), 148-163.
[iv] John Keegan, *The History of Warfare* (New York: Vintage Press, 1993), 5.
[v] Joel Watson, *Strategy: An Introduction to Game Theory* (London: W.W. Norton and Company, 2015), 3.
[vi] Amos Fox, "Conflict and the Need for a Theory of Proxy Warfare," *Journal of Strategic Security* 12, no. 1 (2019): 49. DOI: https://doi.org/10.5038/1944-0472.12.1.1701.
[vii] Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 984), 603.
[viii] B.H. Liddell Hart, *Why Don't We Learn from History?* (New York: Hawthorne Books, 1971), 88-89.
[ix] Kathleen Eisenhardt, "Agency Theory: An Assessment and Review," *The Academy of Management Review* 14, no. 1 (January 1989): 58-59, https://www.jstor.org/stable/258191; Joel Watson, *Strategy: An Introduction to Game Theory* (London: W.W. Norton and Company, 2015) 303-308.
[x] Ibid.
[xi] Ibid.
[xii] "Death Toll Up to 13,000 in Ukraine Conflict, Says UN Rights Office," *Radio Free Europe/Radio Liberty*, February 26, 2019, https://www.rferl.org/a/death-toll-up-to-13-000-in-ukraine-conflict-says-un-rights-office/29791647.html.
[xiii] See the author's works, "Time, Power, and Principal-Agent Problems: Why the US Army is Ill-Suited for Proxy War Hotspots," *Military Review* (March-April 2019), 28-42; "In Pursuit of a Theory of Proxy Warfare," *Land Warfare Paper* 123, (February 2019); and "Conflict and the Need for a Theory of Proxy Warfare," *Journal of Strategic Security* 12, no. 1 (2019): 44-71, https://doi.org/10.5038/1944-0472.12.1.1701.
[xiv] Michael Cohen, "Ukraine's Battle of Ilovaisk, August 2014: The Tyranny of Means," *Army Press Online Journal* 16-25, (February 4, 2017), https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/documents/16-25-Cohen-10Jun16a.pdf; Amos Fox, "Hybrid Warfare: The 21st Century Russian Way of Warfare," Fort Leavenworth, Kansas, (2017), 42-51.
[xv] "Alexander Zakharchenko: Mass Turnout for Ukraine's Rebel Funeral," *BBC*, September 2, 2018, https://www.bbc.com/news/world-europe-45388657.
[xvi] "Separatist Commander 'Givi' Killed in Eastern Ukraine," *Radio Free Europe/Radio Liberty*, February 8, 2017, https://www.rferl.org/a/ukraine-donetsk-separatis-leader-givi-killed/28297344.html.
[xvii] Marc Bennetts, "Rebel Leader Alexander Zakharchenko Killed in Explosion in Ukraine," *The Guardian*, August 13, 2018, https://www.theguardian.com/world/2018/aug/31/rebel-leader-alexander-zakharchenko-killed-in-explosion-in-ukraine; author interviews with multiple Ukrainian army officers, October 2017-December 2019.
[xviii] Ruby Mellen, "A Brief History of the Syrian Democratic Forces, the Kurdish-led Alliance That Helped the U.S. Defeat the Islamic State," *Washington Post*, October 7, 2019, https://www.washingtonpost.com/world/2019/10/07/brief-history-syrian-democratic-forces-kurdish-led-alliance-that-helped-us-defeat-islamic-state/.
[xix] Nicholas Heras, John Dunford, and Jennifer Cafarella, "Governing After ISIS: What's Next for the Syrian Democratic Forces," *Overwatch*, episode 13, February 28, 2020.
[xx] Megan Specia, "Why is Turkey Fighting the Kurds in Syria," *New York Times*, October 9, 2019, https://www.nytimes.com/2019/10/09/world/middleeast/kurds-turkey-syria.html.
[xxi] Aaron Stein, "Operation Olive Branch: Status Update," *Atlantic Council*, March 13, 2018, https://www.atlanticcouncil.org/blogs/syriasource/operation-olive-branch-status-update/.
[xxii] Idrees Ali, "Turkish Offensive in Syria Leads to Pause in Some Operations Against IS: Pentagon," *Reuters*, March 15, 2018, https://www.reuters.com/article/us-mideast-crisis-syria-turkey-pentagon/turkish-offensive-in-syria-leads-to-pause-in-some-operations-against-is-pentagon-idUSKBN1GH2YW; "Coalition Continues Operations to Defeat Daesh in Syria," *U.S. Central Command* Press Release, November 23, 2019, https://www.centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/2025134/coalition-continues-operations-to-defeat-daesh-in-syria/.

[xxiii] Specia.
[xxiv] Shawn Snow, "The End of an Era: 60,000 Strong US-Trained SDF Partner Force Crumbles in a Week Under Heavy Turkish Assault," *Military Times*, October 14, 2019, https://www.militarytimes.com/2019/10/14/the-end-of-an-era-60000-strong-us-trained-sdf-partner-force-crumbles-in-a-week-under-heavy-turkish-assault/.
[xxv] Specia.
[xxvi] Clausewitz, 603.
[xxvii] Michael Gordon, "Iraq's Leader Requests More Aid in the Fight Against ISIS," *New York Times*, December 3, 2014, https://www.nytimes.com/2014/12/04/world/middleeast/iraqi-leader-seeks-additional-aid-in-isis-fight.html.
[xxviii] Tamer El-Ghobashy and Mustafa Salim, "Iraqi Military Reclaims City of Tal Afar after Rapid Islamic State Collapse," *Washington Post*, 27 August 2017, https://www.washingtonpost.com/world/middle_east/iraqi-military-reclaims-city-of-tal-afar-after-rapid-islamic-state-collapse/2017/08/27/a98e7e96-8a53-11e7-96a7-d178cf3524eb_story.html.
[xxix] Michael Knights, "Kirkuk: The City That Highlights Iraq's War Within a War," *BBC*, October 17, 2017, https://www.bbc.com/news/world-middle-east-41656398.
[xxx] Aaron Mehta, "Tillerson: US Could Stay in Iraq to Fight ISIS, Wanted or Not," *DefenseNews*, 30 October 2017, https://www.defensenews.com/pentagon/2017/10/30/tillerson-us-could-stay-in-iraq-to-fight-isis-wanted-or-not/.
[xxxi] The U.S. military refers to these forces as "Guardian Angels" and "Security Forces," or "SECFOR" as they are most referred.
[xxxii] Kenneth Katzman and Clayton Thomas, "Afghanistan: Post-Taliban Governance, Security, and US Policy," *Congressional Research Service*, December 13, 2017, 33-36.
[xxxiii] Global Conflict Tracker: War in Afghanistan, Council on Foreign Relations, last updated February 13, 2020, https://www.cfr.org/interactive/global-conflict-tracker/conflict/war-afghanistan.
[xxxiv] Jibran Ahmad, "Taliban dismiss Afghanistan's Peace Talks," *Reuters*, December 29, 2018, https://www.reuters.com/article/us-afghanistan-taliban/taliban-dismiss-afghanistans-peace-talks-offer-idUSKCN1OT051.
[xxxv] Kyle Rempfer and Howard Altman, "Afghan Forces Facing an Increase in Insider Killings," *Army Times*, February 14, 2020, https://www.armytimes.com/news/your-army/2020/02/14/insider-attack-on-7th-group-involved-two-anp-shooters/.
[xxxvi] Keegan, 12.
[xxxvii] Romanovs, define 'All Russias' in the following manner: Muscovy is "Great Russia," Belorussia, or Belarus, is "White Russia," Ukraine is "Little Russia," Crimea (initially annexed by the Romanovs from the Crimean Khanate in 1783) and southern Ukraine, is "New Russia" or "Novorossiya," and Galacia (parts of modern-day southeastern Poland and portions of western Ukraine), is "Red Russia." Simon Montefiore, *The Romanovs, 1613-1918* (New York: Vintage Books, 2017), 365.
[xxxviii] Paul Sonne, "With 'Novorossiya,' Putin Plays the Name Game with Ukraine," *Wall Street Journal*, September 1, 2014, https://www.wsj.com/articles/with-novorossiya-putin-plays-the-name-game-with-ukraine-1409588947.
[xxxix] Timothy Heritage, "Putin Vows to Protect Ethnic Russians Abroad After Ukraine Truce Expires," *Reuters*, July 1, 2014, https://www.reuters.com/article/us-ukraine-crisis-putin-russians/putin-vows-to-protect-ethnic-russians-abroad-after-ukraine-truce-expires-idUSKBN0F646620140701.
[xl] Jack Watling, "Iran's Objectives and Capabilities: Deterrence and Subversion," *RUSI Occasional Paper*, (February 2019), 13-32.
[xli] Ibid.
[xlii] Lyse Doucet, "Qasem Soleimani: US Kills Top Iranian General in Baghdad Airstrike," *BBC News*, January 3, 2020, https://www.bbc.com/news/world-middle-east-50979463.
[xliii] Nicollo Machiavelli, *The Prince* (New York: Signet Classic, 1999). 71-82.
[xliv] David Hackett Fischer, *Washington's Crossing* (Oxford: Oxford University Press, 2004), 324-345.
[xlv] Jeremy Scahill, *Blackwater: The Rise of the World's Most Powerful Mercenary Army* (New York: Nation Books, 2007), 122-132.
[xlvi] Gian Gentile, et al., *Reimagining the Character of Urban Operations for the US Army, How the Past Can Inform the Present and Future* (Santa Monica, CA: RAND Corporation, 2017), 67-85.
[xlvii] Dana Priest, "Private Guards Repel Attack on U.S. Headquarters," *Washington Post*, August 6, 2004, https://www.washingtonpost.com/archive/politics/2004/04/06/private-guards-repel-attack-on-us-

headquarters/fe2e4dd8-b6d2-4478-b92a-b269f8d7fb9b/; David Isenberg, "Blackwater, Najaf – Take Two," *CATO Institute*, May 16, 2008, https://www.cato.org/publications/commentary/blackwater-najaf-take-two; Jeremy Scahill, *Blackwater: The Rise of the World's Most Powerful Mercenary Army* (New York: Nation Books, 2007), 122-132.
[xlviii] Rebecca Kheel, "Faced With Opposition, Erik Prince Shops His Plan for Afghanistan," *The Hill*, August 24, 2018, https://thehill.com/policy/defense/403146-faced-with-opposition-erik-prince-shops-his-plan-for-afghanistan.
[xlix] Neil Hauer, "The Rise and Fall of a Russian Mercenary Army," *Foreign Policy*, October 6, 2019, https://foreignpolicy.com/2019/10/06/rise-fall-russian-private-army-wagner-syrian-civil-war/.
[l] Ibid.
[li] David Smith, "South Africa's Aging White Mercenaries Who Helped Turn the Tide on Boko Haram," *The Guardian*, April 14, 2015, https://www.theguardian.com/world/2015/apr/14/south-africas-ageing-white-mercenaries-who-helped-turn-tide-on-boko-haram; Scahill, 361-364.
[lii] Maria Tsvetkova, "Russian Toll in Syria Battle Was 300 Killed and Wounded: Sources," *Reuters*, February 18, 2018, https://www.reuters.com/article/us-mideast-crisis-syria-russia-casualtie/russian-toll-in-syria-battle-was-300-killed-and-wounded-sources-idUSKCN1FZ2DZ.
[liii] Peter Singer, "The Truth About Blackwater," *Brookings*, October 2, 2007, https://www.brookings.edu/articles/the-dark-truth-about-blackwater/.
[liv] Thomas Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 94.
[lv] Robert Baer, "Iraqi's Mercenary King," *Vanity Fair*, March 6, 2007, https://www.vanityfair.com/news/2007/04/spicer200704

Endnotes: The Critical Importance of Brown-Water Operations in the Era of Great Power Competition

[i] "How will the Belt and Road Initiative advance China's interests?" Center for Strategic and International Studies. October 18, 2019. https://chinapower.csis.org/china-belt-and-road-initiative/
[ii] Ellyatt, Holly. "From Africa to Azerbaijan, here's how far Russia's global influence stretches." CNBC. February 10, 2020. http://cnbc.com/2020/02/10/russias-global-influence-stretches-from-venezuela-to-syria.html
[iii] Gray, Colin. "Handfuls of Heroes on Desperate Ventures: When Do Special Operations Succeed?" *Parameters* Spring, no. 1 (1999): 2-24.
[iv] Department of the Army. *Special Forces Waterborne Operations (ATP 3-18.12)*. Fort Bragg: John F. Kennedy Special Warfare Center and School, 2016.
[v] Scheffer, Jason. "The Rise and Fall of the Brown Water Navy: Changes in United States Navy Riverine Warfare Capabilities from the Vietnam War to Operation Iraqi Freedom." Master's thesis, U.S. Army Command and General Staff College, 2005.
[vi] Scheffer, 64.
[vii] Scheffer, 66.
[viii] Scheffer, 68.
[ix] Burke, Matthew. "Riverine success in Iraq shows need for naval quick-reaction force." *Stars and Stripes*, October 29, 2012, 1-2.
[x] Rosamond, Jon. "Mk VI Patrol Boat promises greater reach for US coastal forces." *Jane's Defence Weekly*, July 17, 2014.
[xi] Brunson, Richard. "NECC announces formation of Coastal Riverine Force." *The Flagship*, May 17, 2012, 1.
[xii] Department of the Navy. *Naval Costal Warfare Operations (NTTP 3-10.1)*. Washington D.C.: Navy Warfare Library, 2017.
[xiii] Brunson, 3.
[xiv] Harrison, Nicholas. "Professionalize the Coastal Riverine Force." *Proceedings* 146, no. 2 (2020): 34-36.
[xv] Dutton, Timothy & Justin Parker. *Special Operations Craft - Riverine*. Cambridge: Massachusetts Institute of Technology, 2017.
[xvi] Dutton & Parker, 2.
[xvii] Sofge, Erik. "Smoke on the water: behind the scenes with a Special Operations gunboat crew." *Popular Mechanics*. March 1, 2009.
[xviii] Murphy, Jack. "Inside the Philippine Special Forces Regiment." SOFREP. May 15, 2017. https://sofrep.com/news/inside-philippine-special-forces-regiment/
[xix] Murphy, 3.
[xx] Cragin, Kim, Peter Chalk, Sara A. Daly, and Brian A. Jackson. "Mindanao: A Mecca for Transnational Terrorism in Southeast Asia." In *Sharing the Dragon's Teeth: Terrorist Groups and the Exchange of New Technologies*, 23-46. Santa Monica, CA; Arlington, VA; Pittsburgh, PA: RAND Corporation, 2007. Accessed March 13, 2020. www.jstor.org/stable/10.7249/mg485dhs.11.
[xxi] Craigin et. al., 41-43.
[xxii] Ambrum, Sharon. "Special Forces Riverine Battalion." *Philippine Tripod*, April 4, 24, 2007. 1-3.
[xxiii] Robles, Raissa. "Militia fishing ships 'not on agenda' as Chinese coastguard visits Philippines," South China Morning Post, accessed March 2, 2020. https://www.scmp.com/week-asia/politics/article/3046087/militia-fishing-ships-not-agenda-chinese-coastguard-visits
[xxiv] Viray, Patricia. "Fact check: Duterte's claims on US aid to military," *PHILSTAR*, October 23, 2017. 1-4.
[xxv] Sanchez, Katherine. "U.S., Philippines Special Operations Forces Train Together as Part of Flash Piston," United States Navy Press Release NNS0800707-01, accessed March 7, 2020. https://www.navy.mil/submit/display.asp?story_id=38131
[xxvi] LaGrone, Sam. "U.S. Gives Philippine Marines Six Riverine Boats for Counter Terrorism Missions," USNI News, accessed March 2, 2020. https://news.usni.org/2013/09/26/u-s-gives-philippine-marines-six-riverine-boats-counter-terrorism-missions
[xxvii] Viray, 2.
[xxviii] Viray, 3.

[xxix] Livieratos, Cole. "A Cultural Failure: U.S. Special Operations in the Philippines and the Rise of the Islamic State," War on the Rocks, accessed February 15, 2020. https://warontherocks.com/2017/07/a-cultural-failure-u-s-special-operations-in-the-philippines-and-the-rise-of-the-islamic-state/
[xxx] Willey, Paul. "The Art of Riverine Warfare from an Asymmetrical Approach." Master's thesis, Naval Postgraduate School, 2004.
[xxxi] Wiley, 29.
[xxxii] Wiley, 32.
[xxxiii] Munson, Mark. "Columbia's Riverine Force." CIMSEC. July 26, 2013. http://cimsec.org/colombias-riverine-force/6439
[xxxiv] Norman, Jack. "Columbia's military emerges as a global prayer in US-led alliance," Columbia Reports, accessed February 15, 2020. https://colombiareports.com/colombias-military-emerges-as-a-global-player-in-us-led-alliance/
[xxxv] United States Government Accountability Office. *Plan Columbia (Report to the Honorable Joseph R. Biden, Jr., Chairman, Committee on Foreign Relations, U.S. Senate, GAO-09-71)*. Washington DC: GAO, 2008.
[xxxvi] Norman, 38.
[xxxvii] Wiley, 31.
[xxxviii] United States Government Accountability Office, 38.
[xxxix] Wiley, 35-36.
[xl] United States Special Operations Command. *FY07 Joint Combined Exchange Training Program: Annual 2011 Report to Congress.* Washington DC: USSOCOM, 2011.
[xli] Munson, 3.
[xlii] Strangio, Sebastian. "The lawless playgrounds of Laos," Al-Jazeera, accessed February 5, 2020. https://www.aljazeera.com/indepth/features/2016/05/lawless-playgrounds-laos-160504120318409.html
[xliii] Strangio, 1.
[xliv] Sullivan, Michael. "China reshapes the vital Mekong River to power its expansion," *NPR Weekend Edition*, October 6, 2018. 1-5.
[xlv] Strangio, 2.
[xlvi] Sullivan, 3.
[xlvii] Joint Chiefs of Staff. *Command and Control of Joint Maritime Operations (JP 3-32).* Washington DC: Joint Staff/J7/Doctrine Division, 2018.
[xlviii] Congressional Research Service. *Egypt: Background and U.S. Relations.* Washington DC: CRS, 2019.
[xlix] Max Security. "Strategic Analysis: Repercussions of Chinese investments in the Nile River Basin," Max Security Consulting, accessed February 14, 2020. https://www.maxsecurity.com/reports/strategic-analysis-reprecussions-of-chinese-investments-in-the-nile-river-basin/
[l] Mahlakeng, M.K. "China and the Nile River Basin: The Changing Hydropolitical Status Quo." *Insight on Africa* 10, no. 1 (January 2018): 73–97. doi:10.1177/0975087817741043.
[li] Max Security, 4.
[lii] Congressional Research Service, 10.
[liii] Congressional Research Service, 16.