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 https://georgetownsecuritystudiesreview.org

Follow the Georgetown Security Studies Review on Twitter @gssreview

Contact the Editor in Chief at gssr@georgetown.edu
# TABLE OF CONTENTS

**Winning the War of Ideas**
How the United States Can Use Counter-Messaging to Fight the Russian Imperial Movement  
*Carley Berlin*

**Trafficking of Women in Bangladesh**
An Analysis from a Feminist Human-Security Framework  
*Shuva Das and Leo S.F. Lin*

**Hardening the Shield Against North Korea’s “All-Purpose Sword”**
An Evolving North Korean Cyber Threat and Its Policy Responses  
*Jie Gao*

**Authoritarian Friends and Totalitarian Enemies**
The Relevance of the Kirkpatrick Doctrine in the Twenty-First Century  
*Steven Hu*

**Enemies, Allies, and Artificial Intelligence**
Developing Rules and Norms for Lethal Autonomous Weapons Systems  
*Kiseok Michael Kang*

**Irregular Conflict, Irregular Harms**
Analyzing Patterns of Civilian Harm in the South China Sea  
*Alisa Laufer*

**Technology Companies as Emerging Superpowers**
A Brazil Case Study on the Competition Between American and Chinese Technology Companies for Global Influence  
*Ona Spreenberg*
Winning the War of Ideas: How the United States Can Use Counter-Messaging to Fight the Russian Imperial Movement

Carley Berlin

The Russian Imperial Movement (RIM) aims to portray itself in a way that conflicts with how it operates. The group wants to be seen as a politically savvy, nationalist group. However, RIM’s actions reveal it to be a violent and international paramilitary group that is a favorite tool of the Kremlin. Members have engaged in Syria, Libya, and Ukraine to justify Russian aggression and have also been linked to other terrorist groups in their training camps and worldwide conventions. The United States’ decision to designate RIM as a terrorist organization expanded the set of counterterrorism tools available, including some used against groups like ISIS and AQ. The SDGT designation successfully allows the US government to incentivize corporate entities and economically sanction the group.

Violent white supremacy, however, is not contained within a nation’s borders; RIM demonstrated that groups are increasingly interconnected. For that reason, the United States should investigate RIM’s transnational network of white supremacist organizations. The organization has links to like-minded groups that pose threats to the United States. Twenty years ago, the United States underestimated the rise of Islamic terrorism. The United States needs to counter right-wing propaganda online as part of its CT strategy by using former white supremacists as messengers. Beating RIM will require a holistic CT approach, with resources dedicated to countering their online propaganda. This is the best way to halt the number of members joining and provide opportunities for disengagement from the organization and ideology.

Introduction

Shortly before invading Ukraine in 2022, Russian President Vladimir Putin claimed that Ukraine faced a problem with neo-Nazis. “The purpose of this operation is to protect people who for eight years now have been facing humiliation and genocide perpetrated by the Kyiv regime,” he said, according to an English translation from the Russian Mission in Geneva. "To this end, we will seek to demilitarize and de-nazify Ukraine, as well as bring to trial those who perpetrated numerous bloody crimes against civilians, including against citizens of the Russian Federation."¹ This rhetoric, which several other high-ranking Russian officials repeated, has since been debunked.

Moreover, reports surfaced that the alleged neo-Nazi threat is manufactured by Russia; in fact, the Kremlin is sending neo-Nazi groups into Ukraine to justify its violence.² One of the groups being sent to Ukraine is the Russian Imperial Movement (RIM). This is not the first time that RIM has attracted international attention and posed international security threats to the United States and its allies.

In 2020, the US State Department designated the Russian Imperial Movement as a terrorist organization. The 2020 listing was the first time that a far-right group - and three of its leaders - were labeled as Specially Designated Global Terrorists (SDGT) by the United States. The designation symbolized the rising threat of right-wing extremism and the unique threat that this specific organization poses to the United States. A combination of the pandemic, disinformation, and increased political polarization has led to rising rates
of violent right-wing extremism at home and abroad. Since 9/11, jihadists have killed slightly fewer American citizens than far-right terrorists (107 compared to 112 victims). Black separatist/nationalist ideologues, misogynists, and far-left terrorists have killed 12, 17, and 1, respectively.

This paper will look at the dichotomy between how RIM presents itself and how it acts, discuss the current US counterterrorism (CT) strategy against the organization, analyze proposed CT measures, and then offer additional potential countermeasures to better combat RIM’s propaganda in conjunction with the SDGT designation. The United States’ decision to designate RIM as SDGTs is not an effective counterterrorism approach on its own. The United States should counter right-wing propaganda with strong counter-messaging as part of a more comprehensive counterterrorism (CT) strategy. Utilizing former white supremacists will help dissuade potential recruits from joining the organization and persuade members to disengage from the extremist ideology. Deradicalizing, or disengaging from violent political or religious extremism, is a complicated – and necessary - process. This can only be achieved through a carefully coordinated communications approach.

RIM Overview

It is important to understand a terrorist group’s ideology, strategy, and tactics in order to properly assess the best CT strategies to fight it. RIM is a St. Petersburg-based organization, formed in 2002 by Stanislav Anatolyevich Vorob’ev, that promotes a white supremacist, right-wing, Orthodox Christian ideology. RIM is a nationalist organization, promoting ethnic Russian nationalism and the restoration of the Russian tsarist regime. RIM is strongly influenced by Russian philosopher Aleksandr Dugin, an ultranationalist – also known as “Putin’s brain” – who believes that it is the country’s religious imperative to spread Russian Orthodoxy through violence. The language used by RIM and other white supremacists is part of a concerted effort to craft “a less recognizable poison for the disillusioned white masses to swallow.” Old racist tropes are polished to sound more like conservative foreign policy terms, such as the use of the word “globalism” as a euphemism for “Zionism.”

RIM operates within the Russian political system and maintains close relationships with Rodina, a far-right party co-founded by Russia’s Deputy Prime Minister, Dmitry Rogozin. Together, RIM and Rodina convened the World National Conservative Movement (WNCM) in June 2015, which catapulted the organization to the national stage, cemented its international network, and legitimized it as an asset in the eyes of the Kremlin. WNCM’s manifesto claims to bring together like-minded activists who believe that the world is governed by liberalism, multiculturalism, and tolerance that lead to mass migration, a loss of religiousness, overconsumption, and a lack of family morals and values. This is a similar strategy to other right-wing extremist organizations. The Patriot Front, for example, seeks support from other Christian, right-leaning citizens by invoking political topics. RIM aims to project an image of a well-connected, politically savvy organization.

Yet this image is vastly different from how it truly operates. RIM is the epicenter of a global network of militant extremists. The Imperial Legion, RIM’s armed wing, prepares Russian militants to fight government security forces through “Partizan,” a training course led by ex-Russian military members. Intelligence suggests the Kremlin approves of – and may even directly support – the Partizan course.
It teaches bomb-making, marksmanship, combat medicine, assault, and building clearance. Imperial Legion members fought in Libya, Syria, and most recently, Ukraine. Analysts believe that RIM members are fighting in Libya on the side of the Libyan National Army, to support the Russian-backed Khalifa Haftar – but it is unconfirmed when RIM entered the region. According to RIM’s own social media, RIM has been sending fighters to Syria to protect Christians in the region since at least April 2019. In addition, RIM fighters have been reinforcing pro-Russian separatists fighting against the Ukrainian government since at least 2014. In 2015, RIM leader Stanislav Vorobyev explained that he does not believe in a separate Ukrainian nation and that the donations to the armed wing provide “clothes, shoes, special equipment—communications, body armor” for every militant it sends to Ukraine.

Partizan also provides paramilitary training to foreign nationals from its facilities in St. Petersburg. Some of these individuals were linked to international terrorist incidents, such as the 2017 bombing in western Sweden by two Swedish participants of Partizan and anti-lockdown protests and vigilante anti-migrant border patrols conducted by members of two German extremist groups (The National Democratic Party and The Third Path) in 2020. The organization is known for having a network of violent members and sympathizers abroad in preparation for the alleged war against the “globalized elite” who reject “traditional” values. It is a violent, paramilitary organization that spreads its ideology online and through in-person training. This ideology is not unique to RIM. The Irish Republican Army (IRA), for example, portrayed itself as an anti-British and non-violent organization, but undoubtedly employed violence. This strategy is common for extremist organizations; the good news is that the United States can learn from past organizations to determine what might hinder RIM.

The Kremlin and RIM

RIM and the Kremlin have a symbiotic relationship because they often share the same international goals. VOA reported that the Kremlin knew – and never hid - what the Russian Imperial Movement was doing. RIM’s recruitment efforts and pledge to send members to combat zones were beneficial to the Kremlin in its aggression against Ukraine. RIM is not officially sponsored by Russia, but it is tolerated by the Kremlin because it helps spur extremist action in countries opposed to Russia - one of the reasons why the State Department designated RIM as a terrorist organization. RIM has an outsized role on the international stage; it trains, recruits, shares information with, and builds connections with domestic extremists in the United States and its allies. RIM posts content online in English, German, and Russian to spread its ideology, and its propaganda videos include detailed paramilitary training.

RIM is a successful tool of the Kremlin because it created an international network of extremists. The transnational network helps to undermine and divide democracies, by sharing information and empowering other actors. Numerous American neo-Nazis traveled to Russia to attend networking conferences, where they were welcomed with open arms – a vast difference from how Russia treats internal dissent. In turn, white supremacists perceive benefits in supporting Russia. Firstly, they claim to have the same enemy – “globalism” and the “system” of elites. Second, both challenge the liberal world order and the current foreign policy.
Third, they use similarly sexist language and masculine imagery. Both white supremacy and Putin’s ideology also have misogynistic roots. This is not a coincidence, as each of these claims happens to be antithetical to democratic institutions and the West. This allows white supremacists an opportunity to bond over qualities that separate them further from the United States.

Social media further enables white supremacists. Its decentralized structure allows individuals to connect and share information in a new way, enabling terrorists to directly and quickly reach a large audience without significant infrastructure, an ideal environment for “lone wolf” attacks. The fewer people believe in the value of political solutions, the more violence and division look like viable solutions. The Kremlin copies how RIM uses social media to further its agenda and will likely continue to impact US politics by influencing the political narratives in the United States. The Russian government uses sites like Gab and Parler to capitalize on existing support for the far-right, encourage chaos, and decrease trust in governments.

These efforts by the Kremlin have had successes in the United States, most notably related to the 2016 US presidential election, for which eleven Russian military intelligence officers were named in connection with a hacking conspiracy to undermine Hillary Clinton’s campaign. More recently, a January 2022 YouGov poll showed that Republicans viewed Putin more favorably than Democratic politicians, and in February 2022, two Republican members of Congress chanted for Putin and against Democrats. Previous Kremlin efforts focused on small, niche, social media websites but are gaining more prevalence on mainstream sites such as Facebook and Twitter.

Current CT Strategy: Overview of the SDGT Designation

Counterterrorism tools are chosen based on the threat that the terrorist organization poses, and the State Department’s decision to designate RIM as an SDGT in August 2020 demonstrated the significant threat that it posed to the United States. SDGT is both a symbolic and practical step in the fight against international white supremacist networks. Under Executive Order (EO) 13224 – authorized by the International Emergency Economic Powers Act – the President can declare national emergencies and direct the Departments of State and Treasury to designate foreign groups or individuals as Specially Designated Global Terrorists. The SDGT designation allows the United States to fight international white supremacy, by utilizing the power of sanctions. Significantly, the SDGT designation of RIM is the first time that the United States recognized a white supremacist group as an SDGT. Previously, the designation was reserved for jihadi terrorist groups, including ISIS, al-Qaeda (AQ), and its affiliates.

It is important to note that labeling a terrorist organization does not always create the desired effect. Terrorist designations can create a backlash effect because the listing is used as a status symbol and recruiting tool. There are several reasons why measuring the impact of a terrorist designation is difficult: a) it is difficult to connect national security strategy to direct outcomes and changes in how terrorists act; b) it is difficult to measure progress because of the challenges associated with measuring a counterfactual; c) it is hard to define how tactics impact strategy outcomes; and d) clandestine groups do not broadcast metrics. The designation itself does not change terrorists’ behavior, but the financial, legal,
operational, and immigration consequences can impact their behavior.\textsuperscript{31}

The tools in the counterterrorism “toolbox” can be grouped into seven categories: diplomatic, information, military, economic, financial, intelligence, and law enforcement, also known as DIMEFIL. Different policies allow decision-makers the opportunity to use different tools, and the SDGT designation unlocks a set of CT policy tools that can be used against RIM: financial, law enforcement, and information.

The first tool is financial, and it has largely been a success. For example, the Department of Treasury designated al-Shabaab financial facilitators and weapons smugglers, who are closely integrated with ISIS-Somalia.\textsuperscript{32} The SDGT designation allowed the Treasury to target the network of weapons traffickers, their associates, and affiliated businesses. An SDGT designation also allows the federal government to block and interdict assets of those affiliated with the organization. It can lead to criminal prosecutions, although it more commonly leads to civil penalties. Financial institutions are required to freeze RIM’s assets after being alerted by the State and Treasury Departments. The United States has an outsized impact on the global financial system, so these measures are particularly effective at blocking RIM’s access to assets in the US and the ability to move money.\textsuperscript{33} The SDGT designation successfully allows the US government to incentivize corporate entities and economically sanction groups such as RIM.

The second CT tool is a combination of intelligence and law enforcement measures. This tool has limited success because civil liberty protections granted by the First Amendment limit law enforcement from investigating US citizens who potentially consume RIM content.\textsuperscript{34} The First Amendment curtails the FBI and the Department of Homeland Security’s ability to investigate Americans but guarantees more authority to investigate individuals and groups associated with terrorist organizations. This differs from the expansive European and Canadian laws, which grant authorities the ability to outlaw domestic extremist groups and surveil suspects.

The SDGT designation is successful, however, against foreign agents of RIM or non-US citizens who provide support to RIM. They can be investigated, surveilled, and potentially prosecuted under SDGT. Even though the designation has not yet changed how law enforcement organizations investigate or build cases, it could lead to greater interagency cooperation between the domestic and international terrorism offices at the Department of Homeland Security, State Department, and National Counterterrorism Center, or through the Joint Terrorism Task Force.\textsuperscript{35} Furthermore, the designation will allow law enforcement to share intelligence with partners, aiding in the fight against terrorism.\textsuperscript{36} The 2018 National Strategy for Counterterrorism, a strategy document that complements the government’s rights to designate terrorists under SDGT, declares that the US government will work with state and local law enforcement, civil society, the private sector, and allied governments in the fight against terrorism.\textsuperscript{37} Measures by the State and Treasury Departments restrict RIM members from traveling to the United States and designate them as terrorists themselves.\textsuperscript{38} Additionally, RIM leadership is now restricted from building relationships with US citizens in person.\textsuperscript{39}

The third CT tool unlocked under the SDGT designation is related to information. This is considered the biggest failure of the campaign against RIM because recruitment and the sharing of ideology are done online and are therefore not impacted by the SDGT designation. Like other right-wing extremist
groups, RIM relies heavily on the Internet for recruiting, training, fundraising, propagating its ideology, and defining its enemies.\textsuperscript{40} Even though RIM was banned from Facebook, Twitter, and YouTube, it began moderating its content and moved to different platforms, including Google Forms and Russian social media sites, like VKontakte (the Russian equivalent of Facebook).\textsuperscript{41} Despite de-platforming initiatives, RIM has continued to recruit, train, fundraise, and spread its propaganda online through pages on Russian social media sites with more than 30,000 followers. Compelling technology companies to police users or require labels on extremist content risks violating First Amendment protections and is therefore not an effective CT strategy on its own.

### Evaluation of Current CT Strategy

Gauging the success of CT strategies is challenging because it is impossible to know whether the outcome was a result of the strategy or some other factor. Terrorists are independent actors and often do not behave like the US government, nor do they share details about the outcome of certain strategies implemented against them. An internal schism, the death of a leader, or a shift in ideology could change the activity of the terrorist organization instead of it being a direct result of a CT measure.\textsuperscript{42} It is important to try to measure the effectiveness of certain strategies, however, because it “would allow policymakers to more efficiently allocate resources toward those activities having the greatest success.”\textsuperscript{43}

There are three outcomes one can use to quantitatively measure the effectiveness of CT programs: a) frequency, location, and targets of attacks; b) the number of groups and membership; and c) the frequency, lethality, simultaneous attacks, and types of weapons used before and after the designation. The US Government measures success by looking at the frequency of attacks, as well as the quantity of CT information shared.\textsuperscript{44} RIM has not committed a major attack outside of war zones since July 2020, suggesting that the current CT strategy is successful.\textsuperscript{45} However, a closer analysis paints a different picture. Since the 2020 terrorist designation, RIM engaged in violent campaigns, trained individuals who have perpetrated violent acts, and influenced a global network of white supremacists. In December 2022, German police arrested nearly 3,000 federal and regional law enforcement officers with connections to – if not support from – the Russian Imperial Movement.\textsuperscript{46}

The COVID-19 pandemic also changed the nature of how extremist groups spread propaganda. Increasingly more content is shared online, and actors see themselves as part of a global conversation.\textsuperscript{47} To reflect this change, counterterrorism success should thus be measured based on influence through online propaganda — a more qualitative measure than incidents or attacks. Influence can best be measured by how many people disengage from the right-wing ideology, but it can alternatively be measured by the presence (or absence) of key RIM messages online. One problem confounding a comprehensive evaluation of the strategy against RIM is that the United States designated RIM and its leaders as terrorists only in 2020. While there is not a set amount of time established in the literature on the length of time to measure progress against an organization, effectiveness is often measured across a longer period than two years. One can therefore use other terrorist organizations as case studies to predict how RIM may react to certain measures, but a more accurate assessment will be difficult until after a longer period of time.
Ineffective Proposed CT Strategy – FTO Designation

The SDGT designation allows the government to incentivize corporations and sanction groups – however, some analysts believe that the designation is not an effective military or law enforcement tool, nor does it properly stop individuals from being drawn into the ideology. The Secretary of State can designate a group as an FTO if it meets three criteria: it is a foreign entity, engages in terrorism, and threatens the United States. Advocates of this type of countermeasure believe that RIM should be designated as a Foreign Terrorist Organization (FTO), either in addition to or instead of an SDGT, even though listings are not mutually exclusive and can both be applied to foreign groups. The State Department’s SDGT designation is different from the more well-known FTO designation. Under an FTO listing, the FBI and Justice Department have more leeway to pursue criminal cases, as they are able to investigate anyone with close ties to FTOs. Since September 11, 2001, most charges have been related to individuals providing material support to a terrorist group. FTO has most frequently been applied to jihadi terrorist organizations and has not been applied to a far-right or white supremacist group to date.

There are several reasons why RIM has not been designated as an FTO. The first reason is that under the authority for SDTG designation, EO 13324, the government can sanction individuals and entities that provide training to terrorists. As RIM has a proven history of training an international network of white supremacists, this may be a particularly effective tool against the group; an FTO designation, on the other hand, more narrowly targets terrorist organizations that impact the United States. As the US has a documented list of individuals that have been trained through RIM and because RIM has not launched a physical attack against the US, FTO is less effective. The second reason is the SDGT is faster to officially designate and thus allows rapid action on countering the group. FTOs require a letter of concurrence from high-ranking officials in the Departments of Justice and Treasury to be sent to the State Department, as well as advance notification to Congress of the designation. The EO process does not require letters of concurrence nor advance notice to Congress, thus expediting the process. Third, SDGT designs last longer than FTO designs - indefinitely compared to a renewal every two years. Moreover, FTO listings are subject to administrative reviews every five years, which entails a compilation of classified and open-source information to demonstrate whether the statutory criteria are satisfied. If the Attorney General, Secretary of the Treasury, and Secretary of State determine that the group no longer meets the legal requirements for an FTO designation, it is taken off the list. If RIM was removed from the FTO list, it would send a troubling message about how the US views white supremacist groups. It is much harder to remove an SDGT designation, signifying the importance of countering RIM’s influence.

Ineffective Proposed CT Strategy – State Sponsor of Terror

Since 2020, Congress has debated the best way to combat RIM. The House Committee on Homeland Security voted to approve the Transnational White Supremacist Extremist Review Act, which “require[s] that the US Department of Homeland Security (DHS) ‘develop and disseminate a terrorist threat assessment of foreign white extremist groups.’ This would have helped counter RIM – and other white supremacist groups – by giving DHS
the authority to centralize collection of this intelligence. The legislation, however, does not seem likely to pass in the Senate because of how polarized the topic of white supremacy has become. In April 2022, members of the House Foreign Affairs Committee wrote a letter to Secretary of State Blinken urging him to consider whether Russia meets the threshold for state-sponsored terrorism.\(^{54}\) They cited Russia’s war crimes in Ukraine and support of US-designated terrorist groups, like RIM, as examples. Putin has used non-state groups to engage in terrorist activity, prior to and during the Ukraine conflict.\(^{55}\) These two Congressional recommendations are largely symbolic because specific sanctions enabled by the label are already imposed on Russia.\(^{56}\) Such sanctions include arms embargoes, trade restrictions, and foreign aid suspensions. Furthermore, the United States will not likely designate Russia as a state sponsor of terror because the political implications of this label constitute a serious escalation in tensions.

Potentially Effective Proposed CT Strategy – Counter-Messaging

The current SDGT designation provides some CT tools but is not comprehensive on its own. Additional measures should be taken to ensure that the United States can spread counter-messaging to decrease the public and sympathizers’ support and share information with foreign partners. Exposing the falsities in RIM’s messages is one of the best ways to counter the organization’s ability to recruit and spread its propaganda.\(^{57}\) The government can play an important role in decreasing the demand for radical and extremist messaging.

The United States has previously implemented strategies to counter-message terrorists. For example, a recently declassified 2005 Annex H to the National Military Strategic Plan for the War on Terrorism outlines the Defense Department’s strategic communications plan for the Global War on Terrorism (GWOT).\(^{58}\) This strategy aimed to create and lead an international effort to deny the terrorists the resources needed by focusing on their extremist ideology. Coordination of manpower, technology, and financial resources enabled the US military, in conjunction with other US agencies and coalition partners, to align their own messaging, share information with partners, and counter jihadi propaganda. A similar strategy can be used against RIM and right-wing extremism.

The United States can model its counter-messaging strategy against RIM on how it countered ISIS’s messages. Like that of ISIS, RIM’s propaganda is varied and directed at numerous audiences.\(^{59}\) Both groups are successful at developing a core narrative for each audience and in shaping their message. ISIS’s core message is about a caliphate, or model society, for followers and destruction for non-believers.\(^{60}\) Their network then reinforces the message by creating a sense that the state cannot protect its citizens. This makes it easier to recruit followers and hinder opposition.\(^{61}\) This message is very similar to how RIM communicates. Unfortunately, US government initiatives are often too centralized, reactive, and risk-averse. A more proactive, decentralized approach would have more success and would allow credible authors the ability to counter RIM’s messages.\(^{62}\)

The United States should use a three-tiered communication strategy to combat RIM’s extremism. The first tier is international, in which the US government facilitates an effort to help identify and empower trustworthy actors to communicate. The United States would identify former white supremacists from the United States, RIM, and other extremist
organizations to carry the message because of their unique understanding of the path to radicalization and what it takes to disengage from the ideology. Since RIM has a global reach, the actors engaged could be Russian and US nationals, or from some of the organizations trained by RIM in Partizan. The second tier is the national coalition; this is where the United States would work behind the scenes to develop the core narrative that RIM is peddling a dangerous, extremist ideology. A joint task force comprised of White House, DHS, National Security Agency, FBI, CIA, Defense Intelligence Agency, State Department, and Department of Education personnel would be most beneficial because of the expertise on right-wing extremism, the magnitude of its threat, and its methods for communication and radicalization online that each agency possesses. The third tier is local; these are areas where people are at risk of radicalization. This is the most difficult step to identify because a) viewing white supremacist content does not necessarily mean that an individual is radicalized, b) it is not illegal in the United States, and c) it is difficult to convince technology companies to police content on their sites. As previously discussed, the First Amendment protects the right to view online content, complicating the ability of law enforcement to determine who may be radicalizing, as well as the ability of online websites to prohibit certain terms. Close monitoring of RIM’s social media sites by individuals on the ground and members of the intelligence community would provide insight into individuals most at risk of radicalization or those who had been radicalized. Mandatory training from the Department of Education could help teachers recognize the signs of extremism amongst the demographics of those most at risk – 13–17-year-old males. In Breaking Hate, Christian Picciolini identifies several trends among individuals most at risk to radicalize, such as unresolved emotional, psychological, or physical trauma combined with shame. However, many people undergo traumatic events in their life. What causes certain people to become radicalized is a combination of “potholes and an imperiled search for identity, community, and purpose (ICP).” Trained teachers are an integral part of this strategy because they can identify students who exhibit the signs that make them vulnerable to radicalization.

A coordinating structure led by the United States would need to tie all three levels of the structure together. The group would need to be able to discuss securely and quickly, when necessary, in order to adapt to changing threats. The joint task force mentioned above would meet on a regular basis, discuss current threats, prepare recommended talking points, and flag updates for Congress and the President. A communications plan could serve as this coordinating structure that would identify the most effective communication channels and guarantee success. Ultimately, a long-lasting CT strategy would require the United States to get to the root of the problem. It will take time to change institutions and cultures that allow extremist views. The United States must learn from how it successfully countered AQ to fight RIM (and other right-wing extremist organizations). A combination of laws, government resources, and international cooperation will be necessary.

An effective counter-messaging strategy would both decrease support for RIM and convince supporters and members to leave the organization, as well as reintegrate former radicals into society. A two-pronged approach of decreasing support and encouraging members to leave would ensure that fundraising decreases and the recruitment messages do not circulate as effectively. If the United States were to
pursue this approach, they should measure the number of attacks, number of RIM members, reach of counter-messaging content, and number of members who leave the organization. Similar to how individuals are radicalized, they are deradicalized through a strong ideology instead of behavior and actions; in the case of RIM, individuals may be deradicalized through an ideology based on a new sense of identity, empathy, and sympathy for others. Strong counter-messaging is critical in order to encourage those with extremist beliefs to defect, deradicalize, disengage, and then reintegrate into society.

Twenty years ago, the United States underestimated the rise of Islamic terrorism. It should not wait for the white supremacist equivalent of September 11, 2001. The United States needs to counter right-wing propaganda online as part of its CT strategy by using former white supremacists as messengers. “The US and its allies must take decisive action to challenge these toxic ideas and counter the operatives who embrace them,” said Ali Soufan, former FBI counterterrorism agent, and Ambassador Nathan Sales, former acting U.S. Under Secretary of State for Civilian Security, Democracy, and Human Rights. Defeating RIM will require a holistic CT approach, with resources dedicated to countering their online propaganda. This strategy will provide the best way to halt the number of members joining and provide opportunities for disengagement from the organization and ideology.

About the Author: Carley Berlin is a graduate student in Georgetown University’s Security Studies Program (SSP) with a concentration in US National Security Policy. She is a Senior Consultant at Deloitte and works in the Defense, Security, and Justice sectors.
3 “Terrorism in America After 9/11,” New America, accessed March 28, 2022, http://newamerica.org/international-security/reports/terrorism-in-america/. Data does not show how many people have been radicalized but have not acted violently.
4 “Terrorism in America After 9/11.”
9 Counter Extremism Project, “Russian Imperial Movement (RIM),” Counter Extremism Project, accessed April 5, 2022, https://www.counterextremism.com/threat/russian-imperial-movement-rim. Stanislav Anatolyevich Vorobyev said in January 2015, “Ukrainian nationalists are separatists. Ukrainian nationalism is an ideology used by the Bolsheviks against the Russian people… There is no Ukraine, there is New Russia [Novorosia]. Even the name ‘Ukraine’ is what the Poles called their extreme territories. The official name for this territory was Russian Voivodeship… Ukrainian nationalists are mainly young people born 23 years ago who are brainwashed.” Denis Vallullovich Gariyev said in January 2017, “We see Ukrainian-ness as rabies… A person is sick. Either quarantine, liquidation, or he’ll infect everyone.”
10 Stanford University, “Russian Imperial Movement.” RIM announced that two of its fighters were killed in combat in January 2020. Analysts believe that the number is likely higher than two.
11 Dunlop, “Aleksandr Dugin’s Foundations of Geopolitics.”
12 Dunlop.
13 Counter Extremism Project, “Russian Imperial Movement (RIM).”
14 Picciolini, Breaking Hate.
15 Bruce Hoffman, Inside Terrorism (Columbia University Press, 2017). The US did not designate IRA as a terrorist organization partially because it had strong diaspora support. Additional research is needed into the effect of Russian diaspora support on US policy toward RIM.
19 McCausland.
20 McCausland.
22 Foggett, Saltskog, and Clarke.
30 Stanford University, “Russian Imperial Movement.”
33 Counter Extremism Project, “Russian Imperial Movement (RIM).”
35 Stanford University, “Russian Imperial Movement.”
36 Stanford University.
39 Stanford University, “Russian Imperial Movement.”
40 “Inside The Russian Imperial Movement.”
42 Amy Sturm, “Class 12: Counterterrorism Toolkit.”
44 Foggett, Salskog, and Clarke, “How Are Putin’s Far-Right Fans in the West Reacting to His War?”
45 Stanford University, “Russian Imperial Movement.”
50 “Inside The Russian Imperial Movement.”
“Inside The Russian Imperial Movement.”


“Inside The Russian Imperial Movement.”

Carey, “Congress Members Call for Russia to Be Designated State Sponsor of Terrorism.”

“State Sponsors of Terrorism.” “State Sponsors of Terrorism” is a designation applied by the United States Department of State to countries which the Department alleges to have "repeatedly provided support for acts of international terrorism”. Inclusion on the list imposes strict unilateral sanctions.


Peter R. Neumann, “Options and Strategies for Countering Online Radicalization in the United States,” Studies in Conflict & Terrorism 36, no. 6 (June 1, 2013): 431–59, https://doi.org/10.1080/1057610X.2013.784568. North Korea, Cuba, Syria, and Iran are the only countries on the list.

“Annex H To the National Military Strategic Plan for the War on Terrorism,” March 4, 2005.


Bach-Lombardo.

Bach-Lombardo.


Picciolini, Breaking Hate.

Picciolini.

Picciolini.

Picciolini.


Soufan and Sales, “Opinion | One of the Worst Ways Putin Is Gaslighting the World on Ukraine.”
Trafficking of Women in Bangladesh: An Analysis from a Feminist Human-security Framework

Shuva Das and Leo S.F. Lin

This study aims to conduct a qualitative exploratory single-case study on the trafficking of women in Bangladesh. In current literature, much attention has been given to state-centric security with scholars tending to place less emphasis on the human trafficking issue from a feminist human security perspective. This study provides an empirical analysis using a feminist human security framework that explores what types of violence Bangladeshi women experience when trafficked, and critically assesses the roles of different factors and actors in the trafficking process. It employs a qualitative data collection technique from secondary literature and in-depth interviews with 24 female respondents from the Madaripur district of Bangladesh, who are all trafficking victims. The study reveals that both state and non-state actors commit direct and indirect forms of violence in the trafficking of women in Bangladesh. It also demonstrates how supply-side and demand-side factors maintain a nexus and trigger the trafficking of Bangladeshi women. Finally, it contributes to the feminist literature by developing a feminist human security analytical framework to understand and explain the trafficking of women in a male-dominated society.

Introduction

Human trafficking is envisaged as modern slavery and, as a form of organized crime, it has been an unending human security concern in modern human civilization. The South Asian region is a vast source of human trafficking in general while Bangladesh, though a small country, constitutes an enormous share of trafficking victims in the region. More than 150,000 South Asians fall victim to human trafficking each year, making South Asian states, including Bangladesh, profoundly worried. Around 32,000 Bangladeshis, of whom roughly 20,000 are women, are trafficked each year. These victims are forced to engage in the sex industry, forced into bonded labor, sold as domestic servants, or traded in the human-organ market. Given the situation of human trafficking in Bangladesh, the 2020 Trafficking in Persons Report of the U.S. Department of State listed the country in the Tier 2 category. Ranking a country in this category indicates that its government does not act in complete accordance with the standards of the Trafficking Victims Protection Act of 2000, but is seriously attempting to comply with its standards.

Few research articles regarding human trafficking in Bangladesh have emerged over the years. Rahman argues that trafficking is a grave security concern for Bangladesh due to its uncontrollable nature and its proximity to transnational crimes and illegal migrations. Rahman and Ruhi explore the factors responsible for causing trafficking in persons given the socio-political and economic landscapes of the country.

In survey research, Abdul, Joarder, and Miller highlight the experiences of trafficked migrants who returned to Bangladesh after working in foreign countries. Most respondents regardless of gender pointed out that their required travel documents were forged and that they endured inhospitable working conditions, while almost every female migrant experienced sexual abuse. Likewise, Paul and Hasnath portray what cruel experiences trafficked persons encounter in foreign countries. They identify the weakness and discrepancies in responses against trafficking at the national level of Bangladesh and the regional level of South Asia.
However, a crucial yet unexplored area of research is the types of violence that Bangladeshi women experience during trafficking. Thus, this study aims to apply a feminist human-security framework to their experiences. Using the feminist human-security framework, it also explores the roles of different actors and factors in the trafficking of Bangladeshi women.

Before proceeding to the central discussion, it is crucial to understand human trafficking and to clarify its relationship with gender and smuggling. Human trafficking lacks a satisfying universal definition, with differences between national and international definitions creating barriers to coordinated and effective responses. The UN Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children (UN TIP Protocol) provides a broad definition of human trafficking: “… the recruitment, transportation, transfer, harboring or receipt of persons, by means of the threat or use of force or other forms of coercion… for the purpose of exploitation. Exploitation shall include… sexual exploitation, forced labor or services, slavery or practices similar to slavery, servitude or the removal of organs.”

13 The UN Protocol’s definition emphasizes three particular aspects: sexual and labor exploitation and the removal of organs. However, the removal of organs is not found in some countries’ own definitions of human trafficking. For example, the government of the People’s Republic of Bangladesh enacted the Prevention and Suppression of Human Trafficking Act in 2012 without pointing out the removal of organs. As such, the Act defines human trafficking as the trading and deporting of a deceived person inside or outside the country for the purpose of sexual and labor exploitation or other forms of exploitation.

14 The UN Protocol and Bangladesh’s 2012 Act deem trafficking as a crime and point out that exploitation is its perennial character. Likewise, Watson and Silkston posit that trafficking implies the transfer of people by deceptive means for profitable exploitation.

15 Gender is a key factor in exploitation during trafficking, which can be a form of gender-based violence, comprising any acts of verbal, physical, psychological, and sexual abuse. According to a report from the United Nations Office on Drugs and Crime, women constitute 70 percent of victims of human trafficking while men make up 30 percent internationally. Indeed, women become easy prey to traffickers due to gender-based discrimination in education, wages and employment, marital abandonment, poverty, and domestic violence in society.

Human trafficking should not be confused with human smuggling. The UN Protocol against the Smuggling of Migrants by Land, Sea, and Air defines the latter as the illegal yet voluntary entry of a person with the assistance of smugglers into a foreign country where he/she is not a citizen. The key difference between trafficking and smuggling is that the former is based on force while the latter is based on consent. Thus, trafficking is a crime against a person whereas smuggling can be a crime against a state. Smuggling, nonetheless, often turns into trafficking when a smuggled person is forcefully exploited for labor or sex trade. Therefore, the UN needs to provide an unequivocal definition of human trafficking because an explicit distinction between trafficking and smuggling will support compatible assistance programs and effective judicial processes in a country.

The study proceeds as follows. First, it discusses the analytical framework of feminist human security with cohesive indicators. Second, it provides an overview of the methodology. Third, it explores the factors triggering the trafficking of Bangladeshi women. Fourth, it investigates the roles of non-state actors in the trafficking of women in Bangladesh.
it critically examines the roles of Bangladesh’s government in preventing the trafficking of the country’s women. Finally, it recapitulates the arguments made in the study and provides recommendations to improve the human security of Bangladeshi women.

Analytical Framework: A Feminist Human Security Perspective

Over the past decades, the concept of human security has continued to be developed by international organizations, scholars, and practitioners. The 1994 Human Development Report of the United Nations Development Programme introduced the concept of human security as the safety of people from chronic threats and protection from harmful interruptions in everyday life. The report has pointed out security threats stemming from food, environment, economy, and health, and threats impacting our personal (physical), community, and political security. In 2012, the UN General Assembly adopted Resolution 66/290, which states that human security implies the right of every person to live with dignity and “freedom from fear and want”, and equal opportunities to enjoy his/her rights and realize his/her full potential as a human being.

Nonetheless, there are three camps in human security. The first camp considers human security as a basic individual right to life, liberty, and the pursuit of happiness, and that the government of each country has an international obligation to protect these rights. The second camp is humanitarian, emphasizing international institutional and legal efforts to better international laws and regulations, particularly concerning war crimes and genocides. The third camp views the human security issue from a global perspective. Scholars of this perspective argue that globalization, the global economy, and the global health environment impact the security of individuals.

In human security scholarship, gender perspectives have been underemphasized while pundits of traditional security have predominantly centered their scholarship on security threats to the state, which mainly derive from foreign states. Muthien posits that traditional security generally focuses on military war, thereby ignoring the everyday security needs and concerns of women.

The feminist perspective is crucial in human security since women are victims of different types of crime and violence compared to men. Feminists contend that from a normative perspective, human trafficking is above all a violation of human rights. They also believe that the trafficking of women must be understood in light of a gendered social order cultivating an uneven power relationship between men and women.

From the human security perspective, people are the target of violence in general whereas, from the feminist perspective, women are the primary targets of violence since they are more vulnerable given their material and political positions in society. McKay divides violence into its direct and indirect forms. Direct violence implies physical violence to individuals. Indirect violence, which is often intractable, is embedded in social structures and normalized by institutions of societies and states.

Based on the above discussion, this study falls into the third camp of human security and argues that the safety of individuals is the key to global security. To better analyze the case of Bangladesh, the research employs a feminist human security perspective with the modification of the direct and indirect violence thesis provided by McKay. The analytical framework is summarized in Table 1 below.
Table 1: Feminist human security analytical framework (Source: Based on data compiled by the authors)

<table>
<thead>
<tr>
<th>Actors</th>
<th>Direct (physical) violence</th>
<th>Indirect (structural) violence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-state actors</td>
<td>Type 1</td>
<td>Type 2</td>
</tr>
<tr>
<td>Direct violence (for example, harassment, injury, forced labor, forced organ harvesting, rape, and murder) from non-state actors such as organized crime groups</td>
<td>Indirect violence (for example, poor health environment, lack of food, water, and housing, forced marriage) caused by non-state actors such as organized crime groups</td>
<td></td>
</tr>
<tr>
<td>State actors</td>
<td>Type 3</td>
<td>Type 4</td>
</tr>
<tr>
<td>Direct violence (for example, harassment, injury, rape, and physical assaults) from state actors such as police officers, military personnel, and government workers</td>
<td>Indirect violence (for example, lack of access to education, health care, religious service, political rights, and gender justice) caused by state actors such as decision-making government authority within political and economic systems</td>
<td></td>
</tr>
</tbody>
</table>

To operationalize the variables of the research, indicators are designed to capture the concept in the analytical framework. Direct (physical) violence refers to the acts of harming the victims physically in various forms (for example, harassment, injury, rape, murder, etc.). Indirect (structural) violence refers to the systemic unfavorable situations in the victims’ living areas, including lack of access to education, food and water, housing, health care, religious service, political rights, and gender justice, forced marriage, etc. Non-state actors refer to any individuals or groups that are not part of or affiliated with Bangladesh’s government. State actors refer to any individuals or groups that are part of or affiliated with Bangladesh’s government.

Methodology

Data Collection

This research is based on a qualitative exploratory single-case study on the trafficking of women in Bangladesh and uses both primary and secondary data. The case study method has been applied to understand the types of violence experienced by the trafficked women of Bangladesh and the roles of different actors and factors in trafficking. There are myriad sources of data collection in a qualitative case study that expose multifaceted aspects of a selected case.¹⁵

Primary data was collected through in-depth interviews with 24 female participants aged between 23 and 41 who were previously trafficked to India, Pakistan, or Middle Eastern countries. An open-ended interview questionnaire was used to explore and understand the experiences of the trafficked victims. Before the interview, the consent of each interviewee was taken to record the conversation. For the study, we communicated with the Program Officer of the Bangladesh Women’s Foundation. She provided us with important information about some potential respondents. We interviewed nine of them and then employed the snowball sampling technique to select the remaining participants. Snowball sampling is a non-probability sampling technique where research subjects help...
researchers to reach and recruit other subjects for a study.

Madaripur (an administrative district of Bangladesh) was selected as the data collection site. Interviews were conducted in four Upazilas (sub-districts) of Madaripur – Madaripur Sadar, Shibchar, Kalkini, and Rajoir, from each of which 6 participants were selected. According to Bangladesh’s Bureau of Manpower Employment and Training (BMET), approximately 105,593 people from Madaripur migrated abroad as laborers from 2005 to 2017, placing it in the top 20 migrant-sending districts of Bangladesh. Madaripur is also listed among the top ten districts of the country in sending women abroad. Human trafficking in the district is also growing rapidly.

To support the aims of the study, secondary data were also collected from the United Nations report, the U.S. Trafficking in Persons Report, news and NGO reports, government publications, books, journals, and magazines.

Data Analysis

Thematic analysis was conducted to analyze the interview data. It consists of a list of themes a researcher anticipates exploring from the collected data. In doing so, data preparing and organizing, data coding, generating data themes, interrelating themes, and interpreting the meaning of themes were cautiously carried out to make the meaning of the data more comprehensible to readers.

Recorded interviews were first transcribed into the native language (Bangla) of the respondents. Following this, data were translated into English and then coded. The coding of qualitative data generates systematic and in-depth analysis and assists in revealing the underlying meaning of every qualitative response. Open coding of suitable and crucial words, phrases, sentences, and sections was carried out in the written transcripts of the recorded data to identify themes for analysis. The themes were labeled and then interpreted to generate the major results of the study. Although all the respondents of the study underwent different experiences, their narratives corresponded with thematic constructions.

Findings and Discussion

Factors Triggering the Trafficking of Bangladeshi Women

Human trafficking is an intractable crime posing serious challenges for Bangladesh’s government to address. If actual factors triggering trafficking can be identified, they can be tackled effectively and efficiently. Factors are divided into demand and supply sides in Table 2. The demand side mainly reflects the external dimension of the trafficking of women on a global level, while the supply side indicates the internal dimension of trafficking in Bangladesh.

<table>
<thead>
<tr>
<th>Factor category</th>
<th>Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Demand side</td>
<td>Booming sex industry, forced labor, increasing need for women in domestic work, and human organ business</td>
</tr>
<tr>
<td>Supply side</td>
<td>Poverty, unemployment, patriarchal social norms, domestic violence, economic bondage, lack of education and advanced work skill, and natural calamities</td>
</tr>
</tbody>
</table>

Table 2. The demand-supply factors for the trafficking of Bangladeshi women (Source: Based on data compiled by the authors)

On the demand side, globalization – which promotes a free market economy and eases the movement of people, goods, technology, and ideas across state borders – plays a prominent role in trafficking.
Women have been commoditized in the labor and sex markets of the capitalist global economy where they are purchased and put on sale and resale as modern slaves as long as they have commercial productivity. U.S. Congressman Chris Smith contends that the market demand for prostitution is a major reason behind the trafficking of women. As stated earlier, around 20,000 women from Bangladesh are trafficked around the world annually – namely to India and Pakistan, and Middle Eastern countries – and many of them become the victims of sex trafficking. The trafficked women are also often subjected to forced labor without due pay in underground mining, narcotic farming or production, and work in hazardous environments, which severely damage their health and reduce their longevity. Any kind of forced labor violates the bodily autonomy of a person and makes him/her disempowered.

The interviews revealed that all of the participants were lured with the promise of better jobs and higher living standards by the traffickers, but they were forced into prostitution, domestic servitude, or agricultural or mining work without due salary. This can be seen in the following quote from Interviewee no. 23. “I was looking for a job after my husband died of cancer… My brother-in-law offered me a restaurant chef job in Delhi, India, and I accepted it. He handed over me along with some girls to two unfamiliar men… We were taken to Delhi where I was segregated from the other and was confined for forced prostitution. With the help of a sex client, I escaped and was rescued by a women’s rights organization that helped me to return to Bangladesh…” (Interviewee no. 23, personal communication, November 26, 2021).

The excerpt reveals how the demand for sexual services results in the trafficking of individuals like her. Moreover, a study conducted by Ovibashi Karmi Unnayan Program, a Bangladesh-based migration and advocacy research organization, has found that 86 percent of the study’s subjects (110 trafficked women) who were able to return to Bangladesh did not get their full remuneration, 61 percent experienced physical tortures, 24 percent did not get sufficient daily foods, and 14 percent underwent sexual abuses in their forced labor works. When trafficked women lose their productive value of either labor or sex they are often traded to organ business groups for kidneys, eyes, livers, and other organs. Although there is inadequate data regarding this issue, it cannot be ruled out as the trafficked victims leave no reliable evidence of their death after organ removals. The UN Protocol clearly states that exploitation in trafficking includes the removal of organs of trafficked persons. According to the World Health Organization, around 10,000 underground market operations in human organs occur annually. The human organ business involving human trafficking is also a lucrative part of the black market. In 2017, Pakistan’s police raided a private clinic and arrested five medical personnel preparing to perform organ harvesting operations on three people, among whom one was a trafficked Bangladeshi woman, and the rest were Pakistani men.

On the supply side, factors need to be understood because a combination of two or more factors makes Bangladeshi women susceptible to traffickers. Compared to men, women in Bangladesh are unprivileged in accessing economic, political, social, and educational resources, causing them to be more vulnerable to traffickers. In particular, the age-old hegemonic patriarchal norms of Bangladesh encourage them to solely take on the roles of reproduction and homemaking and discourage them from engaging in public life. Indeed, the 2018 Gender Inequality Index ranked Bangladesh 129th out of 162 countries. The following excerpt from Interviewee no. 10 is pertinent to mention here. “…I was convinced by traffickers to go to India for better income because I had no alternative. My family stopped my education and made my early
marriage… After my divorce, my family did not accept me congenially…” (Interviewee no. 10, personal communication, November 28, 2021).

As of 2020, women in Bangladesh accounted for around 31 percent of the entire workforce, demonstrating not just discriminatory recruitment and gender preference in the country’s employment system, but also their lack of education and skills. Apart from this, a survey from UNICEF on trafficked women ranging from ages 17-32 in ten villages in Bangladesh found that 95 percent of this age group was illiterate.

Further, around 21 percent of people in Bangladesh live below the national poverty line, according to the 2019 estimation of the Asian Development Bank. Poverty mostly harms women compared to men and thereby it has become feminized. To make matters worse, when women become widowed, attempt marital separation due to domestic violence, or experience marital abandonment, many of them confront serious economic hardships. To improve their financial capacity, traffickers or loan-giving organizations provide them with debt that locks them into economic bondage. Traffickers attempt to exploit this condition of women and persuade them to go abroad so that they can pay off their debt and become financially prosperous. The following verbatim from Interviewee no. 12 can explain it better.

“My marriage with my husband did not last more than half a year because of his violent behavior. After the divorce, I was not well-accepted by my parents… I failed to manage to get a job due to my lack of education and skills. My paternal uncle proposed me a gardener job in Saudi Arabia… Reaching Saudi Arabia, I ended up as a domestic servant to a cruel house owner. I underwent a severe physical illness there and was admitted in a hospital from where I escaped… I returned to Bangladesh in 2019 …” (Interviewee no. 12, personal communication, December 7, 2021)

This excerpt highlights how domestic violence can lead to divorce and economic hardship if they do not have support, education, and proper job skills, the lack of which can make them easy prey to traffickers.

In addition, Bangladesh is one of the most climate-vulnerable countries in the world due to its disadvantageous geographical location and dense population. In 2016, a study by the Bangladesh Institute of Social Research Trust found that the country’s female population is more vulnerable to natural disasters, and they constitute around 70 percent of the total displaced people of Bangladesh. During natural disasters, the suffering of girls and women is compounded if they belong to a lower socio-economic group, especially in the context of the Global South. It can be found in the words of Interviewee no. 5.

“In 2007 when Cyclone Sidr struck southern Bangladesh, our family became destitute… A well-known neighbor convinced my older father to migrate my sister and me in Oman with a promise of beauty parlor jobs. After taken in Oman, we were, however, forced into domestic servitudes in two different houses. Though I escaped the inhuman treatment of my house owner and came back in Bangladesh with the help of Bangladesh’s embassy in Oman in 2014, the whereabouts of my sister are still unknown to me…” (Interviewee no. 5, personal communication, November 14, 2021)

The above case articulates that when a family falls into serious economic troubles and concomitantly does not have males able to earn an income, females can be encouraged to seek outside employment. And disaster-affected women undergo more economic troubles and often need to earn for their families, thereby becoming extremely susceptible to traffickers.

This section has clarified that a combination of factors from the demand and supply sides causes the trafficking of
women in Bangladesh. The following section will look at the role of non-state actors in trafficking Bangladeshi women.

The Role of Non-state Actors in Trafficking Bangladeshi Women

Human trafficking is an organized crime, and a trafficking network is business-oriented by nature since everything is calculated with the goal of profit maximization. Richmond argues that the principal cause of trafficking is traffickers who always seek to exploit vulnerable situations of people for financial gain.

The process of trafficking is complicated and sophisticated. As shown in Figure 1 below, the trafficking of women can take place in two ways in Bangladesh.

![Figure 1: Two-way trafficking of girls and women (Source: Based on field data and data compiled by the authors)](image)

On the one hand, brokers of traffickers start the initial process of trafficking. The brokers are familiar to the would-be trafficked women, and their familiarity gives them access to their targets. The brokers look for women who are socially and economically disadvantaged in society and who are then offered jobs abroad with lucrative salaries. After they are convinced to accept the offer, the brokers take them to the traffickers who, in turn, transfer them to the trafficking or criminal syndicate.

On the other hand, traffickers can play a direct role in the first stage of luring women into trafficking, and so do not employ brokers in this context. Traffickers directly traffic women and then transfer them to the trafficking/criminal syndicate. Since traffickers are not always familiar to female victims, they might employ several strategies to appear credible and accessible to their targets.

First, some traffickers have weaponized marriage for trafficking poor girls after marrying them. For example, Monirul Islam Monir married 75 poor girls and individually took his wives to India where he sold them into brothels. The Indian police have recently arrested him. Furthermore, nearly 450 tribal girls from remote areas of Bangladesh were trafficked in China in the last 5 years through marriage traps. A police investigation found that 10 Bangladeshi matrimonial organizations were involved in the trafficking, offering marriage proposals to the tribal girls on the behalf of Chinese male citizens. The Chinese men married those girls who accepted the proposals, took the new brides into China, and sold them to sex traders.

Second, traffickers use the social media platform TikTok to lure younger girls belonging to lower socio-economic groups in Bangladesh. They maintain Facebook groups that add young female TikTokers who are then offered well-paid jobs and opportunities to be TikTok stars in India. Indeed, the use of TikTok in trafficking girls has come into the limelight in 2021, when an investigation of a video clip of an alleged sexual assault of a Bangladeshi girl in India linked the incident to a transnational trafficking gang. Through the use of
TikTok, over 1,500 girls have been trafficked from Bangladesh to India in recent years.63

Finally, traffickers operate dance clubs that particularly encourage lower socio-economic girls to enroll. They offer girls jobs in entertainment industries in foreign countries.64 For instance, Bangladesh’s Criminal Investigation Department detained award-winning film choreographer Ivan Shahriar Sohag who owns two dance clubs which, in collaboration with business tycoon Azam Khan, is accused of trafficking 1,000 Bangladeshi women to Dubai.65 In this context, the experience of Interviewee no. 18 can provide clear insight. “I wanted to be a dancer celebrity and got admitted in a Dhaka-based dance club… I felt ecstatic when I was offered by my dance master that I would join in a Dubai dance club… On reaching Dubai, I found that I was cheated. I was forced to prostitution for 3 months in a hotel. Then, the traffickers sent me back to my country…” (Interviewee no. 18, personal communication, November 5, 2021).

In both methods of trafficking (Figure 1), though the trafficking/criminal syndicate is placed on the top, traffickers or their brokers are the key agents who are familiar to the would-be trafficked girls/women and who initiate the process of trafficking. However, though law enforcement agencies, politicians, and lawmakers are not directly part of the process of trafficking, they are highly crucial for its success.66 The traffickers receive strategic support from those who have an influence on the legal and administrative system of Bangladesh.67 In this regard, the trafficking recruitment system is not completely independent; its power stems from outside the trafficking ring. In each of the methods of trafficking, familiarity appears vital because it generates credibility of the traffickers and their brokers to the would-be trafficked girls/women of conservative Bangladesh.

Table 3 shows the relationship between trafficked women and members of trafficking gangs.

<table>
<thead>
<tr>
<th>Relationship</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Husband</td>
<td>01</td>
</tr>
<tr>
<td>Family relatives</td>
<td>11</td>
</tr>
<tr>
<td>Relatives of family relatives</td>
<td>07</td>
</tr>
<tr>
<td>Community neighbors</td>
<td>05</td>
</tr>
<tr>
<td>Total</td>
<td>24</td>
</tr>
</tbody>
</table>

Table 3. Relationship between the respondents (trafficked women) and members of trafficking gang (Source: Based on field data)

Among the 24 respondents of the study, the most frequent brokers were their family relatives (11) who were almost numerically equal to the rest of the combined number of husband (01), relatives of family relatives (07), and community neighbors (05).

Trafficked women undergo different forms of violence that are closely associated with trafficking from the very beginning. It was found that all of the participants of the study experienced direct and indirect violence. In the context of direct violence, sexual exploitation and physical coercion are highly common.68 If the women are immediately sold into brothels, they are often forced to take sedative drugs to break their physical resistance to client sex or sexual violence.69 In terms of indirect violence, the trafficked women experience a filthy environment during the transition period of their travel and this continues when they are sold to pimps or forced labor syndicates. They do not get adequate food, healthy shelter for survival, or health facilities.70 Direct and indirect violence is intertwined because when a woman undergoes direct violence such as physical
coercion or sexual exploitation, she concomitantly experiences indirect violence like an unhygienic environment, insufficient food, deprivation of health facilities, and forced marriage. An excerpt from Interviewee no. 26 is vital to mention here. “I experienced psychological fear and sexual molestation and got insufficient food and dirty house during my journey into Mumbai and after I was sold to pimps there” (Interviewee no. 26, personal communication, November 5, 2021).

This section has discussed that trafficking rings are complex and transnationally organized, and traffickers use the strategy of familiarity-induced credibility. Trafficked women are always subject to direct and indirect violence. The next parts of the study will examine whether or not the role of Bangladesh’s government in preventing the trafficking of women is adequate and effective.

The Role of Bangladesh’s Government in Preventing the Trafficking of Women

Human trafficking has posed a significant challenge to the government of Bangladesh for decades. Its response is so far insufficient and ineffective in several contexts, which gives traffickers needed opportunities to continue their illicit network in the country.

Per Figure 2, Bangladesh was placed into the Tier-2 category from 2013 to 2016. In the next three consecutive years, its ranking position fell to the Tier-2 Watch List category while in 2020 the country was able to reinstate its previous Tier-2 ranking position.71 This implies that the government of Bangladesh is not fully following the prescribed standards to prevent human trafficking, though it is attempting to take important steps against its expansion.

To critically examine the government’s role in fighting against female trafficking, a critical look into the existing laws, judicial system, law enforcement agencies, and politicians of Bangladesh can provide some vital insights. The government of Bangladesh enacted the Prevention and Suppression of Human Trafficking Act in 2012, which posits that human trafficking is the trading and deporting of a deceived person inside or outside Bangladesh for the purpose of sexual and labor exploitation or other forms of exploitation.73 As prescribed in the 2012 Act, the government set up anti-trafficking tribunals in all administrative divisions of Bangladesh except Mymensingh in 2020 to prosecute human trafficking cases. These special tribunals have replaced the Women Violence Protection Tribunal that had previously managed trafficking cases of women and drawn criticism for not having expert prosecutors on such criminal cases.74

Undeniably, the 2012 human trafficking Act of Bangladesh is a sign of determination by the country to fight against traffickers, but the limits and ineffectiveness of the judicial system could not translate the government’s objectives into reality. Criminalizing the trafficking of a person for sex, labor, or other exploitative purposes, the 2012 Act penalizes criminals with a five-year sentence and a fine of not less than $595.75 The Act’s increased sentences are commendable, but the implementation of the provisions of the Act is sluggish. The experience of Interviewee no. 19 is pertinent to mention here.
“With the persuasion of a local politician, I went into Qatar in 2017 to change my destiny after my husband abandoned me… I was taken there for prostitution… I escaped and came into Bangladesh in 2018 with the help of an international NGO… I filed a case in court against the local politician for compensation. The accused is moving freely and there is no progress in the case. I think that he has bribed the police…”
(Interviewee no. 19, personal communication, November 24, 2021).

The above excerpt reveals a negative picture of the country's legal-administrative system. She was trafficked due to her lower socio-economic background and she is now deprived of justice for the same reason.

Moreover, under the 2012 Act, the government of Bangladesh had 592 recorded cases with 1,324 suspects until 2019, but the courts had not yet shown how many cases were prosecuted or continued from the previous periods.76

Besides, there are not enough investigations into the corrupt immigration agencies: just 14 in 2017 and 15 in 2018, though the country has thousands of such agencies.77 Now, a question arises over the country’s legal system and whether it has been hamstrung by the influence of traffickers or their political bedfellows.

In fighting trafficking, law enforcement agencies such as the police, Border Guard Bangladesh (BGB), and Bangladesh Coast Guard (BCG) play important roles. The government of Bangladesh has started training programs for police, BGB, and BCG with advanced technology. Law enforcement does have records of arresting some traffickers and rescuing trafficked women. Figure 3 shows the number of arrests of suspected traffickers in each month of 2021.

![Figure 3. The number of arrestees of traffickers/suspected traffickers](image)

As seen in Figure 3, June and December were the peak months of arrests with 12 each while no suspected traffickers were detained in February, April, July, or September of 2021. It is remarkable to note that around half (23) of the total arrests in that year happened from October to December. There was a single arrest each in March and November whereas there were 4 and 3 arrests in May and August respectively.

It is important to note that the 2019 Human Trafficking Report of the U.S. Department of State revealed that there were a number of recorded cases where some police, BGB, and BCG personnel took bribes or sexual favors during the process of transnational trafficking of people, mainly women.79

For instance, two BGB members seized trafficked girls from the Bangladesh-India border and raped them.80 Though the BGB commanding officer claimed this as a rumor, the two rapists have not yet faced any legal procedure, and police did not permit NGO personnel to inspect the victims in the hospital.81 This particular case demonstrates that if law enforcement agencies maintain a transparent standing regarding the issue, their image would be tarnished by a third party (in this case, an NGO). These loopholes inside law enforcement agencies provide the needed
incentive and permission for trafficking gangs.

Furthermore, the 2020 Trafficking in Persons Report of the U.S. Department of State mentioned the direct engagements of some politicians and lawmakers in human trafficking. A glaring example can be drawn from Mohammad Shahid Islam, a Bangladeshi Parliamentarian, who has been accused of money laundering and human trafficking including women through his migration agency, and is now in custody in Kuwait.

This section has demonstrated that the government of Bangladesh has undertaken several crucial steps in fighting the trafficking of women; however, the ineffectiveness and inefficiency of the legal and administrative systems of the country could not deter the growth of trafficking networks. It has also pointed out that the government commits direct and indirect violence against women, whether trafficked or not.

Conclusion

The study has examined the trafficking of Bangladeshi women under a feminist human-security framework. It has found a nexus between supply and demand side factors triggering women’s trafficking from Bangladesh. On the supply side, trafficking in the context of Bangladesh is significantly gendered because of its gendered socio-economic practices, which persistently generate female trafficking victims. On the demand side, globalization has accelerated the trafficking of women because of the diverse needs of the global economic market, such as the booming sex industry, forced labor, and the human organ business. The combination of the supply and demand sides has been an issue of concern because as long as this remains intact, the fight against trafficking will not reach a desired end.

Moreover, the study has investigated the role of non-state actors in the trafficking of Bangladeshi women. Non-state actors (trafficking gang members) commit direct and indirect violence against trafficked women and traffickers to employ the strategy of familiarity-induced credibility to trap women in trafficking. Trafficking of women is conducted in two important ways: from brokers to traffickers to a trafficking/criminal syndicate; and from traffickers to a trafficking/criminal syndicate.

Furthermore, the study has scrutinized the role of Bangladesh’s government in preventing the trafficking of women. It has shown that Bangladesh’s government commits indirect violence in social, political, and economic domains, which can make an underprivileged or poor woman susceptible to traffickers. Law enforcement agencies of Bangladesh’s government often also commit direct violence against women during and after trafficking. The role of Bangladesh’s government is not adequate to prevent the trafficking of women due to its ineffective and inefficient legal and administrative system, notwithstanding some significant improvements in recent years. Also, it appears that the basic principle of the politics-administration paradigm in state affairs is absent in Bangladesh since there is no clear segregation between its political and administrative systems.

Considering the overall findings of the study, it makes eight recommendations for Bangladesh to improve the human security of its women:

1. Making the country’s legal system fairer and speedier and promptly yet carefully handling the backlog of trafficking cases;
2. Maintaining strong monitoring of immigration agencies in the country;
3. Strengthening the cyber-policing of Bangladesh’s police force to halt and identify online and technology-facilitated trafficking.
4. Beefing up security in the country’s transit points where trafficking is known to occur;
5. Strengthening the country’s cooperation at regional and global levels in fighting human trafficking;
6. Enhancing the access of women, particularly vulnerable ones, to education, healthcare, politics, and public religious service to reduce structural violence against them;
7. Integrating more women into the country’s economy; and
8. Raising awareness among women to combat trafficking through television, social media, advertising, and awareness sessions.

Making these changes would improve the security of the women of Bangladesh.

About the Authors:
Shuva Das has experience working as a Research Associate at the Bangladesh Institute of Social Research (BISR) Trust, Bangladesh, and as the Editor-in-Chief at the Atlas Institute for International Affairs, UK. He obtained his BSS and MSS degrees in International Relations from Bangabandhu Sheikh Mujibur Rahman Science and Technology University, Gopalganj, Bangladesh. Email: shuvadasbsmrstu@gmail.com
Leo S.F. Lin is currently an Adjunct Assistant Professor at the Department of Criminal Justice, Ming-Chuan University, Taiwan. He is a former affiliate lecturer at the School of Social & Political Sciences, University of Glasgow, UK. He obtained his Ph.D. degree from the School of Social Science and Global Studies, the University of Southern Mississippi, USA. Email: lin.leonidas@gmail.com.
29 Watson and Silkstone, “Human Trafficking.”
32 Ibid.
33 Ibid.
34 McKay, ‘Women, human security’.
39 M. Q. Patton, Qualitative research and evaluation methods (California, USA: Sage Publications, Inc., 2015).
40 Ibid.
43 Rahman, “Human Trafficking”.


S. Nasrin, Nari Pachar: Pacharkarider Voyongkor Opokousol o Protirodher Khanti (“Trafficking of Women: Traffickers’ terrible tactics and lack of Resistance”), DW, October 8, 2021, https://www.dw.com/bn/%E0%A6%A8%E0%A6%81%E0%A6%B0%E0%A6%81%E0%A6%97%E0%A6%A8/E0%A6%95%E0%A7%8D%E0%A6%A8%


Hardening the Shield Against North Korea’s “All-Purpose Sword”: An Evolving North Korean Cyber Threat and Its Policy Responses

Jie Gao

North Korea’s cyber warfare is an evolving security threat to the United States, its allies, and the international community. Pyongyang’s advancement in cyber weapons complements its broader strategy of creating an asymmetrical advantage vis-à-vis the U.S.-ROK alliance and is rooted in its guerrilla tradition. Cyber tools are also attractive to the regime because of their cost-effectiveness and low risks of retaliation. Given these motivations and the militarism in North Korean politics, cyber capabilities will continue to receive substantial investments from Pyongyang. This paper proposes four policy recommendations to deter North Korea’s cyber capabilities build-up: 1) establish a cyber defense and cyber deterrence mechanism in the U.S.-ROK alliance, 2) facilitate international cooperation, 3) strengthen public-private partnership, and 4) design a comprehensive government strategy.

Introduction

North Korea often makes news headlines for its use of high-profile nuclear weapons and missile tests. However, the regime also leverages threatening unconventional force through its cyber warriors. The current leader Kim Jong Un himself has acknowledged the significance of cyber warfare by equating it with nuclear weapons and referring to it as an “all-purpose sword” (만능의 보검).

1 In recent years, North Korea has demonstrated increasing frequency and improved sophistication of its government-sponsored cyber operations. These capabilities will continue to help North Korea evade sanctions, collect sensitive information, disrupt the global economy, and threaten critical infrastructure if left unchecked.

This paper will provide a tailored overview of the North Korean cyber force and outline a strategy for the United States and South Korea to countermeasure this challenge. An analysis of North Korea’s political culture and security environment that drives it to invest in cyber capabilities will follow. Next, the paper will elaborate on the current state and future trajectory of the North Korean cyber threat by examining its cyber capabilities, objectives, and characteristics. The paper will conclude by offering four policy recommendations suggesting improvements in the U.S.-Republic of Korea (ROK) alliance cyber strategy, increased international cooperation, public-private partnership, and comprehensive U.S. government strategy to build a robust cyber defense and deterrence system against North Korean cyber threats.

Background of the North Korean Cyber Threat

Ruled by a repressive yet insecure regime, Pyongyang applies all instruments of state power to defend its rule. Its insecurity derived from the Korean War when the United States thwarted Kim Il Sung’s plan to unify the Korean Peninsula and almost subverted the newly established government in the 1950s. Thus, regime preservation has become the top priority for Kim and his successors, and developing a strong military force is deemed the most critical means to achieve that.

Against this backdrop, North Korean politics features militarism represented by Kim Jong Il’s Songun, or “military-first policy.” Under Songun, military advancement overrode the prosperity of the civilian economy and...
received disproportional resources from the government. The current leader Kim Jong Un has pledged to alleviate the country’s prolonged economic grievance under byungjin—a policy that aimed to balance nuclear programs and the civil economy. Nevertheless, North Korea still maintains a high level of military spending, which accounts for around 16% of its total government expenditure since 2012, according to the budget plans announced by its Supreme People’s Assembly (SPA).\(^2\) Furthermore, a North Korean defector, previously a computer science professor at North Korea’s Hamheung Computer Technology University, estimated that the regime allocates between 10% and 20% of its military budget on cyber operations.\(^3\) These numbers reflect the salience of the military in North Korea’s politics and provide clues to its evolving cyber capabilities despite economic hardship.

The establishment of the Korea Computer Center (KCC) in 1990, the primary agency responsible for information technology strategy, marks the beginning of North Korea’s cyber capabilities. Following the creation of KCC, Kim Jong Il, in 1995 and 1998, issued two directives for the Korean People’s Army (KPA) General Staff to pursue cyber capabilities.\(^4\) North Korea’s arms capabilities, fighter traditions, and the incentives cyber operations provide have all served as the foundation for North Korea's cyber strategy from its inception. First, North Korea’s weak conventional forces dictate its pursuit of asymmetric advantage. Although the KPA manages a troop twice larger than its South Korean counterparts, it lags far behind in equipment, capabilities, and skills.\(^5\) Thus, North Korea turned to new weapons, such as nuclear warheads and cyber tools, for asymmetric advantage to make up for its gap in conventional forces.

Second, the decentralized nature of cyber operations is consistent with North Korea’s guerilla tradition. North Korea’s founding leader, Kim Il Sung, established his reputation by fighting against Japanese colonialists as a guerrilla fighter in the 1930s. Kim Il Sung’s guerilla fellows later made up most of the North Korean political elites who led subversion campaigns against South Korea with guerrillas during the Cold War era. North Korean hackers today resemble guerilla fighters, as they sneak in the dark and ambush at the strategic weak points. These cyber guerrillas also seek financial resources through banditry and robbery, similar to their old comrades during the Korean War.\(^6\)

Third, cyber campaigns are associated with low risks and rarely receive retaliation. Since internet users enjoy a high level of anonymity, investigations to attribute cyber-attacks to a specific party are challenging. Anonymity enables North Korea to deny responsibility for its cyber operations while avoiding the risk of retaliation.\(^7\) Furthermore, as the international community primarily focuses on monitoring and sanctioning North Korea’s nuclear and missile programs, Pyongyang takes advantage of the international communities’ diverted attention and a lack of effective deterrents to conduct its cyber operations.\(^8\)

Fourth, cyber operations are cost-effective, with relatively low barriers to entry and potentially high yield. Although the initial stage of knowledge build-up and personnel training can be laborious, the maintenance and improvement of established cyber capabilities require fewer investments in materials and human resources than other forms of warfare. In addition, North Korean hackers can access technical know-how from open-source resources or illegal domains.\(^9\)
Despite these incentives, North Korea’s international isolation and economic backwardness have led the international community to underestimate the regime’s determinations and capabilities to develop cyber weapons. A 2009 U.S. National Intelligence Estimate downplayed the possibility of an imminent North Korean cyber threat. However, high-profile incidents such as the 2014 cyber-attack on Sony Pictures and the 2016 cyber theft from the Bangladesh Bank highlight the rapid evolution of North Korea’s cyber capabilities.

In sum, North Korea’s weak conventional force and guerrilla tradition, paired with cyber operations’ cost-effectiveness and low level of risks, suggests North Korea will continue to invest in strengthening its cyber capabilities, regardless of its dire economic situation.

**North Korean Cyber Threat Today and Its Future Trends**

Kim Jong Un has further strengthened North Korea’s emphasis on cyber warfare. Pyongyang has mainly leveraged cyber tools for disruption, espionage, and financial theft. While North Korean hackers have targeted a broad array of countries, South Korea and the United States are the most frequent targets. This section will introduce the structure of North Korea’s cyber-relevant organizations and analyze its cyber capabilities and future trends based on reported cases.

**Organization**

Figure 1 illustrates the structure of the North Korean government and military organizations relevant to cyber operations. According to an estimation by the South Korean government, the Reconnaissance General Bureau (RGB) is generally considered the center of North Korean cyber activity, with more than 6,000 full-time cyber experts. RGB directly reports to the State Affairs Commission (SAC), chaired by DPRK leader Kim Jong Un. Subordinated to the RGB, Bureau 121 is North Korea’s most significant cyber unit that conducts various cyberspace missions, including offensive and defensive cyber operations, cyber espionage, network exploitation, and cybercrime. In addition to the RGB, KPA’s General Staff Department (GSD) also engages in North Korea’s cyber operations with missions such as electronic warfare, information warfare, and psychological operations. The five GSD bureaus relevant to cyber operations include the Operations Bureau, Communications Bureau, Electronic Warfare Bureau, Command Automation Bureau, and the Enemy Collapse Sabotage Bureau.
Other identified North Korea-tied hacker groups include the Lazarus Group, the Bluenoroff Group, the Andariel Group, TEMP.Firework, and Kimsuky. In addition, Pyongyang’s Mirim College for Electronic Warfare Research reportedly serves as the training camp for future North Korean hackers.

Objectives

North Korea’s cyber operations mainly serve three objectives: causing disruption, conducting espionage, and generating revenue. First, North Korea has carried out cyberattacks on critical infrastructure to disrupt conventional operations and provoke its opponents – two traditions in North Korea’s strategic concepts. For example, in 2008, North Korea conducted large-scale cyberattacks against the South Korean government, which shut down 400 computers at the transition office of South Korea’s President Lee Myung-bak. Even before adopting cyber operations, North Korea’s special forces had attempted to disrupt the South Korean government, for example, with its “Blue House Raid” in 1968. North Korea’s cyber campaigns that jammed airline GPS signals to gain control of the aircraft are also new technology for an old strategy, as one may recall from the bombing of Korean Air Flight 858 in 1987. North Korean common cyberattack targets include media, banking systems, nuclear power plants, transportation networks, and government websites. By focusing on these targets, North Korean cyberattacks try to instill fear and inconvenience in general populations by crippling their infrastructure and services crucial to everyday lives.

Second, North Korea seeks to collect classified and sensitive information through cyber espionage. While South Korean and U.S. military departments and defense industries are the main targets of North
Korean hackers, academic institutions and pharmaceutical companies have also reported information theft tied to North Korea. In September 2016, North Korean hackers infiltrated the South Korea Defense Integrated Data Center and stole 234 gigabytes of classified military documents, including war plans. As previously mentioned, North Korea most likely relies on cyber espionage to overcome its lack of conventional military capability compared to its U.S. and South Korean targets. Pyongyang has also used cyber operations to collect information for its nuclear programs. In 2019, the North Korea-affiliated hack group Kimsuky broke into the network of a nuclear power plant in Kundakulam, India, for proprietary information on thorium-based reactors.

Third, cyber financial thefts are critical channels for North Korea to generate revenue. As its economy is under heavy sanctions imposed by the international community, particularly the United States, North Korea has been conducting cybercrimes to evade sanctions. One of the most notorious examples is the Bangladesh Bank cyber heist in February 2016. North Korean hackers managed to transfer nearly $81 million from the central bank of Bangladesh after compromising its computer network. A report by the United Nations Security Council (UNSC) estimates that North Korean hackers have stolen a cumulative $2 billion as of 2019. With illicit funds raised from cybercrimes, the Kim regime can continue to develop its nuclear and missile programs as well as provide private benefits to its political elites – both essential to its regime survival.

**Capabilities**

North Korean hackers have demonstrated increasing sophistication in their tactics. The aforementioned cyber theft of Bangladesh banks in 2016 is a representative case revealing Pyongyang’s cyber proficiencies. During this theft, North Korean hackers took advantage of the Society for Worldwide Interbank Financial Telecommunication (SWIFT)’s global network and inserted malware into a SWIFT terminal used by Bangladesh’s central bank. Noted by the FBI, such an operation “was the culmination of years of methodical preparation by a shadowy team of hackers and middlemen across Asia, operating with the support of the North Korean regime.”

In addition to attacking the weak points of the cyber systems, North Korean hackers are adept at social engineering to exploit human vulnerabilities. For example, North Korean cyber groups have previously sent fake job offers from defense contractors to defense and aerospace experts and retrieved classified information with the data-gathering implants in the emails. North Korean hackers disguised themselves with fictitious social media accounts on WhatsApp, Facebook, and LinkedIn and built their credibility through extensive dialogues via email and phone calls.

However, some observers have also pointed out the limitations of North Korea’s cyber capabilities. Josephine Wolff, an associate professor of cybersecurity policy, noted the WannaCry ransomware policy, noted the WannaCry ransomware launched in 2017 “was surprisingly unprofitable” for a financially-motivated campaign. While the ransomware had attacked around 200,000 computers in 150 countries and requested $300 for each device, estimates by a cybersecurity company showed that North Korea might only have earned $386,905 – though the costs inflicted on affected systems summed up in billions.

**Future Trends**

In the following years, the international community can expect North Korea to...
conduct more frequent cyber operations. Statistics from the South Korean Ministry of Defense showed that “hacking attempts against South Korean forces increased from 4,000 cases in 2017 to approximately 5,000 cases in 2018, and 9,533 cases in 2019.”

Through an analysis of data from the UNSC, the Heritage Foundation, and the Council on Foreign Relations, this paper finds that nearly half (43%) of North Korean cyber operations are financially motivated, followed by aims to disrupt (36%) and espionage (21%) (Figure 2). As a result, financial institutions, including banks and cryptocurrency exchanges, are the most common targets of North Korean hackers (Figure 3). Since Pyongyang continues to suffer from economic sanctions, North Korea will likely increase the intensity of its cyber thefts from financial institutions in the near future. In terms of locations, while North Korea has attacked countries worldwide, its cyber operations have

concentrated on targets in South Korea and the United States (Figure 4). This trend will likely continue, given Pyongyang’s hostility toward Seoul and Washington. Moreover, there is a notable trend that North Korea’s cyber operations have been expanding in their scope with campaigns against individuals and organizations from multiple countries at one time.
Policy Recommendations

North Korea’s cyber-attacks constitute a growing threat to the United States, its allies, and the international system, as Pyongyang uses cyberweapons to cause disruption, conduct espionage, and generate revenue. This paper proposes four policy recommendations to deter Pyongyang’s cyber capabilities build-up:

- Establish a cyber defense and cyber deterrence mechanism in the U.S.-ROK alliance,
- facilitate international cooperation,
- strengthen public-private partnerships,
- and design a comprehensive government strategy.

First, Washington and Seoul should further align their cyber defense and cyber deterrence capabilities through their military alliance. South Korea’s recent participation in the cyber defense center for the North Atlantic Treaty Organization (NATO) is a positive development. Established in 2008, NATO’s Cooperative Cyber Defence Centre of Excellence (CCDCOE) provides member nations with “unique interdisciplinary expertise in the field of cyber defense research, training and exercises covering the focus areas of technology, strategy, and law.” Seoul’s membership in the CCDCE will improve its understanding of North Korea’s cyber strategy and enhance its cyber defense against Pyongyang’s persistent attacks.

Though it is debatable whether current cyber-attacks from North Korea have strategic effects on South Korea, deterring North Korea’s low-level attacks may be challenging, as deterrence experts assess Pyongyang as “a very determined cyber actor.” Therefore, the U.S.-ROK alliance should focus on strategic-level attacks in the cyber domain. Specifically, Washington and Seoul should issue joint statements on cyber deterrence with unambiguous language indicating the incorporation of cyber deterrence in their mutual defense treaty. Furthermore, the alliance should formulate a detailed cyber deterrence strategy, identifying the corresponding retaliation against North Korea’s cyber-attacks and properly signaling to Pyongyang.

Second, Washington and Seoul should reach out to the international community for broader cooperation. While North Korea’s Internet is largely isolated from global networks, its hackers operate around the world and launch cyber-attacks via overseas servers. Additionally, considering North Korea’s escalating scope and scale of its cyber operations against multiple countries, combined efforts from the international community to protect critical global infrastructure like the SWIFT are immediately needed to tackle the North Korean cyber threat.

The first step should be expanding the narrow focus on North Korea’s conventional weapons capabilities to incorporate cyberspace into international monitoring and regulation. By sharing information with international partners on suspicious cyber activities and tactics North Korean hackers use, U.N. members will be better prepared to defend against North Korea’s cyberattacks and expose their footprints for global warnings. Developing countries in Southeast Asia, Africa, and Latin America should receive special attention in this effort. Based on the historical records, their relatively poor cyber defense systems make them attractive and vulnerable targets of Pyongyang for financial thefts. The United States can assume leadership in facilitating inter-government coordination, establishing the international legal framework and law enforcement agencies, and promoting compliance with cybersecurity standards.
These efforts also have broader implications for defending and deterring malicious cyber operations by other actors. However, Washington should also be aware of potential pushback from other international actors who may interpret it as Washington’s attempts to dominate cyberspace.

**Third, the United States should strengthen public-private partnerships to countermeasure North Korean cyber-attacks on private corporations and financial institutions.** Private firms tend to “underestimate cyber risks and underinvest in cybersecurity or prefer to ‘free ride’ while expecting the government to manage the North Korean cyber threat.” Moreover, private firms often refrain from reporting cyberattack incidents to protect their reputation. However, the surprising similarity in the cyber tactics used by North Korean hackers suggests the importance of information sharing to alarm the public and private sectors. For example, the malware that attacked Sony Pictures in 2014 had many overlaps with the one used against South Korean banks in 2013. Therefore, it is imperative to encourage information sharing and compliance with cybersecurity rules to improve the resilience of private sector systems.

Washington can achieve this through both formal and informal channels. The government can use legal frameworks such as The Cybersecurity Information Sharing Act to coordinate information sharing among various entities. The Internet Corporation for Assigned Names and Numbers (ICANN) is a model for establishing an informal private-public partnership. Established in 1998 to ensure the network’s stability and security, ICANN has expanded from a U.S. national focus to global governance under the guidance of an international board of directors with diverse backgrounds. In addition, the government should promote education and training programs for individuals to raise public awareness of North Korean cyber tactics.

**Fourth, the United States should establish a comprehensive whole-of-government strategy.** The diversity of Pyongyang’s cyber operations in its targets and effects would require collaborations from at least “the Departments of Treasury, Justice, Defense, Commerce, and Homeland Security as well as the Intelligence Community” directed by the White House. The Department of State International Cyberspace Policy Strategy released in March 2016 is an inspiring attempt. It described a whole-of-government approach to cyber deterrence with diplomacy, law enforcement, economic tools, military force, and intelligence capabilities. The creation of a National Cyber Director that advises the President on cyber policy is another welcomed development. Washington will need to specify the authority and procedures for inter-agency coordination to consolidate these efforts.

**Conclusion**

North Korea’s cyber warfare is an evolving security threat to the United States, its allies, and the international community. Pyongyang’s advancement in cyber weapons complements its broader strategy of creating an asymmetrical advantage vis-à-vis the U.S.-ROK alliance and is rooted in its guerrilla tradition. Cyber tools are also attractive to the regime because of their cost-effectiveness and low risks of retaliation. Given these motivations and the militarism in North Korean politics, cyber capabilities will continue to receive substantial investments from Pyongyang.

To date, North Korean hackers have demonstrated increasing sophistication in their techniques while expanding the scope and scale of their operations. Pyongyang
mainly applies cyber weapons to cause disruption, conduct espionage, and generate revenue. As such, North Korea poses significant threats to critical infrastructure, classified and sensitive information, and financial institutions around the world.

Defending and deterring North Korean cyberattacks requires extensive inter-government and intra-government cooperation and a public-private partnership. Furthermore, strengthening the U.S.-ROK alliance in cyberspace is critical to preventing North Korea from undermining the stability and security of the Korean Peninsula. Washington and Seoul should send clear messages and take firm actions to counter Pyongyang’s aggression in the cyber domain.

**About the Author:** Jie Gao is an M.A. candidate in Security Studies at Georgetown University. Her research interests include U.S.-China relations, Chinese domestic politics, security issues in Asia, and artificial intelligence.


12. The State Affairs Commission replaced the National Defence Commission in 2016 and expanded its scope to include issues aside from defense and security.


14. ROK Ministry of National Defense, 2018


24. Thorium is a safer and more efficient alternative to uranium. Klingner, 2021.


29 Kim, 2022, pp.8.
30 Klingner, 2021, pp.7.
31 Wolff, Josephine, “How Big of a Cyber Threat Is North Korea?” The National Interest, Mar 2022,
39 Ibid.
40 Kim, 2022, pp.9.
43 Pinkston, 2016, pp.64.
44 Kim, 2022, pp.10.
45 Jun, LaFoy, and Sohn, 2015, pp.75.
47 Ibid.
49 Klingner, 2021, pp.11.
51 Klingner, 2021, pp.11.
Authoritarian Friends and Totalitarian Enemies: The Relevance of the Kirkpatrick Doctrine in the Twenty-First Century

Steven Hu

Since the Cold War, the United States has maintained a foreign policy that relies heavily on arms sales to allies and partners, even those governed by authoritarian regimes that hold values incongruent with its own. The justification behind these sales can be best summarized and explained by the Kirkpatrick Doctrine, an international relations theory developed by U.S. Ambassador to the United Nations Jeane Kirkpatrick. The premise of this theory is that the United States ought to supply arms to "authoritarian friends" to prevent them from becoming "totalitarian enemies." Thus, by sharing weapons systems and dictating the terms of their use, the United States can theoretically influence its authoritarian allies to adhere to the laws of armed conflict and prevent them from adopting belligerent foreign policies.

However, developments throughout the Global War on Terrorism prompt questions regarding the ethics of U.S. arms sales policy. Specifically, the Saudi Arabia-led coalition’s intervention in the ongoing Yemeni Civil War displays how the U.S. has struggled to control how its friends employ U.S. exports. Multiple human rights organizations have accused the coalition of war crimes. This paper argues that the Kirkpatrick Doctrine’s presumption that the United States can significantly influence state behavior through arms sales is outdated.

Introduction

The Kirkpatrick Doctrine has embodied U.S. policy around arms sales since the Cold War. In her 1979 Commentary Magazine article, “Dictatorships and Double Standards,” Jeane Kirkpatrick first explains the necessity for the United States to supply arms to regimes and groups, even when their values are incongruent with those of the United States, like democracy and individual liberty. The article caught the eye of then-California Governor Ronald Reagan, who, as U.S. President, adopted the doctrine as a central strategy to his foreign policy. Reagan oversaw landmark arms sales to dictatorships such as Saudi Arabia, Guatemala, the Philippines, and Iraq, as well as anti-communist paramilitary groups such as the Nicaraguan Contras and the Afghan Mujahideen. Kirkpatrick asserts that an authoritarian regime is less ideological compared to a totalitarian one, and only seeks to control and regulate its society rather than influence its people’s thoughts and beliefs through active propaganda, espionage, and subversion. Therefore, the United States could 1) more effectively regulate and control authoritarian allies’ employment of U.S. military exports, compared to if these allies purchased arms from the Soviet Union or China, and 2) have an easier process of rehabilitating said authoritarian regimes into liberal democracies due to U.S. influence on recipient governments and their military structures. The doctrine, written in the context of the Cold War, has continued to be relevant even after the Soviet Union’s collapse. With the emergence of threats from non-state actors such as Al-Qaeda and the Islamic State, as well as those from authoritarian states such as Iran, Russia, and China, the demand to maintain a balance of power through allied capacity building.
became essential once more to enable U.S. foreign policy objectives abroad. Not only do these partnerships provide overseas U.S. military forces with staging grounds, logistical networks, and intelligence collection and sharing capabilities, but also the ability to deter without having to deploy boots on the ground.

The Kirkpatrick Doctrine hypothesizes that a democratic arms-selling state can influence how an authoritarian arms-buying state employs said arms to accord with conditions and the laws of armed conflict. Furthermore, the military and economic relationship between buyers and sellers could foster democratization among arms recipients, as they fulfill certain prerequisites to continue receiving exports. However, recent experiences in wars of the Post-9/11 era have demonstrated difficulties in ensuring that countries that receive U.S. security assistance act in congruence with their foreign policy ethics.

Security partnership between Saudi Arabia, UAE, and the United States has strengthened in recent years due to growing political instability in neighboring Arab nations and the rise of Iran as a regional power. In 2015, a Middle East proxy war commenced with international intervention in the Yemeni Civil War. A Saudi-led coalition consisting of other U.S. allies such as Jordan, Qatar, and Kuwait entered the war on the side of the Hadi government. At the same time, Iran initiated funding and support for the Houthi rebel movement. Since then, security assistance to the Saudi-led coalition has continued to be vital in countering Iranian influence in the region to maintain the balance of power in the Middle East. The integration of US-produced systems in their arsenals enables greater interoperability between nations and provides allied forces with the technological superiority to deter and respond to belligerent activities and influence. Furthermore, providing U.S.

Saudi Arabia’s national security through both arms sales and U.S. troop deployments. For example, when Saddam Hussein’s Iraq threatened Saudi Arabia in 1990, the United States commenced Operations Desert Storm and Desert Shield to protect Saudi Arabia from invasion—its largest force mobilization since the Vietnam War.

Similarly, the UAE has become a major ally of the United States in the post-9/11 era. Heralded by senior U.S. military officials as “Little Sparta,” the UAE has enabled U.S. military operations in the Middle East with joint deployments throughout Operations Enduring Freedom, Iraqi Freedom, and Inherent Resolve, and served as a staging ground for resupply, support, and logistics.

Security partnership between Saudi Arabia, UAE, and the United States has strengthened in recent years due to growing political instability in neighboring Arab nations and the rise of Iran as a regional power. In 2015, a Middle East proxy war commenced with international intervention in the Yemeni Civil War. A Saudi-led coalition consisting of other U.S. allies such as Jordan, Qatar, and Kuwait entered the war on the side of the Hadi government. At the same time, Iran initiated funding and support for the Houthi rebel movement. Since then, security assistance to the Saudi-led coalition has continued to be vital in countering Iranian influence in the region to maintain the balance of power in the Middle East. The integration of US-produced systems in their arsenals enables greater interoperability between nations and provides allied forces with the technological superiority to deter and respond to belligerent activities and influence. Furthermore, providing U.S.

Saudi Arabia and the UAE

Saudi Arabia has been one of the largest recipients of U.S. military aid since the end of World War II, as well as an economically and militarily important ally, enabling the United States and NATO to project power in the Middle East. The United States has consistently supported

Georgetown Security Studies Review 43 Volume 10 | Issue 2
regional allies with the most advanced weapons systems in the global market allow them to defend their national interests without the commitment of significant U.S. troop deployments, putting servicemembers at risk of hostilities. However, Saudi and Emirati military operations have attracted scrutiny from some of the public and Members of Congress, both of whom have accused Saudi Arabia of not abiding by the laws of armed conflict.14

Since 1995, Saudi Arabia’s military expenditure has almost quadrupled, increasing from $20 billion to a high of $80 billion in 2015, and leveling out at around $60 billion in 2020.15 Saudi Arabia is the world’s largest arms importer, accounting for 12 percent of all total activity in the sector.16 In 2020, 79 percent of Saudi Arabia’s arms imports came from the United States.17 U.S. arms exports also comprise 64 percent of UAE weapons imports.18

The U.S. military command structures have significant authority and influence over how Saudi Arabia and the UAE conduct military operations. Under the advice of western military advisors and due to a lack of ground combat experience, the Saudi Arabia-led coalition has primarily relied on air assets to conduct its operations, while other coalition forces such as Sudan fulfill the demand for ground combat.25 Though U.S. arms sales have greatly enabled Saudi Arabia’s ability to project power, the Saudi military is still heavily reliant on certain U.S. military capabilities and infrastructure, such as Command and Control (C2), Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR), and logistics.19 This is known as remote warfare, as the bulk of combat troops are removed from direct fighting, delegating kinetic strikes to indirect fire and intelligence collection to unmanned ISTAR assets. Thus, operating under the scope of their remote warfare doctrine, the bulk of Saudi and Emirati military operations in Yemen have been conducted through the air and naval assets, striking targets using a combination of fighter aircraft, drones, cruise missiles, and ground and naval artillery.

This reliance on air power has led to staggering collateral damage. Based on the reporting from the Yemen Data Project, since March 2015, there have been a total of 24,025 coalition air raids, resulting in 8,796 dead and 9,865 injured.27 During that period, more than a quarter of the raids were on non-military targets, and approximately 40 percent were on unknown targets.28 This did not deter the United States from making additional sales, as exports steadily increased during that period. Civilian casualties continued to fluctuate as UN researchers did not find any change in attitude by coalition C2 in changing their strategies to prevent human suffering.31 The Yemen Group of Eminent Experts concluded that "the parties to the conflict continue to show no regard for international law or the lives, dignity, and rights of people in Yemen, while third States have helped to perpetuate the conflict by continuing to supply the parties with weapons."32

The alleged human rights violations by Saudi Arabia and UAE have not gone unnoticed. In 2016, then-US President Barack Obama temporarily halted arms sales due to concerns over how US-made munitions were being employed, and senior U.S. lawmakers have also voiced their concerns in
congressional hearings and sessions. In 2021, U.S. President Joe Biden and Secretary of State Antony Blinken adjusted U.S. missile and air defense policy in Saudi Arabia, directly removing U.S. troops, advisors, and C2 elements from ISR and offensive operations.

This decision sheds light on the shortcomings that sellers have in effectively controlling how their buyers use their weapons systems. Amid discussions within the United States to prevent a $23 billion aid package that would include the UAE in the F-35 Joint Strike Fighter program, both Arab states have begun talks with Russia and China regarding possible procurement opportunities. China also has a keen interest in supplying Saudi Arabia and increased its arms exports to the country by 40 percent from 2013 to 2019 to become Saudi Arabia’s ninth large supplier. With Germany, Sweden, and Switzerland beginning to impose embargoes on their exports to Saudi Arabia, and a reduced U.S. commitment, Saudi Arabia may seek out alternative suppliers with less concern for the laws of armed conflict and how their arms will be used.

Egypt’s About Face

The Egypt case study indicates how a buyer state may react when it has ethical differences with its seller over foreign policy. The United States’ relationship with Egypt is complicated, albeit important to its geopolitical aims in the Middle East. Beginning in 1979, the United States began developing a military relationship with Egypt, and would eventually provide approximately $1 billion of military assistance—mainly tactical assets—to the country for decades to come. More recently, following the 2013 overthrow of Egyptian President Mohamed Morsi, relations between the two countries have strained. President Obama temporarily froze military assistance due to new Egyptian President Abdel Fattah el-Sisi’s poor human rights record. This signaled to Egypt that the United States could not be trusted as its only arms seller, and thus Cairo began to look elsewhere. As U.S. defense policy expert Anthony Cordesman noted, “Egypt has been so dependent on the U.S. that it is beginning to try to find some kind of contingency arrangement so that it can’t be levered by Congressional pressure to change.”

From 2000 to 2009, 75 percent of Egypt’s military imports came from the United States. However, this share declined to 20 percent over the following decade. Egypt has replaced the bulk of its U.S. arms imports with Russian ones, which accounted for 41 percent of its imports between 2016-2020. Russia now represents Egypt’s largest arms supplier.

Due to the influence of the military in Egyptian politics and government, Egypt’s human rights violations have long been associated with its armed forces. Its recent human rights record includes extrajudicial killings, forced disappearances, jailing of political prisoners, violations of laws of armed conflict in its Sinai counterinsurgency operations, restrictions of movement using military forces, and uses of military courts to prosecute and trial civilians. President Biden has withheld $300 million of military aid and prevented the approval of a further $130 million assistance package in the current fiscal year.

Though not actively engaged in the same conflict intensity as Saudi Arabia and
the UAE, the Egyptian military faces a growing counterinsurgency campaign in the Sinai Peninsula. Egypt’s position as a critical junction between unstable areas of the Middle East and Africa places a multitude of national security demands on the Egyptian military. To meet these challenges, Egypt has sought out a variety of weapon systems from Russia. These purchases include attack helicopters, fifth-generation fighter jets, and various types of guided and unguided munitions. Furthermore, Egypt's procurement of Russia's S-300 missile system also challenges Israel's qualitative military superiority in the region, a status quo that the United States would like to preserve.

US attempts to influence Egypt’s foreign and domestic policy have only pushed Egypt closer toward Russia, as they continue to negotiate new arms agreements and participate in joint military exercises, such as Moscow’s Black Sea Naval Drills. Congressional research analysts have assessed that further attempts by the U.S. administrations to withhold military aid will only encourage Egypt to partner with regimes with few concerns for human rights. Egypt is not alone in shifting its arms purchases away from the United States. The Philippines, a U.S. ally since the end of the Cold War, began to procure Russian MI-17 helicopters after completing a new arms deal with the United States to diversify the country's military portfolio. More countries have begun to realize the dangers of buying arms overwhelmingly from one seller, especially when those arms come with strings attached.

A Catch-22?

The Kirkpatrick Doctrine was born into a bipolar world during the Cold War when the dichotomy between allies and enemies was far more visceral than it is today. In many ways, global power came down to a zero-sum game between countries siding with the Soviet Union and the Warsaw Pact or the United States and NATO. A different set of geopolitical realities in the twenty-first century highlights the shortcomings of the Kirkpatrick Doctrine.

First, the overwhelming number of systems purchased serves an offensive role in tactical and operational levels of warfare, mainly for air domains. This highlights the changing nature of modern warfare, as states begin to rely more on the effectiveness and relative safety of airpower as a means of power projection. Thus, the high demand for these weapons systems in a competitive defense market gives buyers abundant choices without having to consider factors such as the foreign policy ethics of their sellers. Furthermore, the Saudi-led coalition in Yemen has shown that arms-selling states are often willing to continue to export arms and even augment C2 capabilities when their recipients share similar strategic-level interests. Sellers have minimal control over their recipients’ operations, as exemplified by the Saudi Air Force making minimal adjustments in its targeting procedures to better align with the laws of armed conflict. Similarly, consistent U.S. military assistance to Egypt has also not led to meaningful strides in Egypt’s human rights record.

Given arms sellers’ inability to alter buyers’ behavior, they should cease their exports to, at the very least, avoid complicity in human rights abuses and war crimes. The alternative, according to Kirkpatrick, would be a continuation of the status quo and possibly worse, as arms recipients can easily seek out new
exporters to fulfill their needs. By attaching strings to its arms exports, however, the United States risks aiding in the resurgence of Russian and Chinese weapons industries. This leaves democracies like the United States in a catch-22 scenario: remain complicit in the authoritarian regimes’ violations of human rights and the laws of armed conflict or allow even less concerned authoritarian states to export their weapons and exacerbate the status quo.

**About the Author:** Steven is currently pursuing his Master's Degree in Applied Intelligence. He received his Bachelor's Degree in International Relations and History from Victoria College, University of Toronto. In his free time, Steven enjoys playing sports, reading, cheering for the New England Patriots, and confusing Americans with his Canadian accent.
1 George Packer, *The Assassins' Gate: America in Iraq*. Faber and Faber, 2007, 16
4 Packer, *The Assassins’ Gate: America in Iraq*. Faber and Faber, 2007, 16-18
5 Kirkpatrick, “Dictatorships & Double Standards.” *Commentary Magazine*.
6 Kirkpatrick.
7 Packer, 32
9 “Excerpts From Pentagon's Plan: 'Prevent the Re-Emergence of a New Rival.’” *The New York Times*
19 “Arms Sales in the Middle East: Trends and Analytical Perspectives for U.S. Policy,” 23
20 “Arms Sales in the Middle East: Trends and Analytical Perspectives for U.S. Policy,” 23
21 Ibid.
22 Ibid, 26
23 Ibid.
24 Ibid.
27 “Yemen data project, 2021.” [https://Yemendataproject.org](https://Yemendataproject.org)
28 “Yemen data project, 2021.”
32 UN (2020) Fresh war crimes fears highlighted in new Yemen report.
33 “Arms Sales in the Middle East: Trends and Analytical Perspectives for U.S. Policy,” 33
Yemen: Civil War and Regional Intervention *Congressional Research Service*, November 2021, 13

“Arms Sales in the Middle East: Trends and Analytical Perspectives for U.S. Policy.” 40

Bogers and Semesters, 251


Alexandra Kuimova, “Understanding Egyptian Military Expenditure,” SIPRI Background Paper, October 2020, 24


“Egypt: Background and U.S. Relations.” 29

“Russia, Egypt to Hold Joint Naval Drills in the Black Sea This Year.” TASS. https://tass.com/defense/1210037.

“Egypt: Background and U.S. Relations,” 33

John V. Parachini Ryan Bauer, and Peter A. Wilson, “Impact of the U.S. and Allied Sanction Regimes on Russian Arms Sales,” 28
Enemies, Allies, and Artificial Intelligence: Developing Rules and Norms for Lethal Autonomous Weapons Systems

Kiseok Michael Kang

With the advent of artificial intelligence in recent years, countries are developing and testing lethal autonomous weapons systems (LAWS), a class of weapon systems that leverage AI to select and engage targets with little to no human intervention. For decades, the international community has regulated the conduct of hostilities through the laws of armed conflict (LOAC) and other relevant norms. Despite the significant impacts LAWS will have on the battlefields, there are currently no agreed rules or norms for the responsible development and use of LAWS. This paper explores the potential challenges that the lack of common standards in the area of LAWS poses to the United States. It finds that the absence of norms can trigger inadvertent escalation and undermine geopolitical stability in the context of renewed great power competition. Furthermore, the U.S. alliances will face serious interoperability problems should the United States and its allies fail to establish common grounds on LAWS. To address these challenges, the U.S. government should pursue a minilateral, not multilateral, and differentiated approach to building rules and norms on LAWS with its adversaries and allies.

I. Introduction

Artificial Intelligence is becoming “the new fire” that transforms various sectors in our society, including international security. Ben Buchanan and Andrew Imbrie argue that AI, like fire, can play both a constructive and destructive role for human civilization depending on how humanity handles it. AI enables computers and machines to perform tasks that normally require human intelligence. Many believe that AI, playing a constructive role in international security, will revolutionize warfare as it can make military operations more agile, efficient, and lethal with less manpower. Leading AI expert Kai-Fu Lee, calls LAWS “the third revolution in warfare” following gunpowder and nuclear weapons. Intelligence analysis, logistics management, and command and control are among many military functions that can benefit from AI. However, perhaps the most watched and debated development pertaining to military applications of AI is the development and use of lethal autonomous weapons systems (LAWS). Like AI itself, there is no agreed definition of LAWS, but the U.S. Department of Defense (DOD) defines it as “weapon system[s] that, once activated, can select and engage targets without further intervention by a human operator.” This paper will use the DOD’s definition when referring to LAWS from this point on.

From crossbows to drones, emerging technologies time and again disrupted and shaped the law of armed conflict (LOAC), a set of international rules and norms regulating armed conflict. LOAC has helped humanity to curb “the evils of war” and make the conduct of hostilities more humane since the time of ancient Greece and Rome. Agreeing on common rules is important for both enemies and allies alike because the lack of the rules of the game can increase uncertainty on the battlefields, lead to unnecessary escalation between adversaries, and hamper coalition operations. Emerging and disruptive technologies can shape how militaries fight one another and necessitate new rules of engagement. For instance, governments are trying to establish new norms for cyberspace and outer space, the two newest warfighting domains. Given the
far-reaching impacts AI will have across the military spectrum and the rapid pace of its development, building rules and norms for LAWS is imperative for states. However, when compared to other emerging technologies, international norms regarding the use of AI-enabled weapons remain still at a very nascent stage. The Group of Governmental Experts (GGE), a United Nations working group that addresses emerging technologies in the area of LAWS, has been the main international vehicle for multilateral norm-building for LAWS since 2014. Although the GGE process has facilitated international discussion on the subject and produced some valuable outcomes such as the 11 guiding principles, it has been slow and stalled in recent years.

This paper examines the potential challenges that the ruleless development and use of LAWS will pose for the United States on the battlefield. The next section reviews the existing laws of war and the current status of international efforts applying these rules to LAWS. Section III discusses the ways in which autonomous weapons systems can spark inadvertent escalation and threaten strategic stability in the context of great power competition. Section IV analyzes the implications of LAWS for alliances: the absence of common rules on LAWS may disrupt the interoperability and weaken the reliability of the U.S. alliance systems such as NATO. Finally, Section V recommends that the U.S. government take a minilateral and differentiated approach to developing basic rules and norms for LAWS. Rather than trying to create one-size-fits-all norms through large multilateral settings such as the GGE, the United States should cooperate with its allies to devise a clear and viable code of conduct, while simultaneously seeking high-level, foundational agreements on norms with adversaries that can minimize potential AI-related risks and facilitate confidence-building measures.

II. Existing Laws of War and Their Applications to LAWS

The modern law of armed conflict, also known as international humanitarian law (IHL) or jus in bello, regulates the conduct of hostilities to protect the vulnerable and alleviate human suffering in war. The Geneva Conventions of 1949 and their Additional Protocols have codified most customary rules and norms of IHL. The core principles of IHL include the prohibition of causing unnecessary suffering, the distinction between combatants and civilians, military necessity, and proportionality. Article 35(2) of the 1977 Additional Protocol I explicitly prohibits weapons that “cause superfluous injury or unnecessary suffering.” Article 51 of the same Protocol promotes the protection of the civilian population and forbids indiscriminate attacks. Additional Protocol I also requires state parties to conduct a weapons review “in the study, development, acquisition or adoption of a new weapon” to determine whether the weapon in question violates IHL.

Lastly, even in the absence of a relevant international law or custom, the principle of humanity and the dictates of public conscience apply to any new weapons systems according to the Martens Clause. To further cement norms on what kind of weapons should be used in warfare, states adopted the Convention on Certain Conventional Weapons (CCW) in 1980. The purpose of CCW is to prohibit or limit “the use of specific types of weapons that are considered to cause unnecessary or unjustifiable suffering to combatants or to affect civilians indiscriminately.” Under the framework of CCW, particular weapon types are prohibited, such as projectiles that are not detectable by X-ray, anti-personnel mines, incendiary weapons, and blinding laser weapons. Today, a total of 125 states including the U.S., Russia, and China are party to the CCW. Apart from the CCW, a
separate set of norms and legal frameworks had evolved for weapons of mass destruction. For example, the Chemical and Biological Weapons Conventions have established norms against the use of these weapons in IHL. Similarly, nuclear arms control agreements demonstrate that the major powers have mutual interests when it comes to particularly destructive weapons of war being used. Although many of the Cold War-era nuclear arms control treaties have expired or been terminated, they contributed to the stabilization of strategic competition during the Cold War and led to the conclusion of the New Strategic Arms Reduction Treaty (New START) which is still in force.\footnote{16}

Against this backdrop, the CCW became an appropriate forum to discuss legal and regulatory issues in the area of LAWS. The High Contracting Parties to the CCW decided to establish the aforementioned GGE with a mandate to identify rules and principles applicable to LAWS. Several GGE meetings since 2017 have attempted to achieve a consensus on several key issues pertaining to the use of LAWS. One of the most contentious issues in the GGE has been the question of how to define the technology. Countries differ in how they define LAWS, and the absence of an agreed definition has hindered discussions at the GGE. For instance, the United Kingdom officially opposes the development of LAWS, but its definition of such a system is narrow and futuristic to the extent that it essentially allows the development of “systems with an unacceptably high degree of autonomy.”\footnote{17} Similarly, China supports a ban on the use of LAWS, but it equivocally defines LAWS as “indiscriminate [and] lethal systems that do not have any human oversight and cannot be terminated.”\footnote{18}

Despite their differences in the definition of LAWS, most countries agree that fully autonomous or “human out of the loop” weapons systems are not compatible with IHL. To understand this debate, it is important to differentiate various levels of human involvement in autonomous systems. “Human in the loop (HITL)” refers to AI-enabled systems that require human intervention during the cycle of observe, orient, decide, and act (OODA). For instance, the U.S. counter-rocket, artillery, and mortar system (C-RAM) identify and track incoming rounds autonomously, but needs humans to make final verification before engagement, thus keeping humans in the loop. “Human on the loop (HOTL)” systems do not require human intervention and can engage targets on their own, but human operators can override the decision made by the algorithm. The Patriot air defense system and Aegis systems are examples of HOTL systems. Both HITL and HOTL systems are considered semi-autonomous systems. On the contrary, “human out of the loop (HOOTL)” systems can search for, detect, decide to engage, and engage targets all on their own without any human interaction.\footnote{19}

The following Table 1 summarizes this.

<table>
<thead>
<tr>
<th>Human in the loop (HITL)</th>
<th>Select targets and deliver force only with a human command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human on the loop (HOTL)</td>
<td>Select targets and deliver force under the oversight of a human operator who can override the actions</td>
</tr>
<tr>
<td>Human out of the loop (HOOTL)</td>
<td>Capable of selecting targets and delivering force without any human input or interaction</td>
</tr>
</tbody>
</table>

Table 1: Different Levels of Human Involvement\footnote{20}
Drawing a clear line between semi- and the fully autonomous system is challenging since the notion of autonomy is a continuous spectrum and a weapon can consist of multiple components with different levels of autonomy. Hence, many countries highlight the importance of the concept of *human-machine interaction*—an important factor in deciding whether LAWS can be employed in compliance with IHL. The Campaign to Stop Killer Robots, a coalition of non-governmental organizations led by Human Rights Watch, seeks to ban any autonomous system without “meaningful human control” over the use of force. Germany, France, and many other countries support that human operators must retain control to ensure compliance with the principles of distinction, proportionality, and necessity. On the other hand, the U.S., Israel, and other countries acknowledge the importance of having an appropriate level of human judgment in the use of force but argue that the appropriate level of human-machine interaction should be determined on a case-by-case basis. Israel, in particular, strongly opposes the use of the term “human control” and prefers a more general term like “human-machine interaction.”

Despite vastly differing views of participating countries, the GGE was able to produce 11 guiding principles in 2019. They are not binding norms but can serve as “a useful and valuable starting point to build substance towards a normative and operational framework.” Principle (a) proclaims that IHL continues to apply fully to all weapons systems, including LAWS. Principle (c), which many countries consider to be of primary importance, demands human-machine interaction to ensure that the potential use of LAWS complies with applicable international law, in particular IHL. Although the adoption of 11 guiding principles is a commendable achievement, there have been criticisms of their lack of specificity and enforceability. For example, Principle (a) fails to elaborate on when and how IHL can apply to LAWS in different situations. Will the principle of precautions, which requires a state to take measures to minimize civilian harm, apply only to operators of LAWS, software developers, or data collectors that will enable the algorithm to calculate potential harm to civilians? Similarly, it is unclear how to understand human-machine interaction in Principle (c) given countries’ varying opinions on the appropriate level of human control or judgment over machines. To resolve this problem, the Campaign to Stop Killer Robots and a diverse set of states including Austria, Brazil, China, Mexico, New Zealand, and the Philippines expressed their support for a new legally binding instrument on autonomous weapons systems. Others, particularly the United States and Russia, continue to assert that a new treaty is unnecessary and that existing norms suffice. These countries further argue that LAWS can improve compliance with IHL on the battlefields. For example, AI-enabled platforms can “dramatically improve target identification and discrimination” resulting in fewer unintended civilian casualties. Still, other countries such as Germany and France favor a political declaration over a binding instrument. This “enduring impasse” has paralyzed the GGE process in recent years.

In sum, no international rules currently exist in the areas of LAWS. On the contrary, the multi-year GGE process has demonstrated that there is significant disagreement among countries on how to regulate LAWS. Interestingly, countries are not divided into their usual geopolitical camps on this issue. The United States and Russia advocate a more laissez-faire approach, while some NATO allies such as Germany and France voice concerns over
the unethical development and use of LAWS. In the absence of globally agreed rules, individual countries have sought to write their own rules. The U.S. DOD Directive 3000.09, which lays out U.S. policy on LAWS, is a notable example. Other countries like Russia and China have adopted a more general AI strategy that includes some military implications. In the absence of mediating ground rules, great power competition involving LAWS could lead to dangerous escalation.

III. LAWS and the Strategic Competition

The absence of common norms not only creates legal and ethical challenges but also can lead to practical problems on the battlefield. Great powers, especially, need to agree on basic rules of the road to avert inadvertent escalation and maintain strategic stability. LAWS is no longer science fiction. The 2017 SIPRI report identified 49 military systems from different nations that could engage targets autonomously “without the direct involvement of a human operator,” meaning HOTL or HOOTL. Some systems such as Israel’s Harpy, a loitering munition that can self-target radar emitters, and U.S. Tomahawk Anti-Ship Missile (TASM) have been fielded for years. As the SIPRI report points out, some of these systems are “automated” rather than “autonomous” as they carry out tasks through predefined procedures. However, with the advance of AI technology, more systems can perform sophisticated decision-making processes and cope with uncertain and complex environments. In this context, militaries around the world are pouring billions of dollars to build more capable LAWS that are not automated weapons but truly autonomous. Both the U.S. Third-Offset Strategy and the 2022 National Defense Strategy underscore the importance of leveraging AI and robotics in fighting and winning the wars of the future. The U.S. military and its industry partners are experimenting and developing a wide range of autonomous weapons systems that include AI-powered flying, underwater, surface, and ground vehicles with lethal capabilities. Some believe the widespread deployment of such systems is still decades away, while others believe that there is a real possibility of deployment within 10-15 years. Russia already deployed and test-drove its robotic tank known as the Uran-9 on the actual battlefield of the Syrian war. Moscow is eager to contend for superiority in AI, which can make Vladimir Putin “the ruler of the world” according to his own words. Besides the Uran-9, Russia is working on other autonomous systems such as self-destructing kamikaze drones. China is likewise aggressively developing a variety of AI-enabled weapon systems in order to counterbalance “technologically advanced adversaries” and achieve “battlefield singularity.” There will be significant strategic risks should the great powers begin to field LAWS without agreeing to ground rules for the responsible development and use of such systems. The “wait-and-see” approach advocated by the United States and Russia is particularly dangerous. First, LAWS can spark unintended escalation due to their inherent fallibility. Intensified competition can incentivize militaries to deploy LAWS that are fallible and more prone to inadvertently violating LOAC. The fear that the enemies are “operating at machine speed and we’re operating at human speeds” can also make militaries more risk-acceptant. Although the U.S. military promised a responsible, reliable, and governable approach to AI-powered weapons systems and a thorough review process, there is suspicion within the United States that its adversaries will not abide by the same moral codes. But this distrust could be mutual. Since there are no detailed rules regarding the appropriate level of human control, any government could delegate authority to machines.
largely unchecked. A 2020 RAND wargame concluded that in this situation, an autonomous system might employ force without human approval and intention. Given that LAWS will be trained on data from a controlled environment, the probability of these technologies behaving in an unexpected situation is high.

Second, the lawless development of LAWS could threaten geopolitical stability. This is because LAWS enable governments to pursue more risky operations without worrying about the cost of human lives. The frequent use of drone strikes today shows how governments might use more capable autonomous weapons to remove high-value targets in the future. China has already been employing unmanned and autonomous assets to probe contested areas in the South and the East China Sea. Even inadvertent non-lethal actions by poorly-designed LAWS such as crossing the border could lead to unintended escalation. Widespread use of LAWS will also lower the cost of war in general. The LAWS might in fact weaken deterrence and stability because adversaries would know that striking the opponent’s LAWS, typically unmanned, is less likely to trigger a wider conflict than attacking manned assets.

Lastly, great powers may seek to incorporate AI into the strategic command, control, and communication systems to improve the speed and precision of their nuclear arsenal. This will shorten the required response time and increase pressure on decision-making in a crisis to the point where human commanders and operators can be sidelined. AI-powered Intelligence, Surveillance, and Reconnaissance (ISR) capabilities coupled with autonomous missile defense systems can also seriously undermine strategic equilibrium. Although this looks like a bridge too far, with the development of hypersonic missiles, an AI-enabled missile defense system is becoming a necessity, not a luxury. This danger of AI potentially undermining strategic stability is a direct consequence of an absence of regulations limiting its use in warfare.

IV. LAWS and Alliances

Russia’s massive cyberattacks on Estonia in 2007 perplexed NATO leaders as there was no code of conduct for the alliance on the conduct of cyber warfare. The alliance lacked consensus on how to respond to non-kinetic cyberattacks, let alone whether a cyberattack constitutes “an armed attack” that can trigger Article 5. In the 2012 Wales Summit, NATO drafted the Tallinn Manual on the International Law Applicable to Cyber Warfare, affirming that cyberattacks such as the one against Estonia could lead to the invocation of Article 5. This case illustrates how military alliances can lag behind military innovations—and LAWS are no exception.

Without common standards across the alliance, NATO will face considerable interoperability challenges concerning LAWS. NATO recently adopted an AI strategy in 2021, but the strategy only prescribes broad principles and lacks substance. As discussed above, NATO allies differ in their views on the ethical use of LAWS. For example, Spain maintains that HITL is only acceptable for strictly defensive systems such as the Iron Dome, while offensive weapons should always include HITL. Portugal suggests time and space restrictions on LAWS to ensure compliance with IHL. When allies disagree on jus in bello, coalition operations can falter. During the Kosovo War, the United States and France had a considerable disagreement over the legality of bombing a civilian radio station that disseminates the regime’s propaganda. The discord delayed the operation for days. Similarly, the Trump administration’s reversal of the landmine ban policy troubled NATO operations as all other NATO members banned the use of anti-personnel mines under the Ottawa
The United States and other NATO member states, thus, need to devise a common policy position on the legal and ethical aspects of LAWS to avoid any interoperability problems on the battlefield.

Putting the legal and ethical issues of LAWS aside, NATO still has other pending issues for the alliance’s interoperability with LAWS. First, the free flow of data among the allies will be critical for the success of NATO’s AI strategy, but it is unclear how much data national governments will readily share, as there are strategic as well as privacy concerns associated with data sharing. While NATO established the Data Exploitation Framework Policy to facilitate data sharing among the allies, it still needs to set more detailed rules. Second, NATO should address the technology gap between the advanced and the less advanced. If the technologically advanced allies start to field LAWS on the battlefield while the less advanced continue to operate legacy systems and large infantry, a range of practical and ethical problems will arise. Third, NATO’s former Warsaw Pact states still operate the Soviet-era equipment which can be problematic for automated target recognition whether it uses visual or heat signature to distinguish targets. Fratricide can be a real danger to the alliance’s use of LAWS. For example, during the Iraq War, the U.S. Patriot air defense system shot down a British aircraft when the automated system misidentified the aircraft as an anti-radiation missile and the human operator accepted the system’s incorrect identification.

The introduction of LAWS into the alliance will also complicate the reliability of U.S. defense commitment to its allies. Historically, U.S. soldiers in Europe and East Asia have acted as “tripwires” to deter adversaries. However, maintaining a large military presence has become politically and economically costly for the U.S. government. By enhancing the alliance’s military capability and reducing personnel costs at the same time, the deployment of LAWS provides an attractive option for Washington. The allies, nonetheless, could interpret that as a sign of reduced security commitment by the United States. The United States also needs to reassure its allies that the deployment of LAWS does not necessarily reduce the threshold of war. Furthermore, should more U.S. strategic assets become AI-integrated and machine-controlled, the allies will demand to know more about what algorithms and data are used for these systems. In other words, the development of LAWS might lead U.S. allies to question the credibility of the American nuclear umbrella.

The highly institutionalized NATO is better positioned to address some of these challenges than other U.S. allies. As discussed above, NATO has already begun to discuss AI-related issues internally and made some progress such as the adoption of the NATO AI strategy and Data Exploitation Framework. In contrast, the United States lacks similar arrangements with its bilateral allies such as Japan, South Korea, and Australia, although their position on the legality of LAWS is more aligned with the United States than their European counterparts. South Korea, for instance, has already deployed autonomous sentry guns along the demilitarized zone and Australia explicitly opposed any premature ban on LAWS. Since these American allies do not have formal alliance relations with one another, data sharing for the Indo-Pacific theater could be particularly challenging. Also, several important actors in the region like India and Vietnam do not belong to either block. The multiplicity of actors will increase the complexity of the operating environment for LAWS and thus render unanticipated behaviors more likely.
V. Policy Recommendations

With the ongoing war in Ukraine and the atrocities committed there, the United States has a strong incentive to develop rules and norms regulating LAWS vis-à-vis enemies and allies. Moscow allegedly fielded “killer robots” in Ukraine, while Kyiv also employed Turkish kamikaze drones that have some autonomous capabilities. Future wars, in which the belligerents might seek to employ LAWS to win, could be even more catastrophic and inhumane if LAWS continues to be unregulated.

It took two devastating world wars for humanity to universally adopt the laws of war. After the atomic bombs were dropped on two Japanese cities and the Cuban Missile Crisis brought the world to the precipice of a nuclear war, the superpowers agreed to establish bilateral nuclear arms control and global non-proliferation regimes. The international community should learn from history and it still has a chance to prevent an AI-led world war. With the most advanced military and global interests, the U.S. has an imperative not only to develop bleeding-edge AI technologies but also to build international rules and norms that can create more predictable and secure environments for these systems to operate. As such, I recommend the following two approaches to the U.S. government.

1. Minilateral Approach

   The United States should take a minilateral, not multilateral, approach, which could expedite the process of drafting rules and norms pertaining to LAWS. While technology is advancing at a rapid pace, international efforts to build common standards for technology have been lagging. The GGE, the main international forum on the subject, struggles to move forward because of the diverging interests of participants. This is in part unavoidable since it includes a very broad group of stakeholders and adopts the final reports on a consensus basis. The most recent GGE on LAWS meeting was plagued by the conflict between Russia and Ukraine.

   Given the arduous and protracted nature of international negotiation on regulating LAWS, it is wise to pursue minilateralism, a more focused approach with a small number of countries. Such an approach is more efficient since like-minded states can initially agree to basic rules that are easy to negotiate and build upon. The Tallinn Manual, produced by NATO allies, is a good example. The international community failed to come up with binding rules on cyber warfare even after decades of negotiations, but the NATO-led Tallinn Manual, although non-binding, has provided a basis for global norms on cyber war. Similarly, the World Trade Organization (WTO), which champions consensus-based decision-making, failed to produce any meaningful trade agreements since 2000 due to the profound disagreement among its member states. Another valuable example comes from the “plurilateral trade agreements,” which allow a subset of WTO member states to negotiate and conclude a mini-trade agreement as a solution to inefficient and inoperative multilateral negotiations.

2. Differentiated Approach

   Since Washington has different sets of concerns for its adversaries and allies when it comes to deploying LAWS on the battlefield, it should build different sets of rules. As for its near-peer competitors such as Russia and China, the United States should focus on finding the lowest common denominator: the rules for risk mitigation and management. Although great powers wish to realize the full potential of LAWS, they nonetheless can agree on basic safeguard rules to avoid inadvertent escalation and geopolitical instability. Some skeptics may argue that it is infeasible to produce any meaningful and satisfactory agreement on LAWS. They will further point out that, “the more
useful a technology is at providing armies with an edge, the harder it is to effectively regulate.”67 The international community was mainly successful in restraining the use of weapons that do not decide the outcome of war, such as blinding lasers. Nonetheless, states had successfully negotiated many important and complex issues in the past when they shared a sufficient common interest. To avoid nuclear catastrophe, superpowers voluntarily limited the number of warheads and missiles each country could possess.

The rules of the road can include limiting the incorporation of AI into nuclear control and command systems and enhancing transparency about the development and deployment of LAWS. Great powers can also agree on “off-limit” geographical areas for LAWS that can include contested areas around the world.68 Alternatively, the great powers can jointly prohibit the use of LAWS in densely populated areas. Russia’s flagrant violation of IHL in the Russia-Ukraine war casts doubts on whether powerful countries will abide by these rules and norms. Indeed, the presence of norms does not translate into compliance.69 However, the existence of rules and norms makes it possible to distinguish acceptable behavior from unacceptable and provides a basis for collective action against one who crosses a line. Thus, agreed rules and norms can have a deterrent effect on others.70

At the same time, the United States should work with allies to build more granular rules on LAWS. It should facilitate intra-alliance dialogue on the development and use of LAWS. The United States and its allies can bring experts, scholars, and practitioners together to explore possible rules and norms applicable to LAWS as they did for the Tallinn Manual. Building consensus among like-minded countries can be less laborious. The agreed inter-alliance standards could be then scaled up. The United States employed a similar approach in the cyber and space domain. Relatedly, in the latest GGE meeting, the United States and its like-minded allies circulated “Principles and Good Practices on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems.”71 In addition, the United States and its allies should start discussing both the tactical and strategic implications of LAWS. At the tactical level, the allies should identify and explore potential interoperability problems. At the strategic level, the allies should engage in high-level political dialogue on the impacts of LAWS on extended deterrence and regional stability.

As the Biden administration’s National Security Strategy rightly asserts, the United States has led the creation of global institutions, norms, and standards that “advanced America’s economic and geopolitical aims” as well as benefited people around the world.72 Playing its traditional role of norm setter, the United States should take efforts to shape global norms on LAWS in a way that enhances the existing LOAC and bolster strategic stability, so that humanity can avert another “failure of civilizations.”73

About the Author: Kiseok Michael Kang is a second-year M.A. student in the Security Studies Program, concentrating on technology and security. Before coming to Georgetown, Michael served as a foreign service officer at the Ministry of Foreign Affairs of the Republic of Korea.
APPENDIX I

Guiding Principles affirmed by the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System

(a) International humanitarian law continues to apply fully to all weapons systems, including the potential development and use of lethal autonomous weapons systems;
(b) Human responsibility for decisions on the use of weapons systems must be retained since accountability cannot be transferred to machines. This should be considered across the entire life cycle of the weapons system;
(c) Human-machine interaction, which may take various forms and be implemented at various stages of the life cycle of a weapon, should ensure that the potential use of weapons systems based on emerging technologies in the area of lethal autonomous weapons systems is in compliance with applicable international law, in particular IHL. In determining the quality and extent of human-machine interaction, a range of factors should be considered including the operational context and the characteristics and capabilities of the weapons system as a whole;
(d) Accountability for developing, deploying, and using any emerging weapons system in the framework of the CCW must be ensured in accordance with applicable international law, including through the operation of such systems within a responsible chain of human command and control;
(e) In accordance with States’ obligations under international law, in the study, development, acquisition, or adoption of a new weapon, means, or method of warfare, determination must be made whether its employment would, in some or all circumstances, be prohibited by international law;
(f) When developing or acquiring new weapons systems based on emerging technologies in the area of lethal autonomous weapons systems, physical security, appropriate non-physical safeguards (including cyber-security against hacking or data spoofing), the risk of acquisition by terrorist groups, and the risk of proliferation should be considered;
(g) Risk assessments and mitigation measures should be part of the design, development, testing and deployment cycle of emerging technologies in any weapons systems;
(h) Consideration should be given to the use of emerging technologies in the area of lethal autonomous weapons systems in upholding compliance with IHL and other applicable international legal obligations;
(i) In crafting potential policy measures, emerging technologies in the area of lethal autonomous weapons systems should not be anthropomorphized;
(j) Discussions and any potential policy measures taken within the context of the CCW should not hamper progress in or access to peaceful uses of intelligent autonomous technologies;
(k) The CCW offers an appropriate framework for dealing with the issue of emerging technologies in the area of lethal autonomous weapons systems within the context of the objectives and purposes of the Convention, which seeks to strike a balance between military necessity and humanitarian considerations.
APPENDIX II

AI Ethical Guidelines Recommended by Defense Innovation Board

1. Responsible: DoD personnel will exercise appropriate levels of judgment and care, while remaining responsible for the development, deployment, and use of AI capabilities.

2. Equitable: The department will take deliberate steps to minimize unintended bias in AI capabilities.

3. Traceable: The department’s AI capabilities will be developed and deployed so that staffers have an appropriate understanding of the technology, development processes, and operational methods that apply to AI. This includes transparent and auditable methodologies, data sources, and design procedure and documentation.

4. Reliable: The department’s AI capabilities will have explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to testing.

5. Governable. The department will design and engineer AI capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences, and the ability to disengage or deactivate deployed systems that demonstrate unintended behavior.
established since 2004. For outer space, the international space law regime had been

en established since the late 1960s and the U.N. Committee on the Peaceful Uses of Outer Space (COPUOS) has

been one of the main international bodies for emerging space issues.

The preamble of the Hague Convention of 1907 states that “[the] provisions, the wording of which has been

inspired by the desire to diminish the evils of war, as far as military requirements permit, are intended to serve

as a general rule of conduct for the belligerents in their mutual relations and in their relations with the

inhabitants.”


For cyber norms, the U.N. Group of Governmental Experts had been established since 2004. The Convention

on Cybercrime also entered into force in 2004. For outer space, the international space law regime had been

established since the late 1960s and the U.N. Committee on the Peaceful Uses of Outer Space (COPUOS) has

been one of the main international bodies for emerging space issues.

“Background on LAWS in the CCW,” United Nations Office of Disarmament Affairs, accessed November 9,

2022, https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/background-on-laws-
in-the-ccw/

See Appendix I for the complete list of 11 guiding principles.

Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims

of International Armed Conflicts (Protocol I), Geneva, 8 June 1977.

Ibid.

Ibid.

The Martens Clause affirms that “in cases not covered by this Protocol or by other international agreements,
civilians and combatants remain under the protection and authority of the principles of international law derived

from established custom, from the principles of humanity and from the dictates of public conscience.”


weapons-policy-confusion-remains-widespread


The purpose of the Convention, or to affect civilians indiscriminately

See Appendix I for the complete list of 11 guiding principles.

U.S.-Russian Nuclear Arms Control Agreements at a Glance,” Arms Control Association, accessed 17 Jan


autonomous-weapons-systems


Scharre, Army of None, 47.


“Our Policy Position: The Rules We Need To Adopt,” Campaign to Stop Killer Robots, accessed April 2, 2022,

https://www.stopkillerrobots.org/our-policies/


CCW/MSP/2019/CRP.2/Rev.1, https://documents-dds-

ny.un.org/doc/UNDOC/GEN/G19/343/64/PDF/G1934364.pdf?OpenElement

Austria, Belgium, Brazil, Chile, Ireland, Germany, Luxembourg, Mexico, and New Zealand, “Joint

It is noteworthy to mention that drones are fundamentally different from LAWS because they are remotely piloted and thus do not autonomously select or engage targets. According to some estimates, Governments already spend around $11 billion annually on LAWS according to some estimates. See Buchanan and Imbrie, The New Fire, 137.

The current ongoing projects include, but are not limited to, Skyborg (autonomous drone), Orca (underwater), Sea Hunter (surface), and Ripsaw M5 (ground). The system is known as KUB-BLA and it is claimed that the drones are used in its invasion of Ukraine. See https://www.thenationalnews.com/world/uk-news/2022/03/14/russias-kub-bla-kamikaze-drone-intercepted-in-ukraine/.

To illustrate the difference between automation and autonomy, one can compare cruise control and self-driving car. The former helps a driver with a narrow and preprogrammed task such as maintaining speed at a certain level and a driver has to retain control while its vehicle is on cruise control. An autonomous vehicle, on the contrary, can drive itself and respond to various unexpected situations on its own. See Toby McClean, “The Path From Automation To Autonomy Is Swarming With Activity,” Forbes, April 1, 2021. https://www.forbes.com/sites/forbestechcouncil/2021/04/01/the-path-from-automation-to-autonomy-is-swarming-with-activity/
Again, the drone warfare can provide a glimpse into what the future LAWS warfare will look like. Amy Zagart argues that the downing of drones would not spark war as Iran’s shoot down of the Global Hawk did not provoke the U.S. military response. See Amy Zagart, “Drones Don’t Spark War, People Do,” The Atlantic, June 21, 2019.


Chairperson’s Summary,” 79.


Scharre, Army of None, 137.


Scharre, Army of None, 104.

“Chairperson’s Summary,” 19.


This mechanism is called “deterrence by norms.” See Joseph S. Nye, “Deterrence and Disuasion in Cyberspace,” International Security, Vol. 41, No. 3 (Winter 2016/17)


Irregular Conflict, Irregular Harms: Analyzing Patterns of Civilian Harm in the South China Sea

Alisa Laufer

How do China’s irregular warfare tactics affect the security of civilians in the South China Sea? This paper introduces a conceptual framework for understanding two interrelated patterns of civilian harm that occur as a result of Chinese irregular warfare activities: (1) harassment and violence against civilian fishers and (2) the stifling of civilian livelihoods. This analysis herein describes the components of the framework and provides evidence in support of the framework, including local reporting on civilians’ perspectives, literature on China’s strategy, and evidence of China’s presence in the region. The paper concludes by offering recommendations for reducing civilian harm in the South China Sea.

Introduction

The South China Sea (SCS) has long been the site of competing territorial claims, with the first claims being staked in the early nineteenth century by Spanish colonizers at Scarborough Shoal.1 Throughout the succeeding two centuries, regional powers would spend much blood and treasure to control the waters and maritime features of the Sea. Sporadic conflict was not uncommon, even after the passage of the UN Convention on the Law of the Sea (UNCLOS), an international legal regime meant to bring order to global waters.2 However, while conflict is not new to this region, the recent escalation of a new conflict dynamic—China’s use of irregular warfare tactics—has changed the strategic picture of the theater.3

Over the last two decades, China has conducted its SCS operations in the “gray zone”—the competitive space between the conventional binary of war and peace. China has increasingly leveraged irregular methods of coercion and destabilization to expand its control while staying below the threshold of armed conflict. Facing China’s irregular methods, counter-claimant states’ conventional forces struggle to generate proportionate and effective responses to China’s forceful, yet elusive applications of power.4 Many have studied these evolving strategic dynamics and their implications for regional and global security.5 However, few have studied the effects on those who experience China’s irregular tactics day-to-day: the community of fishers local to the SCS.

This paper explores how China’s irregular warfare tactics have affected civilian security and livelihoods in the SCS. I situate my analysis in the nascent literature that explores how patterns of civilian harm differ in irregular versus conventional conflicts.6 This paper adds new insights to the literature by proposing a conceptual framework for understanding how China’s irregular warfare tactics in the South China Sea harm civilians. I argue that Chinese irregular warfare tactics have caused two categories of civilian harm: (1) harassment and violence against civilian fishers and (2) the stifling of civilian livelihoods. The patterns of harm in the SCS differ from those typically associated with conventional conflicts.

This paper proceeds by describing the framework and presenting evidence in support of it, including local reporting on civilians’ perspectives, literature on China’s strategy, and evidence of China’s presence in the region. I rely primarily on evidence from the Philippines, while providing some
additional evidence from Vietnam and Indonesia to illustrate that the patterns described herein are likely broadly applicable to the experience of other claimant states. I also discuss the policy implications of this framework. Finally, I recommend policies for minimizing harm to fishers and the civilian populations that rely on them, in addition to establishing more robust accountability mechanisms for the responsible parties.
Identifying Patterns of Harm

How do China’s irregular warfare tactics in the South China Sea affect civilians in the region? This question engenders a multitude of answers—each civilian has experienced China’s irregular warfare tactics differently at various points in time. While it is impossible to capture every civilian experience, several consistent patterns of harm can be observed in the literature and local reporting that capture, broadly, some of the conflict’s most pervasive effects on civilians.

I propose a conceptual framework to explain the process by which two patterns of harm transpire from China’s irregular warfare tactics in the SCS. The two interrelated patterns of harm explained by this framework are (1) violence and harassment against civilian fishers and (2) the stifling of civilian livelihoods. Figure 1 presents a stylized depiction of the framework, showing how the second pattern of harm (stifled livelihoods) emerges as a result of the first (violence and harassment). The two succeeding sections discuss the two interlocking patterns of harm in greater detail.

Figure 1.

When considering the deterioration of livelihoods, it is important to acknowledge the counterfactual wherein China does not use irregular warfare tactics in the SCS. Even in such circumstances, illegal fishing and overfishing would likely still plague these waters. Indeed, overfishing and illegal fishing are global phenomena, including in regions where there is no reported Chinese presence. In addition to exploitative fishing, climate change also contributes to the degradation of the health and abundance of fish stocks. Thus, this framework does not suggest that China’s irregular warfare tactics are the sole cause of civilian harm associated with fish stock scarcity in the SCS. Instead, this framework suggests that China’s gray zone activities compound fish scarcity by placing civilians in the middle of the conflict against armed maritime militia vessels. A Filipino fisher describes his on-the-ground experience facing the overwhelming force of China’s maritime militia by asking: “What can small fishermen like us do?... We can complain all we want, but the enemy is powerful, so we try to survive another day and just fish.”

This power asymmetry gives civilian fishers less bargaining power to enforce their rights (i.e., their fishing rights as defined in UNCLOS and national legislation along with their human rights) and provide
vital resources for their communities in an already scarce environment. There have been attempts by regional governments to better regulate fishing in their own waters, but fishers and enforcement officials have little power in upholding these regulations in the face of China’s maritime militia. Thus, this framework suggests that China accelerates the scarcity problem—and thus exacerbates the degradation of livelihoods—by leveraging asymmetric irregular warfare tactics in the SCS.

Pattern One: Violence and Harassment

The process described by the framework begins with an ambiguous assertion of territorial control by the People’s Republic of China (PRC) (Step 1). The PRC expresses these assertions either at a strategic level through policy changes or at a tactical level in-theater. One example of this stage of the framework is the PRC’s announcement of its nine-dash line in 2009. That the PRC drew dashes instead of contiguous border points to its intentionally ambiguous strategy. It is not clear whether the “line” conveys China’s conceptualization of its sovereign maritime rights to fishing and other natural resources, or if it depicts absolute Chinese sovereignty and domestic jurisdiction over the maritime area. Some Chinese legal scholars have argued that the nine-dash line reflects Chinese sovereignty, but the PRC has never stated so explicitly. In response to a 2016 Arbitral Tribunal case at The Hague that disputed China’s claims to “historic rights” in the SCS, the PRC rejected the Tribunal’s jurisdiction over the case without addressing its substance. Even after the Tribunal’s ruling officially rejected China’s claims, the PRC denounced the ruling without providing a precise definition of its claims to counter the verdict. By leaving territorial claims open to further interpretation, the PRC gave itself latitude to adjust its claims as needed.

The PRC’s maritime militia fleets serve as another example of the PRC’s equivocal territorial assertions. The PRC has built a large portion of its militia by providing subsidies for commercial fishing vessels to fish in “specially designated waters,” in support of political objectives. The commercial nature of the militia allows the PRC to expand the PRC’s physical presence without officially involving its armed forces. China first deployed its fishing militias to support the 1974 operation to seize the western Paracel Islands in the SCS from Vietnam. China also urged vessels to maintain a presence around the Spratly Islands beginning in the 1980s, with Chinese fishing activities around Scarborough Shoal increasing substantially in the late 1990s. Since the early 2000s, the PRC has deployed the fishing militia to support a variety of operations such as harassing oil and gas operations in other claimants’ waters, helping “protect” Chinese oil rigs in disputed waters, congregating around Chinese land reclamation projects, and seizing maritime features (most notably, Scarborough Shoal from the Philippines in 2012). That these vessels are neither entirely civilian nor military in character underscores the ambiguity of their legal status and purpose as the vessels approach contested areas.

Once the PRC has made an ambiguous claim to new territory, a set of vague and untested rules emerges (Step 2). In contrast to a conventional military victory, there are no clear winners nor losers when the Chinese maritime militia patrols new regions of the Sea—nor is there a formal, public declaration of control. Similarly, given its equivocal borders, the
nine-dash line does not send clear signals on where fishers can expect to face confrontation from PRC-supported vessels.

At this stage of the framework, fishers continue to traverse the seas.† Faced with new, but loosely defined rules, some vessels cross into territory the PRC views as its own (Step 3). Once fishers begin testing these new rules, the first pattern of harm emerges: Chinese vessels increase violence and harassment against counter-claimant vessels (Step 4). A June 2019 ship-ramming incident illustrates this stage of the framework. At Reed Bank in the Spratlys, a Chinese fishing boat struck a Philippine fishing boat and promptly sailed away with its signal lights off as the Philippine ship sank and its crew struggled to stay afloat. This occurred shortly after China had built up a presence of over two hundred suspected militia vessels around nearby Thitu Island.16

In addition to ship ramming, the Chinese maritime militia has used tactics such as swarming, water cannon attacks, and dangerous maneuvering to repel counter-claimants’ vessels in the Spratly Islands. In 2014, for example, Filipino fishers described being attacked with water cannons as they tried to approach Scarborough Shoal.17 In 2021, hundreds of militia vessels swarmed around Whitsun Reef and Thitu Island (again) with the alleged purpose of intimidating Filipino and Vietnamese fishers.18 In 2022, the militia pushed deep into the Philippines’ EEZ as vessels swarmed Sabina Shoal and the allegedly oil-rich Iroquois Reef.19

The militia has also used irregular tactics to assert the PRC’s control in the SCS’s Paracel Islands. In 2014, Chinese militia vessels supported operations to place an oil rig south of the Paracels. The militia encircled the rig and would attack Vietnamese ships with water cannons and ship ramming when they approached.20 More recently, in March 2019, a Chinese vessel rammed and capsized a Vietnamese fishing boat near Discovery Reef.21

There have been many other documented cases wherein the maritime militia or the Chinese coast guard harass counter-claimant vessels traversing areas of the Sea that the PRC views as its own.22 However, it is important to consider that many “warning shot” harassment cases may go unreported if they do not escalate to or involve physical violence. These cases are nonetheless meaningful when measuring civilian harm given (1) the potential psychological effects of intimidation and (2) these cases’ effects on civilian livelihoods, as I discuss in the succeeding section.

Additionally, some cases may go unreported given the incentives that government officials in counter-claimant states might have to appease the PRC by suppressing media coverage of Chinese harassment. Philippine President Rodrigo Duterte—a leader known for warming ties with China—downplayed China’s role in the Reed Bank incident, dismissing it as “a little maritime accident.”23 Given the Duterte administration’s broader reputation for being hostile to journalists who went against the government’s message, it is likely that many journalists refrained from reporting on other incidents during his tenure.24 Additionally, Vietnamese fishing vessels and the government in Hanoi have reportedly kept the media from reporting on cases of Chinese harassment and ship ramming in the interest of smoothing bilateral ties with

---

† In some cases, counter-claimant states’ coast guard vessels test the PRC’s new rules instead of civilian vessels. While coast guard vessels may similarly face harassment by Chinese vessels, given the scope of this paper, we focus on incidents involving civilian vessels. However, it should be noted that even when other coast guard vessels face harassment or violence from Chinese coast guard or militia vessels, the “new rules” may similarly harden, which can have the same long-term result for civilians: the stifling of their livelihoods.
China. Many Indonesian officials have also been wary of reporting incursions of Chinese vessels in their waters, recognizing the need to appease their largest trading partner. Given China’s leverage over counter-claimant states, the effect of harassment and violence against civilians is unlikely to be captured in full by public information sources. These political dynamics ultimately further China’s irregular tactics by obscuring information about the causes and outcomes of harassment. Without reporting, information about these “below the threshold” incidents that happen far out at sea may not reach the general population.

**Pattern Two: Stifled Livelihoods**

After one or several such incidents unfold in a particular region in the SCS, the PRC’s new rules for the area are clarified (Step 5). With a better understanding of the rules and consequences of crossing into PRC-controlled territory, commercial fishers from the counter-claimant states avoid traversing the area. The framework now considers rules “hardened” and fishers begin adapting to the new status quo. This period is associated with a reduction in violence and harassment given that commercial fishers adjust their patterns of life to avoid confrontation with the Chinese coast guard (Step 6).

The PRC’s recent imposition of a recurring fishing ban during the summer season in a large portion of the SCS and the reaction from local fishers illustrates this stage of the framework. This ban was ambiguous given that under international law, China lacked the authority to impose it—the territory in question fell inside the Philippines’ exclusive economic zone (EEZ). The government of the Philippines advised its fishers to disregard the PRC’s ban, but fishers have reported that they have no choice but to obey due to the heavy presence of Chinese vessels in the region. Fishers reported diverting to other areas that lacked a presence of Chinese vessels but also lacked abundant fish. Fishers also report being fearful of fishing in Scarborough Shoal after the Philippine government similarly stated that China’s fishing ban there should be disregarded.

Indonesian fishers have also reported diverting from the Natuna Islands, which fall within Indonesia’s EEZ in the southernmost portion of the South China Sea due to the illegal presence of Chinese fishing vessels closely followed by Chinese coast guard vessels. Vietnamese fishers have similarly been “chased away” by Chinese fishing vessels several times larger than their small wooden boats and flanked by Chinese coast guard vessels.

Adaptation by fishers to the new rules gives rise to the second pattern of harm identified by this framework: the stifling of civilian livelihoods (Step 7). Under the new rules, fishers no longer access the fish stocks that they used to, including some within their country’s EEZ. Especially where the new rules prohibit access within an EEZ, a country’s finite resource pool has categorically shrunk, thereby limiting the available catch and stifling fishers’ income.

The loss of income can be observed across counter-claimant states. Philippine fishers from towns nearby Scarborough Shoal report having lost approximately 70% of their income due to China’s burgeoning

---

‡ The fishing ban is imposed in the SCS waters north of the 12 degrees north latitude line; see “Vietnam Protests as China Declares Annual South China Sea Fishing Ban.”

§ For example, Scarborough Shoal was seized by China in 2012, in spite of the fact that the shoal falls within 200 nautical miles of the Philippine Island Luzon, meaning it falls within The Philippines’ EEZ under international law.
In many coastal communities in Western Luzon, fishing has long been the dominant industry and there are few alternative employment opportunities for displaced fishers. As such, the impact of Scarborough Shoal’s closure has had devastating impacts on Filipino families; some fishers’ spouses and children have been forced to adapt by seeking employment overseas as domestic laborers. In Vietnam, some provincial governments provided loans for fishers to build steel-hulled ships for offshore fishing given the depletion of coastal fish stocks. However, many have struggled to pay back their loans given the inability to make a profit further out at sea due to harassment and overfishing by Chinese vessels. In Quang Ngai province, 80 percent of steel-hulled ships built through the loan program went bankrupt as of 2022. Anecdotal evidence also suggests that Indonesian fishers in the Natunas have experienced staggering drops in their catch as a result of the growing Chinese presence there. In sum, China’s irregular warfare tactics effectively function as an exogenous negative supply shock to the market, which limits the supply of fish available for fishers to catch and sell. The shock seems to have a devastating economic effect on fishers and their families. However, it is important to recognize the full extent of damage is unknown because of the dearth of data collection in remote coastal regions.

The denial of access to fish stocks compounds an already competitive fishing market in the region; as early as 2012, the majority of stocks in SCS-adjacent countries had been overfished. While all claimants bear some responsibility for declining fish stocks, China has the largest commercial fishing fleet in the world by far and Chinese vessels account for the preponderance of illegal, unreported, and unregulated fishing in the region. Ground-level accounts confirm the pervasiveness of Chinese overfishing; Philippine fishers along the Luzon coast report that overfishing by Chinese boats in their waters has led to a steep drop in their catch. Furthermore, demand for fish stocks in the region has been proven to rise as supply falls and thus the denial of access to fish stocks by Chinese militia and coast guard fleets exacerbates overfishing by all players in the region—not just China. This exogenous shock to overfishing further stifles livelihoods in the long term given its effects on future income. The shock compounds overfishing trends that pre-dated China’s use of irregular warfare tactics and thus requires an upward modification of existing projections for the loss of future income resulting from overfishing.

Independent of supply issues and lost future income, the denial of access to fish stocks by Chinese vessels can also drive up the price of fish due to higher input costs for fishing. If the new rules require fishers to travel further or along less direct paths to access fish stocks, the marginal cost of each fish increases. This is because fishers spend more time, labor, and fuel accessing the harder-to-reach stocks. Additionally, if stocks have been overfished by an overwhelming presence of fishing militia vessels, the stocks will be less dense and fishers must therefore exert more effort to find and catch each fish. Eventually, the higher cost of doing business may be passed onto consumers, thereby raising consumer prices for a staple protein for many regional fishers.

** See Gutierrez, who writes, “A survey by Pamalakaya, a group that fights for fishermen’s rights, estimates that fishermen from Masinloc and nearby towns have lost about 70 percent of their income because they no longer have access to Scarborough Shoal.”
The scarcity and higher costs of fish contribute to a burgeoning food insecurity problem that already affects many of the poorest and most vulnerable communities of the region.\textsuperscript{43} Exacerbating the direct effects on fishers’ livelihoods and the elevated price of protein, the negative supply shock (and corresponding increase in fishing competition) triggers additional cascading effects on civilian security. In particular, some fishing enterprises in the region have turned to child labor and coercive labor practices to cut input costs and adjust to the higher marginal cost of production in the fishing market. For example, Vietnam’s fishing industry has relied on child labor as fishers’ catch has dropped as a result of heightened competition for fish.\textsuperscript{44} Additionally, some Vietnamese fishers are now paid according to the quantity of their catch, which has amounted to unlivable wages due to the depletion of fish stocks. Given these circumstances, vessel owners have begun lending fishers money to support their families, thereby entrapping fishers into debt bondage,\textsuperscript{45} which is a known indicator of forced labor.\textsuperscript{46} Additionally, China’s irregular tactics force small-scale fishers to traverse dangerous waters due to restricted access to fish stocks. When fishers cannot access their stocks due to Chinese militia vessels denying access or fishing exploitatively, they may adapt by pursuing harder-to-reach stocks. Although specific cases in the South China Sea are difficult to confirm given data limitations associated with small-scale fishing, fishers have reported traveling further out as their access to fish declines closer to coastlines.\textsuperscript{47} A well-documented case in the waters between North Korea, South Korea, Japan, and Russia illustrates the types of harm that may also occur in the SCS as a result of heightened economic competition and restricted access to fish stocks.\textsuperscript{48} A fleet of fishing vessels owned and operated by Chinese interests has expanded its presence in North Korean waters to exploit squid stocks. Evidence from satellite data and qualitative local knowledge confirms that, as a result of displacement by the Chinese vessels, small-scale wooden North Korean vessels began fishing illegally in Russian waters. These artisanal North Korean boats are severely underequipped for the long journey to Russian waters; between 2014 and 2018, 505 North Korean boats washed ashore on Japanese coasts.\textsuperscript{49} Local Japanese media reports confirm that these incidents frequently caused starvation and deaths. As a result, many fishing villages on the eastern coast of North Korea are now deemed widows’ villages. The dangers of long-distance travel for small-scale fishers have been well-documented on a global scale.\textsuperscript{50} As fishers from counter-claimant states adapt to the PRC’s irregular tactics, they may similarly suffer lethal consequences.

\textbf{Implications of the Framework}

This framework captures two patterns of civilian harm by tracing the arch through which the PRC’s irregular warfare tactics influence fishers’ patterns of life. While this framework does not explain all

\textsuperscript{44} Some may argue that in such scenarios, government subsidies are an easy fix for maintaining a low consumer price. While government subsidies may temporarily stabilize fish prices, many kinds of fishing subsidies have been proven to reduce overall economic welfare (see Sakai, Yagi, and Sumaila, “Fishery Subsidies.” pp. 444-445)

On the centrality of fish to the local diet, see, for example, see p. 58 in Department of Science and Technology – Food and Nutrition Research Institute, “Philippine Nutrition Facts and Figures,” which finds that of 2019, seafood accounts for 42.2% of total animal protein intake in the Philippines. This statistic has declined over time as consumers have had to adapt to scarcer catches.
incidents of civilian harm caused by the PRC in the SCS—and while some of the PRC’s irregular warfare tactics may not directly harm civilians—this framework can help clarify how civilian harm in irregular conflict tends to differ from that of conventional conflict. By acknowledging these unique patterns of harm, policymakers can better understand how civilians experience the conflict and thus better address their grievances and prevent future harm.

The number of casualties caused by China’s irregular warfare tactics in the SCS is far fewer than what we would expect to see if China used conventional force to clear the Sea of non-Chinese vessels. Instead, per the framework, Chinese gray zone operations cause a limited number of violence and harassment incidents in a particular region, followed by a reduction in violence due to China’s asymmetric power over counter-claimants’ commercial fishers.

Unlike brute force—which would cause immediate and tangible harm to civilians—the PRC’s irregular warfare tactics degrade civilians’ security and livelihoods through more elusive and gradual means. The erosion of civilian livelihoods occurs over the course of many years. The effects on civilians are difficult to measure; they cannot be fully captured through conventional methods such as counting civilian casualties or assessing damage to civilian infrastructure. Furthermore, there are significant limitations to data sources that could, in theory, help trace the causal impact of the PRC’s irregular warfare tactics on civilian livelihoods and security. First, catch statistics are severely underreported throughout the region, making it hard to identify the relative gains and losses of different populations. Additionally, there are limitations to remote sensing technology that could be used to measure changes in the behavior of civilian vessels in response to China’s maritime militia presence. Given the subtle nature of civilian harm and the limitations of the available data, it is difficult to know the full extent of damage suffered by civilians in this irregular conflict.

The subtle nature of harm endured by civilians also makes it difficult to empirically prove the attribution of civilian harm to the PRC. While qualitative analysis of China’s strategy and intent make clear that its irregular warfare tactics dramatically alter civilian fishers’ and consumers’ patterns of life, it is hard to isolate the effects on civilians caused specifically by China. China is not the only country that exploits fisheries in the region, and thus not all of the scarcity issues and related security

‡‡ See Sumaila and W.L. Cheung pp. 3-4, which explains, “Incorporating estimated unreported catches would increase total catches to 16.6 million t in 2010; overall, estimated unreported catches from the SCS averaged about 8.1 million annually from 2000-2010.” In other words, “unreported catches would increase total catches statistics by nearly 70%”

§§ For an analysis of how China’s irregular warfare tactics are part of a larger strategy to guarantee China’s exclusive access to resources in the SCS, see Martinson, “Catching Sovereignty Fish.” Also see Chubb, who claims that as of 2007, the PRC adopted, “new domestic legal-administrative structures, organizational systems, and maritime law enforcement capabilities designed to extend wide-ranging state administrative authority over the maritime spaces around China’s periphery.” Also see Grossman and Ma, “A Short History of China’s Fishing Militia,” which explains how the maritime militia establishes a de facto Chinese operating presence in disputed areas, effectively changing the facts to challenge counter-claimants’ ability to maintain control over disputed features. They argue China’s strategy is to, “‘win without fighting’ by overwhelming the adversary with swarms of fishing vessels usually bolstered from the rear together with the China Coast Guard (CCG), and possibly PLAN ships, depending on the contingency, in escalatory concentric rings.”
challenges are attributable to the PRC.*** Opposing forces may therefore struggle to build a case against China for its specific impact on civilian livelihoods and security. Although all signs point to the PRC’s irregular warfare tactics as a leading cause of overfishing and damage to civilian livelihoods, China has strategically deployed these tactics in an equivocal manner to evade accountability.

**Recommendations**

The framework herein describes patterns of civilian harm that are new and unfamiliar to policymakers and implementers accustomed to working within the construct of conventional conflicts. Typical methods for civilian harm prevention, attribution, and accountability are unlikely to be effective in this context. This section, therefore, describes policy recommendations that will help facilitate two important outcomes: prevention and mitigation of civilian harm and stronger accountability for the relevant parties.

*Establish and Exercise Coast Guard SOPs for Testing New Rules*

To prevent more confrontations that could harm civilians, the counter-claimant states should establish standard operating procedures (SOPs) for coast guard vessels to test “new rules” after new ambiguous assertions of territory by China. These SOPs should establish processes for coast guards to respond to civilian reports of suspicious PRC activity. These SOPs should be designed such that coast guard operations are merely testing the waters, not provoking conflict with militia vessels. These procedures can help pass the burden of the “test” from civilian vessels to coast guard vessels that are better equipped to defend themselves in the face of harassment or violence.

In areas where counter-claimants’ EEZs overlap, the relevant parties should write joint SOPs for testing China’s new claims. Concerned international partners such as the United States can facilitate workshops to help counter-claimant states write these SOPs intending to foster greater collaboration among them. The counter-claimant states should also jointly exercise this capability to ensure a smooth and collaborative response to reports of new territorial assertions by China. These exercises will improve counter-claimant states’ coordination capacity in addition to presenting a united front to China.

There are two major implementation barriers to consider with regard to this recommendation: (1) the will of claimant states to participate and (2) China’s reaction to the exercises and eventual operations. It is possible that China will perceive the exercises as escalatory and as such, counter-claimant states may be shy to participate. Given these dynamics, counter-claimants should be mindful of the public messaging they use when drafting, exercising, and implementing the SOPs. Counter-claimants should emphasize the humanitarian nature of the activity and ensure the exercises are not co-opted by other interests.

*Establish Independent Claims Commission for Victims of Harassment and Violence at Sea*

To fully capture the extent of harassment and violence experienced by fishers in the SCS, it is critical to establish better monitoring and documentation of civilian harm. Local NGOs and fishers’ advocacy organizations should therefore

---

*** While illegal, unreported, and unregulated (IUU) fishing is difficult to track, there is evidence that other claimants’ fleets have engaged in IUU fishing. For a case of IUU concealment by Malaysia, for example, see Sumaila p. 9
collaborate to establish an independent commission to which fishers can report incidents of harassment and violence at sea. This commission must maintain independence from the regional governments so that fishers do not fear retributive action for reporting incidents that may strain their country’s relations with China.

This commission should share anonymized data on the incidents with the public. This information will help policymakers, scholars, and fishers better understand the threat China poses. This data can provide further insights into where China’s maritime militia has the strongest effect. These insights can be merged with remote sensing data and economic data to corroborate the impact of militia presence on variables such as fish prices and nutrition in nearby regions. The synthesis of this information can also be used to help predict the most dangerous and likely scenarios for fishers, thus providing an opportunity for policymakers and fishers to develop better security and self-protection measures.

The establishment of the commission also provides an opportunity for involvement by countries interested in facilitating greater transparency in the SCS. NGOs should solicit funding for the commission from governments concerned with security in the region. The United States and other nations may wish to fund this effort as a means of promoting a rules-based order in the SCS without directly involving themselves in an escalatory manner.

Increase Awareness Among Fishers of Their Rights

Fishers are among the poorest and most vulnerable populations in many counter-claimant states. With limited access to education, many fishers may not understand their rights at sea. Further, local governments’ suppression of reporting about violence against fishers may further convolute fishers’ understanding of their rights.

It is critical that fishers have a clear understanding of their rights so they can better advocate for their own needs. If fishers understand their rights, they will be more capable of reporting suspicious activity at sea to the relevant authorities in their government. Greater awareness is also necessary for a claims commission to succeed as a data-gathering mechanism. If fishers are unaware of their rights, they will be unable to report violations.

NGOs and local advocacy organizations should work directly with fishing communities to increase awareness. This awareness campaign should include training on how to spot early signs of illegal territorial assertions and illegal fishing. Training should also provide fishers with information on how to report territorial violations to government authorities and information on reporting harassment and violence to the claims commission.

Similar to the previous recommendations, this awareness campaign should be supported by international partners with interests in maintaining security and a rules-based order in the SCS. This provides another opportunity for the United States and other concerned governments to advance their interests and support local voices in the region without directly confronting China.

Conclusion

The conflict in the SCS serves as one case among a growing body of cases that illustrate new patterns of civilian harm present in irregular and gray zone conflict. For policymakers to be effective in protecting civilians in these environments, it is critical that they understand how patterns
of harm manifest uniquely in each irregular conflict. Addressing civilian harm in the SCS can be a unifying issue for counterclaimant states, as it can help illuminate the common struggle they share. Additionally, by establishing more robust mechanisms to monitor and address civilian harm, counterclaimant states will have more evidence that can be used to hold the PRC to account. Finally, many efforts to improve monitoring and responses to civilian harm provide opportunities for global support. Global involvement in this issue can help give greater attention and resources to the protection of civilians, while simultaneously imposing reputational costs on the PRC.

About the Author: Alisa Laufer is a Master of Public Affairs candidate in International Relations at Princeton University, where she studies the evolving nature of conflict. Prior to Princeton, Alisa worked in support of the U.S. Department of State. The views expressed in this article are her own and do not necessarily reflect those of the U.S. government.
4 The term, “counter-claimant states” refers to the governments of Brunei, Indonesia, Malaysia, the Philippines, Taiwan, and Vietnam
13 台山政府网 [Taishan Government Network], “台山市海洋与渔业局召开广海镇特定水域渔船管理工作会议 [Taishan Ocean and Fisheries Bureau Holds Meeting on the Management of Guanghai Town Special-Waters Fishing Vessels].”
15 Ibid, pp. 3-11
18 Jason Gutierrez, “Philippines Accuses Chinese Vessel of Sinking Fishing Boat in Disputed Waters.”


Beech and Suhartono, “China Chases Indonesia’s Fishing Fleets, Staking Claim to Sea’s Riches.”


Ibid

Gutierrez, “Overwhelmed by Chinese Fleets, Filipino Fishermen ‘Protest and Adapt.’”

Beech and Suhartono, “China Chases Indonesia’s Fishing Fleets, Staking Claim to Sea’s Riches.”


Beech and Suhartono, “China Chases Indonesia’s Fishing Fleets, Staking Claim to Sea’s Riches.”

Whaley, “A Leviathan Turns Philippine Fishermen Into Desperate Darters.”


38 Gutierrez, “Overwhelmed by Chinese Fleets, Filipino Fishermen ‘Protest and Adapt’.”

39 Sumaila and W. L. Cheung, “Boom or Bust: The Future of Fish in the South China Sea,” p. 9

40 For current projections, see ibid, p. 7


42 Ibid


45 Ibid pp. 24-25


47 Basu, “In Deep Water.” p.6


49 Ibid (see “Supplementary Materials”)


Technology Companies as Emerging Superpowers: A Brazil Case Study on the Competition Between American and Chinese Technology Companies for Global Influence

Ona Spreenberg

Technology companies are accumulating power as the developers and providers of emerging technologies, projecting it abroad through their pertinent development strategies. Through a Brazil case study, this paper demonstrates that U.S. and Chinese cloud providers, the largest procurers of cloud services, are already entrenching themselves abroad and servicing emerging economies by exerting state-like capabilities. Firstly, they are laying the infrastructure to operate their products and services, creating a technological and infrastructure dependence in the receiving state. Secondly, they are expanding infrastructure by creating networks of citizens who rely on the platforms to build successful businesses and grow alliances by providing training on their specific platform rather than generalist training. U.S. and Chinese technology companies’ fierce competition has constructed a game of three players, where the PRC and the Chinese technology companies operate as one while they compete against U.S. technology companies and the U.S. government as different entities. The Brazil case study demonstrates that the United States government stands a chance at competing against the PRC’s proposed national security plan in developing countries by forging a stronger relationship with the U.S. private sector. The United States will need to strengthen its competitive technology edge by partnering with technology companies to lay out infrastructure and offer alternatives and more economical solutions while harnessing the power of technology to improve the democratic process to compete against Chinese development practices. Either the United States government adapts, integrates, and accepts the changes brought about by technology or it will cease to remain a leader in global technological innovation and development.

Introduction

The convergence of digital technologies is creating a fourth industrial revolution that is transforming how industries and states operate. No industry is more globalized than the technology industry. It harnesses the power to shape interactions between states, including competition between great powers.

In 2010, digital technologies for public consumption, such as online platforms, mobile devices, and apps, matured into powerful new global industries capable of disrupting national economic structures. At that time, the most globally successful technology companies were in the United States. China boiled at the entrenchment and extension of U.S. influence and developed a national security strategy to keep up with U.S. technological dominance. In the late 2010s, emerging technologies like 5G and cloud computing hit the public sphere. These innovations were said to be more transformative technologies, but China simultaneously emerged as a competitor to U.S. capabilities. The United States realized that technology became a critical arena for great power competition that could not simply be left to the marketplace. Varying degrees of state support have made it so that technology firms have transformed into international players in and of themselves, wielding unprecedented economic power through influencing innovation and development.

This paper seeks to expose the depth and breadth of technology companies’ capacity and influence. Technology companies are accumulating power like states, which has implications for great power competition. This paper will start by delving into the existing literature on the
structures that allow U.S. and Chinese technology companies to amass economic, political, and innovative power. It will then identify strategies, previously relegated to states, that these technology companies utilize to enter new markets. An analysis of competing U.S. and Chinese firms offering cloud computing in the Brazilian market will follow to demonstrate their influence in receiving countries. Finally, it will conclude by determining the future of nation-states by focusing on ways states can partner with technology companies to enhance services and democratic governance.

Literature Review

Technology Companies Stockpiling Power: Economic, Technological, and Political Capacity

Traditional approaches to estimating power in the international system often focus on measuring the resources and capabilities of states. However, most expressions of national power and influence result from interactions between states across economic dimensions. These frameworks of state power fail to consider technology companies as autonomous players in the economic dimension. Technology companies operate as semi-independent actors, under varying degrees of state control, shaping the arena where great power competition between the United States and China unfolds.

The concept of great power competition describes how powerful governments compete with one another for supremacy in the defense, economic, or both realms, within anarchic systems. By excluding technology companies as players in great power competition, academics and policymakers overlook the capabilities technology companies exert in geopolitics. Although an emerging body of literature explores how China’s national security approach to technology presents a threat to the U.S.-led rules-based international order, limited explicit comparisons in international relations have been made between U.S. and Chinese technology companies’ competition in emerging markets.

Before delving into the power technology companies have accumulated, it is worth establishing the definition of a technology company. This paper will refer to technology companies as a business that operates on the frontier of economy and science in the high technology sector and manufactures high technology items. These companies conduct market research, invest in innovation, and support development activity globally. In addition, they use a large extent of modern information technology and remain open to cooperation with other organizations and government entities by creating various network connections. The technology companies mentioned in this paper constitute businesses that sell innovative digital technical services, products, platforms, or hardware that influence state development and the economy. Through the products and services they sell, technology companies have been accruing economic, technical, and political power, in some cases at more significant rates than nation-states.

Technology Companies’ Economic Power

Technology firms comprise a quarter of the global stock market. Visual Capitalist illustrates the economic power technology companies wield by comparing the market capitalization of multiple technology giants to countries’ annual Gross Domestic Product (GDP). Below is a visualization (Figure 1) comparing Microsoft’s market capitalization to several countries’ GDPs. Based on GDP, if Microsoft were a nation-state, it would rank as the 10th richest country in the world, surpassing global powerhouses like Brazil, Canada, Russia, and South Korea. This visualization illustrates how technology companies’ substantive growth compares to state economic power.
Geographically, U.S. and Chinese firms account for 76 of the world’s 100 most valuable firms. *The Economist* captures the dominance of U.S. and Chinese firms by comparing their share of world output with their share of business activity. U.S. companies account for 24% of global GDP and 48% of business activity, while Chinese companies account for 18% of GDP and 20% of business activity globally.⁹ Economically and commercially, both U.S. and Chinese technology companies yield enormous influence in their mastery and ownership of innovative digital technologies.

*Sources of Technical Supremacy*

Technology companies’ accumulation of economic power and influence stems from the business models that they rely on. Technology companies rely on a platform business model connecting suppliers to consumers, creating what is known as the network effect. A platform business is a business model that focuses on helping to facilitate interactions between a large number of participants. The role of the platform business is to provide a governance structure and a set of standards and protocols that facilitate interactions at scale so that network effects can be unleashed.¹⁰ The platform business model does not own the means of production but rather creates and facilitates the means of connection. Therefore, platform businesses benefit from the network effect; the more consumers they acquire, the more appealing they are to suppliers, leading to a zero-sum game where the winner takes all.¹¹ Technology companies are creating a global network of users that blurs nation-state lines with the potential to create online communities that threaten the function of the nation-state.

By providing convenience, technology companies have developed a business model that relies on consumption and creates a tacit alliance with consumers.¹² Consumers can be individuals who use search engines or smartphone software or whole industries, like the finance and energy sectors, which rely on its technologies to facilitate the delivery of their products.¹³ Consumers, by using technology companies’ platforms and services, are generating data...
that explains how they behave and operate. Technology companies then capitalize on the data flows going through their IT infrastructures by either improving their products and services or selling them to third-party vendors.

The platform business model is scalable, allowing technology companies to use their infrastructure, reach, and data assets to enter and disrupt new markets. As masters of the dominant platforms, U.S. and Chinese technology companies design the models of operation in their interests and impose them on other actors. The major U.S. and China-based technology firms have become vast, multinational, digital-physical enterprises with complex loyalties and their own foreign policies.

*The Power of Innovation: The Private-Public Convergence*

As the largest procurers of digital technology, U.S. and Chinese technology companies harness control over the economic and political webs upon which they expand. This is particularly concerning because technology systems have become the infrastructure on which economic, social, and political processes occur. Technology giants design and operate technology systems, which gives them considerable power and influence. In addition, where technology companies are headquartered (usually determined by where they first emerged as start-ups) influences the values and the norms they follow. However, U.S. and Chinese technology companies’ management of digital technologies run the risk of being directed by their respective governments. Respective governments determine how technology companies operate, and whether they support them economically and politically. The PRC’s financial support of its technology companies allows these enterprises to exert robust capabilities in the global markets beyond what these technology companies can accomplish by themselves. In comparison, the United States government minimally supports U.S. private enterprises in developing new capabilities and competing in global markets.

The lack of U.S. government funding for technological innovation in the United States leaves the private sector dominating technology R&D, relinquishing the development of technologies for public consumption to technology companies. For example, the *American Association for the Advancement of Science* report noted a 68% decline in R&D expenditures as a percentage of the U.S. federal budget from 1962 to 2017. Currently, venture capital plays a disproportionate role in financing innovation for start-ups. The U.S. venture capital industry is highly concentrated, with the top 5% of investors accounting for 50% of the capital raised. Funneling innovation through venture capital firms makes it so that only a select few start-ups that develop technology hit the market. This trend yields decision power to venture capital firms which can determine what innovations are worth pursuing based on the start-up’s possibility of generating a return on investment, potentially missing out on technologies that can bring global good.

On the other hand, the People’s Republic of China (PRC) blurs the lines between the public and private sectors. The PRC and the private sector work closely together to develop information technology (IT) infrastructure and deploy new technological innovations. In exchange, the PRC leverages Chinese companies to funnel to PRC authorities the data that flows within IT infrastructures upon request. Chinese technology researchers and companies operate in an environment where the state is free to direct, subsidize, and coerce private sector support for official government priorities and policies. Such practices have
raised concern over the security and privacy of Chinese technology companies’ IT infrastructure in emerging markets globally. For example, the PRC has been pushing to expand its 5G networks in Chile using a third-party provider, Wom S.A. Wom, a subsidiary of the British company Novator Partners LLP, and has been recognized as acting on behalf of Huawei. Wom now controls about 23% of the Chilean telecommunications market, which can be attributed to the fact that from 2015 to 2019, the China Development Bank extended $415 million in loans to Wom. The loans require Wom to grant Huawei preferred network partnerships. The interoperability between the PRC and Chinese enterprises provides Chinese technology companies with a competitive advantage in global markets.

The PRC presents a united front in the international system and flaunts Chinese technology companies’ innovations as their own, while the United States’ laissez-faire approach allows the private sector to drive innovation. The United States government frequently fails to collaborate with the private sector, both domestically and abroad. However, the United States could improve the delivery of public services and enhance democratic governance by leveraging technology companies’ innovations to strengthen its capacity-building efforts. By working closely with technology companies to improve these functions, the U.S. government and technology companies can coexist and contribute to innovative applications of technology.

Projecting Power Abroad: Capabilities and Strategies in Competition

All major technology companies compete in every major market around the world. Out of the 19 technology firms worth over $100 billion created in the past 25 years, nine are in the United States, and eight are in China. U.S. and Chinese companies’ market dominance translates into competition for market share abroad. Technology companies employ international talent that develop their products and services, wielding international power. The power of innovation then becomes a tool for development in new markets. When entering underdeveloped new markets, technology companies not only need to deploy products and services but also need to build IT infrastructure. Therefore, technology companies accumulate an expanding global presence and a growing list of transnational corporate interests that directly influence and are influenced by geopolitical events.

The least developed countries often remain far behind in receiving the economic and social benefits of technological innovation, mainly due to infrastructure limitations. Developing nations’ low levels of investment in R&D, limited supply of skilled labor, and inadequate regulatory environments all play a role in the poor state of science, technology, and innovation. The United Nations notes that traditional development assumptions that increasing imports of capital goods and direct foreign investment would lead, through the diffusion of technology and innovation, to development gains, have not worked out to the extent predicted. A lack of technology development forces technology companies to venture into new markets to build infrastructure before deploying their products and services abroad.

When U.S. and Chinese technology companies venture into new markets, they ought to supply the receiving state with physical infrastructure and develop legal, financial, and educational frameworks to deploy their product and services. However, these companies are more than just players in the game of global politics; they are often the arena itself. U.S. and Chinese technology companies’ strategies to expand outside their native markets can also be packaged into U.S. and PRC foreign policy.
strategies. Technology companies’ strategies for projecting power abroad are influenced by how states compete across economic dimensions. Two competing national security strategies guide how U.S. and Chinese technology companies interact with foreign governments. The PRC has explicitly integrated Chinese technology companies into their development plans to leverage them for great power competition, while the United States has not done the same.

The PRC has made the information contest a key part of its national security strategy, prioritizing both cyberspace and the information space. In 2013 the PRC adopted the Belt and Road Initiative (BRI), a global infrastructure and investment development strategy. Within BRI lives the Digital Silk Road (DSR) strategy, which allows Chinese enterprises to speed their growth plans, taking advantage of state support as they expand globally, assisting them in competing against U.S. technology companies in emerging markets. Furthermore, the PRC leverages DSR to deploy technologies that will allow them to dominate data and communications in the political, economic, and social realms across the vast geographic scope of the initiative. The United States, on the other hand, has yet to propose a technology development plan like the PRC’s DSR. U.S. Congressman Ruben Gallego and Congresswoman Vicky Hartzler have suggested the United States create a “Digital Marshal Plan” to compete against China’s DSR initiative. While a Digital Marshal Plan is still not a reality, the Biden Administration has taken welcomed steps to strengthen U.S. technology-centric programs in Africa and the Western Hemisphere. Most recently, President Biden announced the launch of a new Digital Transformation with Africa (DTA) initiative that seeks to expand digital access and literacy and strengthen digital enabling environments across the continent. Additionally, the U.S. State Department announced a new public-private partnership in collaboration with Amazon in support of the Academy for Women Entrepreneurs (AWE) program in Latin America and American Spaces in Mexico. Such initiatives, if implemented successfully, could serve as case studies for the United States and harness support for a U.S.-led effort to strengthen global digital economies.

**Case Study: Cloud Computing in Brazil**

U.S. and Chinese technology companies need to understand which innovative products are required to satisfy targeted economic needs in new Latin American markets. Cloud computing is an innovative product illustrating U.S. and Chinese technological influence in developing countries like Brazil. Accelerating digital business transformation requires the use of on-demand, scalable cloud models to achieve cost efficiency and business continuity, which has popularized the adoption of “the cloud.”

The use of cloud computing is spreading globally with a significant economic impact in both developed and developing countries. Cloud computing, an internet-based general-purpose technology, has become a technological innovation that promises cost savings on technology infrastructure and faster software upgrades for users. The distributed nature of the cloud has led to massive increases in reliability, uptime, and latency. Data is stored and processed on servers across the globe rather than in a specific location, making the data more accessible, faster to securely access, and harder to disrupt. Through cloud computing, firms can rent computing power and storage from a service provider and pay on demand.

There are three major benefits of cloud computing for small businesses and
entrepreneurs. Firstly, cloud services regularly include IT services of highly skilled and trained personnel, cutting costs for in-house IT services. Secondly, cloud computing makes it so that businesses do not have to purchase hardware and infrastructure that will become outdated. Thirdly, it is a pay-as-you-go service, where businesses only pay for the storage needed, and if the business grows, there is always more space to purchase. These benefits amount to a reduced barrier to entering the market. Emerging markets like Brazil are expected to benefit from this revolution, as it could spread the benefits to Latin America as a whole and close information and technology gaps with technologically advanced developed countries.

Cloud computing is expected to benefit countries that heavily rely on the internet. Brazil has the fifth most mobile and internet users globally and enjoys a 70% penetration rate. In terms of the number of internet users, Brazil ranks below China, India, the United States, and Indonesia. However, among these countries, only the United States surpasses the internet penetration rate of Brazil. Brazil is seeing major growth in public cloud computing, which is composed of software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS), even as the larger IT outsourcing and business process outsourcing markets have stagnated there.

The Brazilian state of Sao Paulo is specifically experiencing a technology boom related to software for web and mobile development. With the increasing internet penetration, businesses’ use of cloud-based services is growing. Huawei Mobile Cloud, a subsidiary of Chinese company Huawei Technologies, and Amazon Web Services (AWS), a subsidiary of U.S. company Amazon, have taken notice. The Brazilian cloud infrastructure, or IaaS market, is dominated by three major global brands: AWS, Microsoft, and Huawei. This is a slightly different scenario to the global market, where AWS is the overall leader, followed by Microsoft (United States), Alibaba (China), Google (United States), and Huawei (China). At the end of 2020, AWS had a 53.7% share of Brazil’s IaaS market, up from 50% by the end of 2019. Microsoft and Huawei also increased their market shares last year, upping them to 15.8% and 7.7%, respectively, from 14.4% and 7.1% at the end of 2019.

However, there are also downsides to cloud computing. In terms of accessibility, if the internet connection goes down, businesses’ access to remote data stores disappears, affecting businesses’ operations. This can be an issue for businesses in Latin America since Latin America and the Caribbean is the world’s second most natural disaster-prone region. Additionally, cloud services are operated on physical cloud data servers. The actual hardware is managed and run by the cloud company in question, which means yielding proprietary information to another firm. Thus, because Brazilian businesses are using cloud computing services, they are lending the data to the largest public cloud-based providers in the region, particularly U.S. and Chinese, giving these technology firms their data.

As the benefits of cloud computing become widespread in Brazil, technology companies hold ever-higher responsibility for its availability. Currently, U.S. and Chinese technology companies largely dominate the cloud-based computing market in Latin America (Figure 2). U.S. and Chinese firms providing cloud services and servers are located mainly in Brazil, Chile, and Mexico.
Figure 2: Mapping Cloud Service Providers in Latin America

<table>
<thead>
<tr>
<th><strong>U.S. Cloud Providers</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Company</strong></td>
<td><strong>City</strong></td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>Sao Paulo</td>
</tr>
<tr>
<td>AWS</td>
<td>Sao Paulo</td>
</tr>
<tr>
<td>Google Cloud Platform</td>
<td>Sao Paulo</td>
</tr>
<tr>
<td>IBM Cloud</td>
<td>Sao Paulo</td>
</tr>
<tr>
<td>Oracle Cloud</td>
<td>Sao Paulo</td>
</tr>
<tr>
<td></td>
<td>Colima</td>
</tr>
<tr>
<td></td>
<td>Santiago</td>
</tr>
<tr>
<td></td>
<td>Bogota</td>
</tr>
<tr>
<td></td>
<td>Campinas</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Chinese Cloud Providers</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Company</strong></td>
<td><strong>City</strong></td>
</tr>
<tr>
<td>Huawei Cloud</td>
<td>Sao Paulo</td>
</tr>
<tr>
<td></td>
<td>Buenos Aires</td>
</tr>
<tr>
<td></td>
<td>Lima</td>
</tr>
<tr>
<td></td>
<td>Mexico City</td>
</tr>
<tr>
<td></td>
<td>Santiago</td>
</tr>
<tr>
<td></td>
<td>Santiago</td>
</tr>
<tr>
<td></td>
<td>Sao Paulo</td>
</tr>
</tbody>
</table>

Source: Cloud Infrastructure Map,\(^{42}\) Huawei Cloud Availability Zones\(^{43}\) in 2022

AWS was the first public cloud service to service Latin America. AWS landed in Sao Paulo in 2011, and since then, an array of U.S. and Chinese enterprises have entered the market.\(^{44}\) On the other hand, Huawei Cloud launched its cloud service in Sao Paulo in 2019.\(^{45}\) While AWS’ cloud services have been present in Brazil longer than Huawei’s, Huawei as a company celebrated its first 20 years in the country in 2018.\(^{46}\) The following analysis will focus on AWS and Huawei Cloud offerings in Brazil due to limited data on technology companies’ presence in other Latin American countries. The following analysis will illustrate the technological initiatives and strategies that AWS and Huawei Cloud have undertaken in Brazil. An analysis of how both public cloud providers are deploying and marketing their services showcases the competition for influence AWS and Huawei Cloud are exerting in the receiving countries. Using an advanced search on Google News, an aggregator of headlines that can limit sources by date, source, and location, the results revealed that in the past year (May 2021 to May 2022), AWS and Huawei Cloud have made leeway into the Brazilian market through government partnerships and training programs.

**Partnerships with the Brazilian Government**

The Brazilian government, in 2021, launched a bid for a two-year contract that encompasses the integration of cloud services for federal government bodies. This was the second unified public cloud purchase that the Brazilian government has carried out. The proposal brought forward by cloud broker Extreme Digital Solutions included service providers AWS, Huawei Cloud, and Google.\(^{47}\) The request for proposals called for at least two cloud providers with data centers located in Brazil, which made AWS and Huawei qualify for the bid. This example demonstrates how
investing in infrastructure preemptively allows technology companies to secure government deals. Besides this deal, AWS has been awarded all the government deals between 2021-2022, with no evidence of Huawei Cloud securing any government deals in the analyzed period.

In February 2022, the Brazilian Space Agency and AWS signed a “term of strategic intent and cooperation.” The initiative, supported by the Brazilian Embassy in Washington, is the first of its kind for AWS in Latin America. The initiative aims to support innovation and continued growth in the country’s space industry. In addition, AWS powered remote learning for 2.5 million high school students in Sao Paulo during the pandemic. On the other hand, Huawei Cloud has not secured any exclusive deals with the Brazilian government between 2021 and 2022. A possible explanation for Huawei’s lack of contracts with the Brazilian government could be due to U.S. national security adviser Jake Sullivan’s visit to Brazil in August 2021. The U.S. delegation, during the visit, warned Brazil that Huawei was facing “major challenges” to its semiconductor supply chain that would leave international customers “high and dry.” Local media misrepresented the United States comment as “pressuring” the Brazilian government to abandon any deals with Huawei if Brazil wanted United States support for a NATO partnership with Brazil. NSC Senior Director for the Western Hemisphere at the White House Juan Gonzalez denied reports that the United States had offered support for a NATO partnership with Brazil in exchange for cooperation over 5G equipment made by China’s Huawei Technologies, stating the two issues were not related and there was no “quid pro quo.”

So far, the Brazilian government has not released any official statements indicating that the U.S. warning has affected the government’s rationale for choosing Huawei Cloud. However, another Chinese cloud service provider Alibaba Cloud, which does not currently have any cloud servers in Brazil, has been making a quiet entry into the Brazilian market through UOL Digeo, one of the largest Brazilian data center and technology companies. Small Brazilian outlets speculate that with Huawei facing problems with the United States and its other trading partners, Alibaba Cloud has taken advantage of the opportunity to enter the Brazilian market. Brazilian outlet Baguete notes that Alibaba Cloud said through a spokesperson that it has been working in Brazil “for more than a year.” However, when asked whether Alibaba Cloud had a direct presence in the country or other partners, the company declined to respond. Possibly, Alibaba is learning from the mistakes of Huawei and taking the opportunity to make a quiet entry through Brazil-native data companies. However, Huawei Cloud is not leaving Brazil altogether, and reports have come out of Huawei partnering with smaller start-ups to implement its services.

Training Programs: For the People

Huawei Cloud and AWS are not only venturing into the Brazilian market to secure deals with the government but also to gain favorability with the people of Brazil. AWS and Huawei Cloud have made leeway into the Brazilian market by providing training aimed at up-skilling labor in Brazil in the past year. AWS has only launched one training program in Brazil between 2021-2022, while Huawei Cloud has established two training programs. AWS launched in 2021 the re/Start program, a course aimed at people who are unemployed or looking to pivot careers. The AWS training is entirely free and focuses on IT and AWS cloud fundamentals. This program is being expanded to seven cities in
five countries, three of which are in Brazil: São Paulo, Curitiba, and Fortaleza. AWS Global Vice President of Public Sector Max Peterson promoted the course by stating that “90% of students who complete the course are immediately employed.” On the other hand, in 2021, Huawei Cloud launched the Spark Program, which gives participating start-ups “coupons” of up to $100,000 to spend on Huawei Cloud per year, in addition to technical and market entry support. In addition, Huawei Cloud has teamed up with the Brazilian National Service for Industrial Training (SENAI) to open a professional training and certification lab for the information and communications technology (ICT) and telecom sectors in the municipality of Cachoeiro de Itapemirim.

A media analysis of AWS’s and Huawei Cloud’s presence in Brazil shows how two of the largest technology companies compete for market share in an emerging market. Huawei and Amazon use their subsidiary companies that provide cloud services to compete for dominance in Brazil. Although cloud services are expected to empower and benefit emerging markets from this revolution as they could close information and technology gaps with more advanced developed countries, it also means that these countries are relying on foreign companies to lead their technology development efforts. In the case of Brazil, AWS and Huawei Cloud dominate the cloud service market by selling services to the government and facilitating training programs. While competition is palpable, as both providers compete to secure deals with private businesses, their influence extends to local governments and their constituents.

Government bids can give technology companies an expanding global presence and a growing list of corporate interests that transcend national boundaries and directly influence geopolitical events. The media analysis between 2021-2022 revealed the potential of great power competition influencing market competition. Presumably, the United States’ global campaign against Huawei has affected the Brazilian government’s perception and decision to engage Huawei in its networks. In addition, AWS having the support of the Brazilian Embassy in Washington, DC, in the Brazilian Space Agency deal, instead of the U.S. Embassy in Brazil highlights an opportunity to strengthen private-public partnerships for U.S. technology companies abroad.

Both cloud providers are expanding their influence by engaging with the public directly. Their free training programs are aimed at upskilling the Brazilian force, potentially increasing the labor pool in the country. However, these training programs are solely training the awardees on their proprietary software, creating a labor divide between those who know how to work the Huawei Cloud versus the AWS platform, which begs the question as to whether the trainees have employment success outside of these two providers.

As Huawei carves out a niche as a provider in Brazil, its activities could provide the PRC with data that can be leveraged as intelligence. The United States should prioritize cloud infrastructure and services as an area of strategic competition since the United States already has a competitive advantage in Brazil and seems to enjoy favorability with the Brazilian government.

Digital Future: Concerns and Considerations

Following a detailed description of how U.S. and Chinese technology companies compete for influence in the Latin American market, it is worth discussing the potential implications and concerns surrounding the services both Chinese and American companies provide. U.S. and Chinese cloud service providers end up funnelling
government and business data through their cloud servers, which they own and operate. Cloud servers are subject to the rules and standards of the technology company. While technology is often justified and thought of as bringing net positive results to nations, great power competition plays a role in the development and advancements of technology competition.

**Data Colonialism**

The United States and China are the largest technology providers and developers of technology by proxy of the technology companies. They are exerting technological power as part of their development practices. Developing nations that are not caught up technologically with the great powers are seen as turf for great power competition on the technological front. The least developed and developing nations are at a significant technological disadvantage and are vulnerable to digital colonialism. Digital colonialism is “the use of digital technology for political, economic, and social domination of another nation or territory.” It encompasses the digitization of indigenous data without fully informed consent, the theft or exploitation of data, and the use of digital tools for influence and power over a subject. Digital colonialism aligns with the notion that data is the new natural resource, where great powers deploy advanced tools to mine and extract data from developing nations.

Under the framework of digital colonialism, thinking of data as a new natural resource allows us to view how technology companies can perform as actors or subsidiaries of the state in exploiting developing nations. Given that U.S. and Chinese technology firms dominate the Latin American market, Latin American governments should cautiously engage with foreign technology enterprises since cloud-based solutions rely on clients storing data on another firm’s hardware and infrastructure, which means giving away proprietary information to another firm. Countries being serviced by technology firms must consider the security measures that these companies (and, in some cases, their affiliated governments) provide for the data they handle. As previously mentioned, this is especially important when collaborating with Chinese technology companies, as the PRC authorities often exert varying degrees of oversight over these companies. However, the disjointed relationship between the United States government and American technology firms could become a selling point, and a security guarantee, for countries seeking to expand their cloud service offerings and infrastructure.

**The Future of the Nation-State**

As technology companies continue to grow at the scale and speed they have in the last 20 years, privately owned technology companies are projected to carry the weight of small governments. Under the assumption that technology companies will continue to amass and project power, the question remains whether technology companies or nation-states will yield geopolitical power and whether nation-states will remain relevant through digital transformation. However, as long as technology firms cannot decouple themselves from physical space, they will remain at the mercy of states. Mats Lewan at the Stockholm School of Economics has identified two areas in which technology can strengthen the role of the state: services and governance. The nation-state can adapt to accommodate the digital transformation by partnering with technology companies to improve service efficiency and distribution and overall governance. From an innovation perspective, a state losing independence and gaining another role in an increasingly interconnected world can be seen as a natural evolution resulting from steadily...
improved communications technologies throughout human history. Suppose states heavily collaborate with technology companies in improving these functions, which historically have been relegated to states. In that case, there is a possibility that states and technology companies can, in the near future, coexist and contribute to the global good.

**Services**

The nation-state provides services in the form of health care, social care, education, infrastructure, law and order, and defense, all paid for by tax revenue. The nation-state should prioritize partnering with technology companies to improve its services and, in some instances, establish the technology companies as the leading providers of those services. For example, the COVID-19 pandemic has demonstrated how technology companies have stepped in to improve and deliver services to the population. In Panama, for example, the president’s attempt to distribute food vouchers with on-premises hardware and software crashed almost immediately, only to be rescued by AWS, which set up a system to distribute these vouchers over smartphones in just one long weekend.

Establishing infrastructure usually elicits bridges and roads, but technology infrastructure also falls within the realm of services governments offer. Infrastructure-as-a-service (IaaS) has become a profitable service technology companies provide that benefits recipient countries. As only four companies (Alibaba, Amazon, Google, and Microsoft) currently meet the bulk of the world’s demand for cloud services, they have comprised the essential computing infrastructure that has kept people working and children learning during the COVID-19 pandemic. Since technology companies amass the power of what is possible, governments must partner with these companies to shape how services are improved and implemented. There is an opportunity for nation-states to enlist technology companies as alternative providers of social services that, in turn, may transform their role from producer to facilitator of services.

**Governance**

On the other hand, how governance leverages digitalization largely depends on the form of governance. For both democracies and authoritarian governments, there is the opportunity to strengthen the governance process using technology. For autocracies, there is an opportunity to strengthen the nation-state through increased control and oppression. For democracies, there is an opportunity to combat fatigue in the democratic process through digital tools.

Led by China, today’s digital autocracies use technology like the internet, social media, and AI to supercharge long-standing authoritarian survival tactics. Through DSR, the PRC is exporting potentially repressive technologies. At least 18 countries have bought advanced AI and surveillance systems from Chinese technology companies, due to Chinese technology companies’ high-quality and low-cost technology offerings compared to other alternatives. However, the global trend of internet censorship has marginally declined over the last two years. Except for China, the three countries with the most rapidly increasing censorship from 2011 to 2017, namely Iran, Turkey, and Egypt, staled in their censorship efforts during 2018. There is an opportunity for democratic governments and non-Chinese technology companies to boycott the sale of technology and innovation for repression.

Scholars have been exploring how the emergence of the internet and the plethora of new information and communications technologies has raised hopes that the internet could reinvigorate the democratic experience in representative
democracies. Legal scholar Oren Perez at Bar-Ilan University notes that the e-democracy movement is changing the praxis of democratic engagement. E-democracy, a combination of the words electronic and democracy, also known as digital democracy or internet democracy, uses information and communication technology (ICT) in political and governance processes. Perez’s research denotes that technology can remove some obstacles facing Web use in the context of deliberative democratic processes, particularly the problem of literacy and information overload by developing user-friendly interfaces and reducing the cognitive effort associated with political engagement. New technologies are being developed, such as Google Moderator, for example, to enable public electronic dialogue with the promise of improving the underlying structure of mass deliberation.

Conclusion

The United States and China made efforts in recent years to regulate U.S. and Chinese technology companies domestically. In the United States, a plethora of antitrust bills have been introduced on the House of Representatives’ floor to limit the influence of U.S. technology companies. For example, H.R. 3849, the Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act, tackles the network effects. Whereas China on August 2021 enacted the Personal Information Protection Law of the People’s Republic of China (PIPL), the first national data privacy statute passed in China that imposes protections and restrictions on data collection and transfer in China. The statute is particularly focused on applications using personal information to target consumers or offer them different prices on products and services, preventing the transfer of personal information to other countries. Both U.S. and PRC efforts to regulate technology companies in their own territory do not explicitly regulate U.S. and Chinese technology companies abroad.

As new technological innovations like AI and quantum computing spread globally, nation-states must do better at regulating technology companies’ expansion. Technology companies will continue to gain power and project it abroad through their pertinent development strategies. As demonstrated in this paper, technology companies are already entrenching themselves abroad and servicing emerging economies by exerting state-like capabilities. Four companies, Alibaba, Amazon, Google, and Microsoft, meet the bulk of the world’s demand for cloud services and amass total dominance of the service abroad. U.S. and Chinese technology companies are causing developing countries to be dependent on their services. Firstly, they are laying the infrastructure to operate their products and services, creating a technological and infrastructure dependence in the receiving state. In addition, they are expanding infrastructure by creating networks of citizens who rely on the platforms to build successful businesses and grow alliances by providing training on their specific platform rather than generalist training on IT and cloud services. Secondly, as U.S. and Chinese technology companies dominate developing countries’ markets, they are managing large amounts of data that could be exploited for great power competition. Given that U.S. and Chinese technology firms dominate the Latin American cloud services market, Latin American governments should cautiously engage with foreign technology enterprises since cloud-based solutions rely on clients storing data on another firm's hardware and infrastructure, which means giving away
proprietary information to another firm (and potentially, a foreign government).

The implications of U.S. and Chinese technology companies for developing nations will depend on the level of freedom or restriction placed on them by their respective governments. The PRC will continue to use the data that Chinese technology companies manage to improve their tools for surveillance and repression. Compared to the United States approach, the PRC's control and aid of Chinese technology companies create asymmetry in competition and influence. It has become a game of three players, where the PRC and the Chinese technology companies operate as one while they compete against U.S. technology companies and the U.S. government as different entities.

The Brazil case exemplified that great power competition affected the Brazilian government’s decision to partner with Huawei for government services. The United States should continue to highlight the risks of partnering with Chinese companies and the implications for security and privacy. The United States case could be strengthened by partnering with technology companies to lay out infrastructure and offer alternatives and more economical solutions to compete against Chinese development practices. The United States should prioritize cloud infrastructure and services as an area of strategic competition since the United States already has a competitive advantage in Brazil and seems to enjoy favorability with the Brazilian government. Competing more effectively in developing markets may require packaging cloud services with support for the infrastructure that underpins them. The United States should pool resources to expand financing and funding for digital infrastructure, technical assistance, and training in emerging markets. They should also cooperate to remove and prevent foreign regulatory barriers that disadvantage U.S. and allied cloud providers.

The effects of technology companies, and their varying degree of state control, will affect great power competition. If the United States wants to robustly compete as a united front against the PRC’s proposed national security plans in developing countries, it needs to establish strong relationships with the private-public sectors in target markets, and instead of focusing on controlling the power of technology companies at home, harness their power to improve the democratic process. Either the United States government adapts, integrates, and accepts the changes technology is lending to people, or it will cease to remain relevant in technological innovation and development globally.

About the Author
Ona Spreenberg is a multilingual foreign policy professional with expertise in U.S. foreign policy towards China and Latin America. Born in California and raised in Spain, Ona has experience working in the U.S. federal and local government and has an innate passion for international relations, internet governance, emerging technologies, and gender studies. Ona received her B.A. from UCLA and is currently pursuing an M.A. in Security Studies at Georgetown University’s Walsh School of Foreign Service. She can be contacted at ows7@georgetown.edu.


Gilroy, Chloe. “Great power competition and counter-narcotics in the western hemisphere.” William J. Perry Center for Hemispheric Defense Studies, Occasional Paper. (September 2020) p. 3


10 U.S. Warned Brazil That Huawei Would Leave It ‘high and Dry’ on 5G.” *Reuters.* (August, 2021).


17 “Mob Telecom migra B1 para cloud da Huawei.” Baguete. (June, 2019).

18 “AWS Re/Start Lanço Cursos Gratuítos de Qualificação Em Nuvem No Brasil.” *Sempre Update.* (September, 2021).


21 “90% Dos Unicórnios Brasileiros Usam AWS, Diz CEO.” *Mobile Time.* (June, 2021).


