Georgetown Security Studies Review

Volume 8 | Issue 1
February 2020

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

Disclaimer

The views expressed in Georgetown Security Studies Review do not necessarily represent those of the editors or staff of GSSR, the Edmund A. Walsh School of Foreign Service, or Georgetown University. The editorial board of GSSR and its affiliated peer reviewers strive to verify the accuracy of all factual information contained in GSSR. However, the staffs of GSSR, the Edmund A. Walsh School of Foreign Service, and Georgetown University make no warranties or representations regarding the completeness or accuracy of information contained in GSSR, and they assume no legal liability or responsibility for the content of any work contained therein.

ISSN 2474-8552 (print); ISSN 2474-8560 (online)

GEORGETOWN SECURITY STUDIES REVIEW

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

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

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

Table of Contents

Letter from the Editor

This February, we are excited to present the *Georgetown Security Studies Review Volume 8, Issue 1*.

This cycle, we received a record number of submissions, resulting in some terrific pieces. With articles on Chinese foreign policy, cyber strategy, and the ongoing crisis in Venezuela, this issue will be of interest to a wide range of readers. As always, I am extremely grateful for the authors who submitted such learned articles as well as for our dedicated editorial board who sacrificed many hours of their time to proof and refine the pieces that comprise this issue. I also want to thank Dr. Keir Lieber and Annie Kraft for their continued leadership and support in growing the GSSR and ensuring that everything runs as smoothly as possible. Sustaining and growing this publication is a monumental effort, and it truly would not be possible without the dedication and conscientious work of our entire team.

Going into the spring, the GSSR will be moving to expand its range of publications. Excitingly, we are working with the BMW Center for German and European Studies podcast, the *Europe Desk*, to develop a special issue on European security. The current hope is to have it released sometime in April. And this is just one of several efforts to collaborate more extensively with other SFS programs. Hopefully the GSSR will continue to expand in its size and range of content over the coming semesters.

Finally, I would be remiss not to note the excellent work of Integrated Books International, which produced this handsome volume.

I hope the ideas within the Review allow you as a scholar or practitioner to better make sense of the very real challenges of the day.

Warm regards,

Samuel M. Seitz
Editor-in-Chief, February 2020
Georgetown, Washington D.C.

Why China Continues to Support North Korea

Naomi Garcia

Scholars and policymakers frequently highlight the risks of a war on the Korean Peninsula when explaining China's support of Pyongyang. They argue that the dangers of loose nukes, refugees, and the advance of American forces to the Chinese border are what primarily explain Beijing's aversion to reunification. This article contends that these concerns are not the central motivation behind Chinese actions. Instead, it asserts that Chinese support for North Korea derives from the pecuniary value of the relationship as well as the leverage that the relationship grants Beijing vis-à-vis the United States. Once framed in this way, it becomes clear that Washington's current strategy toward North Korea and China is fundamentally misguided because it rests on false premises.

Introduction

Despite continuous and increasing pressure from the United States, The People's Republic of China (PRC) has failed to exert significant pressure on the Democratic People's Republic of Korea (DPRK) in response to the latter's growing nuclear and missile arsenal. However, since the Carter-era normalization of relations between the United States and China in the late 1970s, Washington has considered China's influence over North Korea to be the primary strategy for containing the threat of North Korean provocation.[1] This paper discusses the increasingly prevalent, though misguided, belief that China represents the key to containing the threat of nuclear war from the DPRK.[2] Furthermore, this research aims to provide insight into China's motivations and intentions on the Korean peninsula in order to explain why China is, and will continue to be, unwilling to cooperate fully with the United States in response to North Korean threats. Established views in both academic literature and media maintain that China supports North Korea largely to avoid the consequences of regime change, such as a refugee crisis and regional instability.[3] This research argues that current views neglect the positive strategic benefits that China extracts from the DPRK's continued existence; these benefits form an integral part to China's support of North Korea and affect U.S. policy-making decisions. Such positive incentives include China's increasing strategic importance to U.S. policy in the region, protracted distraction of international attention from China's other, more significant strategic and economic concerns, and the benefits from growing terms of trade with North Korea.

Precisely because China is responding simultaneously to positive incentives to support North Korea as well as avoiding potential negative side effects of a regime collapse, it is extremely unlikely that China will walk step-for-step with the United States on U.S. foreign policy towards North Korea. This understanding changes the focus of policy decisions directed at China regarding the DPRK. With a better understanding of China's reasons for supporting North Korea, American officials and scholars can approach the issue from more informed angles in future talks and research. To demonstrate these points with clarity, this work is split into the following sections: 1) Examples of Chinese support for the DPRK; 2) An analysis of negative incentives commonly cited for China's support of the DPRK; 3) An analysis of positive incentives for China's support of the DPRK, and 4) Concluding remarks and policy recommendations.

Examples of Chinese support for the DPRK

Despite explicit urging and warnings from the United States to increase pressure, the People's Republic of China has continuously engaged with and supported the North Korean regime for the past four decades—highlighting both the economic benefits that China values in its relationship with North Korea as well as China's unwillingness to impose sanctions that may seriously harm the North Korean regime.[4] Of primary importance is China's role in abetting North Korean efforts to evade United States and United Nations sanctions. According to the United States Treasury, the two primary risks of North Korean sanctions evasion are "(1) inadvertent sourcing of goods, services, or technology from North Korea; and (2) the presence of North Korean citizens or nationals in companies' supply chains, whose labor generates revenue for the North Korean government."[5] China has been essential in enabling North Korea to achieve both types of sanctions evasion, as noted below. Specific examples of Chinese aid in North Korean sanctions evasion are numerous. This research aims to give readers an understanding of the breadth of these sectors, but an exhaustive list of such support remains outside the scope of this work.

In September 2018, the United States Treasury published a press release detailing the actions of Chinese *Yanbian Silverstar Network Technology Co., Ltd.*[6] The U.S. Treasury reported that the company, reportedly earning millions of dollars for the Kim regime, is "nominally a Chinese IT company, but in reality it is managed and controlled by North Koreans."[7] In August of 2018, the United States Treasury reported that the Chinese *Dalian Sun Moon Star International Logistics Trading Co., Ltd.,* in conjunction with the Singapore-based affiliate *SINSMS Pte. Ltd.*, facilitated illicit shipments of alcohol, tobacco, and cigarettes to North Korea using falsified shipping documents.[8] China has also chiefly facilitated North Korean international financial endeavors. In a 2017 report by the United Nations Security Council, the North Korean *Daedong Credit Bank* (DCB) has operated in Dalian, China since 2006 and is responsible for millions of dollars of transfers to North Korea. The report details that the bank "exchanged large quantities of bulk cash transferred to China from the Democratic People's Republic of Korea into newer and larger denomination United States dollar notes," and that in 2011 an unnamed Chinese company became the majority shareholder of the DCB. [9]

Chinese support of North Korea also takes more overt routes. China has long been one of North Korea's largest donors of humanitarian aid and has consistently been North Korea's largest bilateral trade partner since 2007.[10] Despite U.S. pressure, this relationship continues to grow. According to the 2017 Korea Trade-Investment Promotion Agency (KOTRA) report, North Korean exports to China more than quadrupled from 2007–2016,[11] and Chinese exports to North Korea more than tripled in the same period.[12] During this time, the two countries also implemented new ways to enhance their trade, such as the $158 million *Guomenwan* trade zone that opened in 2015 to allow free trade across the border between China and the DPRK. Chinese state news source Xinhua explicitly confirmed in 2015 that the zone was to "help boost the border trade and increase incomes of both Chinese and DPRK people."[13] These bilateral advancements occurred during constant and increasing American and international sanctions against North Korea, effectively undermining the weight of U.S. and international pressure on North Korea.[14]

China's only occasional and temporary attempts at compliance with the imposition of sanctions on North Korea further elicits the PRC leadership's support of the regime for Chinese interests, regardless of U.S. pressure. According to the 2018 annual report by the U.S.-China Economic and Security Review Commission, "Beijing

tightened enforcement of sanctions for a time to encourage Pyongyang to embrace diplomacy prior to the recent improvements in the Sino-North Korean relationship;"[15] however, the report concludes that China has since relaxed sanctions enforcement regardless of its assurances to the contrary.[16] Furthermore, both the Council on Foreign Relations and the Peterson Institute for International Economics credit China's persistence with changing the original draft of the 2017 UN Resolution 2375 that called for a complete ban on crude oil exports to the DPRK.[17] This persistence highlights both the economic benefits that China values in its relationship with North Korea and China's unwillingness to impose sanctions that may seriously harm the North Korean regime—as well as the fact that, despite U.S. persistence in working with China to contain North Korea, China's relationship with the regime has effectively contributed to undermining U.S. efforts at this perceived shared goal. [18]

An analysis of negative incentives commonly cited for China's support of the DPRK

Two of the most commonly cited explanations for China's negative incentives to support North Korea from Western scholars are China's desire to avoid both a refugee crisis and regional instability that would ensue from the collapse of the North Korean regime.[19] While these two negative incentives are both frequently referenced, research indicates that China's perceived threat from a refugee crisis has been significantly reduced as China has become more technologically and economically advanced. Research also indicates that China's threat perception arising from regional instability given North Korean collapse remains a concern that aligns with current rhetoric. This section contextualizes China's overall perception of negative incentives that encourage it to support North Korea in order to underscore the ways in which U.S. foreign policy must also account as much, if not more, for the positive incentives that China receives from the existence of the North Korean regime.

While a refugee crisis from North Korea would not be preferable for the Chinese government, specifically near the autonomous region of Inner Mongolia, the reality is that China is increasingly more equipped to deal with a refugee crisis as it has developed technologically and economically. According to Hazel Smith and Timothy Hildebrandt of the Woodrow Wilson International Center for Scholars, "The issue of refugees [. . .] is less an issue of conflict and more a subject of irritation for China."[20] In a comprehensive commentary published in People's Daily, the mouthpiece of the Chinese government, about the reasons to avoid war on the Korean Peninsula, refugees hardly took mention. The 2017 piece describes the necessary pre-war preparations and the disastrous security consequences of failing to prepare. The article raises only one line about refugees near the conclusion, stating that "once the war has begun, we would still want to think about creating refugee camps within the North Korean border to prevent the flow of refugees into China."[21] While it is clear that the government will take action to prevent North Koreans from flowing into the country, refugees rank very low on the list of Chinese priorities regarding the North Korean situation.

Furthermore, in 2017 a document leaked on social media from China Mobile, China's leading telecommunications network, detailed its plans to construct five camps for North Korean refugees in northern China. The leaked document also highlighted the camp's provision of cellular service and internet connection.[22] China's preemptive plan and concern for the quality of the camps suggests that in the event of North Korean refugee entrance into China, the Chinese central and local governments are prepared and equipped to handle the influx.

Dr. Oriana Mastro, Assistant Professor of Security Studies at Georgetown University, proposes that a refugee crisis

is a low priority for China because of the modernization of the Chinese military in recent years.[23] Dr. Mastro argues that the People's Armed Police (PAP) would be capable of securing the border in the event of North Korean regime collapse, leaving the People's Liberation Army (PLA) to handle international security concerns other than refugees.[24] The 2018 U.S. Department of Defense report on Chinese military power further confirms her hypothesis, listing over 170,000 soldiers and a combination of six air force and naval units, in addition to the PAP, in the northern theatre of China alone. The report concludes that support from other theaters in China can be readily called upon and that emergency response units trained in chemical, biological, radiological, and nuclear incidents are also prepared to act.[25]

The following research indicates that regional instability is of far greater concern to the PRC than the worry of refugees, and thus a much larger incentive to support the nuclear regime. Because of North Korea's incendiary behavior, the United States has successfully united both Japan, a historical enemy of China, and South Korea in line with U.S. policy on one central regional target. This ideological alignment with the United States has led to increased an American military presence in the region. Of particular note is the July 2016 deployment of Terminal High Altitude Area Defense (THAAD) in South Korea and China's mounting fear that THAAD "is only a new start to the U.S. pursuit of zero-sum security in the Asia Pacific."[26] Despite these developments, China favors the status quo over a North Korean regime collapse, especially given that unification following the collapse would likely take the form of a U.S.-backed and South Korea-led state directly bordering China.[27] Moreover, a North Korean collapse would assuredly cause regional instability at a time when Chinese leaders are attempting to unite the region under a stable Chinese economic and political hegemony—the Belt and Road Initiative.[28] This is particularly poignant given that, in the event of a North Korean regime collapse, the United States would be likely to increase both its presence in the region and its military cooperation with at least Japan and South Korea at a time when China is explicitly attempting to gain its own form of regional control and economic partnerships with Asian countries that does not involve the United States.

This section has provided an understanding and analysis of the two most cited modern theories of China's relationship with North Korea from which to proceed. Among these two reasons for China's behavior, research indicates that China's threat perception from a refugee crisis is lower than commonly cited, while China's high threat perception from a North Korean regime collapse aligns with current rhetoric. With an understanding of China's presumed negative incentives to support North Korea, this research can now proceed to further analyze the positive incentives that China additionally receives from the perpetuated existence of the North Korean regime and how these positive incentives interact with China's discussed threat perception.

An analysis of positive incentives for China's support of the DPRK

China's increasing strategic importance to U.S. policy in the region

From China's perspective, active participation in international policies involving North Korea has proven beneficial for both China's position with the United States and its global image as a whole. Negotiators of the 1994 U.S.-DPRK Agreed Framework note that China's prestige as a global diplomatic player increased dramatically due to its leadership role in the 2003 six-party talks.[29] The official Chinese position on historical accounts of the North Korean nuclear issue frequently mentions the indispensable contributions China made to the easing of tensions between the United States and North Korea. For instance, in a

2017 Brookings article, Fu Ying, the Chairperson of the Foreign Affairs Committee of the National People's Congress, details the Chinese perspective on the history of the Korean nuclear issue. Fu Ying concludes that "Chinese Premier Wen Jiabao visited Pyongyang on October 4-6, 2009, as part of regular bilateral exchanges. He met Kim Jong-il and discussed the issue with him. Subsequently, tensions started to ease in January 2010 when North Korea expressed a willingness to sign a peace agreement with the U.S."[30] While there is no doubt that Chinese participation in these negotiations was both helpful to and often desired by the United States,[31] many crucial developments occurred between Wen Jiabao's visit to Pyongyang and January 2010 that the detailed article does not mention. The most notable was the first senior-level meeting between officials of the Obama administration and the North Korean government in Pyongyang from December 8-10, 2009.[32] This is not to say that China's contribution to the easing of tensions was not valuable, but rather to emphasize that the Chinese side notably appreciates the opportunity to applaud its position in the talks to an international (and predominantly U.S.-focused) audience.

In line with this, the Chinese side continues to stress its historic importance in the U.S.-DPRK relationship and to argue for the resumption of the six-party talks to ensure Chinese interests in the region. A 2018 commentary published on the People's Daily website reminds readers that "as the head of the six-party talks, China has always played an irreplaceable role in resolving the DPRK nuclear issue and has made tremendous efforts to build a long-lasting peace mechanism on the peninsula."[33] Further commentaries advocate for a resumption of the six-party talks with China playing a lead role.[34]

China's strategic position on the issue of North Korean denuclearization has allowed China more leverage over U.S. decisions in the region and ultimately granted China leverage over the broader scope of U.S. foreign policy, as will be discussed in the following section. This is what officials crucial to the 1994 U.S.-DPRK Agreed Framework negotiations refer to as "a double-edged sword, increasing U.S. exposure to Chinese pressure while simultaneously increasing Beijing's influence over the broader direction of the multilateral approach to North Korea."[35] For China, leverage over the United States regarding the neighboring Korean peninsula is extremely important to its perceived national security interests in matching U.S. regional influence. Dr. Mastro summarizes China's stake in the U.S.-DPRK relationship with a quote she was told from a PLA officer—"Why should the United States be there but not us?"[36]

Protracted distraction of international attention

Despite years of China's unwillingness to control North Korea's growing nuclear and military capabilities, the United States still prioritizes the North Korean issue in discussions with Beijing, often at the cost of other important matters. September 2018 rhetoric regarding the U.S.-China trade war retroactively included China's effort to aid North Korea as an additional rationale for the tariffs the U.S. imposed against China in July of 2018 in response to unfair trade practices.[37] This addition effectively ensures the United States is losing ground on the initial reasons for the tariffs, including intellectual property rights (IPR) violations and the U.S. trade deficit with China. Furthermore, Xi Jinping recognizes the leverage that China's relationship with North Korea provides within the context of the tense U.S.-China trade war. Analysts at Trivium China regard Xi Jinping's June 20, 2019 visit to North Korea—the first Chinese state visit to North Korea since 2005—that strategically occurred just ahead of the June 29 Trump-Xi meeting as "a pointed reminder that cooperation with China is necessary for Trump's goals on North Korea."[38] Regardless of the

domestic partisan nature of such grievances, the reality is that Washington has diluted its initial message on trade in the hopes of securing Chinese pressure against North Korea—pressure that has historically proven unsuccessful—and Beijing is aware of how to leverage that pressure to its advantage. Not only does the United States forfeit ground in IPR, the trade imbalance, and unfair trade practice negotiations, but the message is effectively clear: *as long as China maintains close ties with North Korea while North Korea is a growing threat to the United States, China faces less stringent regulations on all other matters of security.*

Trade issues are not the only aspects of U.S.-China relations that are overlooked in exchange for a focus on North Korean denuclearization. As Dr. Jennifer Lind notes, "without the North Korean thorn in the American side, Washington might turn its gaze toward Taiwan and the South China Sea."[39] At the same time, China has heavily developed its Belt and Road Initiative and massive Asian Investment Infrastructure Bank, creating a real competition for global economic dominance to challenge the existing framework of global relations.[40] These issues have been overlooked due to the North Korean threat and the U.S. perception that China can and will help to direct North Korea's behavior. Meanwhile, China benefits from a distracted audience as it attempts to gain hegemony in the region and beyond.

North Korea's inflammatory behavior not only distracts the United States from China's activities but also focuses Japanese and South Korean arguments against domestic military proliferation on the U.S.-backed assurance of protection from North Korea. U.S. interest in protecting its allies in South Korea and Japan has effectively ensured that both countries maintain their decisions not to develop their own high-level military capacities or nuclear arsenals. Dr. Michael Heng writes that the single best result of U.S. hegemony in Asia for China "is that Japan has stuck very close to Article 9 of its constitution and remains non-nuclear."[41] China clearly benefits from this indirect side effect of the U.S. presence in the region, underscored by China's stated concerns about recent Japanese and South Korean military proliferation.[42] Furthermore, U.S. officials briefed on the issue indicated that "a peace treaty between the two Koreas could diminish the need for the 28,500 soldiers currently stationed on the peninsula,"[43] giving Chinese officials cause for concern regarding a Japanese or South Korean military expansion. China has long benefitted from unintended U.S. protection in the region, and a collapse of the North Korean regime very possibly spell the end of the U.S. shield against a war-capable Japan or South Korea. In this sense, North Korea's existence provides a dual benefit for China—it is both the reason to maintain the U.S. troops that provide China with unintended protection and the buffer between China and those same troops.

Benefits from growing terms of trade with North Korea.

Not accounting for illicit trade, economic data from 1995 to present shows China's historic and current benefits from trade with North Korea. Apart from an anomalous year in 2001, China has been the largest source of North Korean imports since 1995, and 94% (or $3.23 billion worth) of North Korea's imports came from China in 2017.[44] More importantly, with North Korea's official declaration that the economy will be the regime's main focus, China's continued economic relationship with North Korea puts China in a position to capitalize on a growing market just over the border. In his 2018 New Year's Speech, Kim Jong-un declared that 2018 would see a "breakthrough in revitalization through the economic front."[45] Shortly thereafter, Chinese leader Xi Jinping secretly invited Kim Jong-un to travel to China at his convenience; this marked Kim Jong-un's first recorded diplomatic visit since coming to power.[46] In March 2018, Kim Jong-un arrived in Beijing to discuss the future of

the Sino-DPRK relationship. Notably, according to Xinhua News, Xi applauded Kim's focus on economic development and expressed China's full support.[47] This meeting was followed up with many other high-level meetings between Chinese and North Korean officials in 2018 and 2019, including Xi's June 2019 state visit to North Korea—marking the first visit to the country from a Chinese leader in fourteen years.[48] Their occurrence is also consistent with a changing global landscape as well as U.S. President Donald Trump's unprecedented willingness to engage directly with North Korean leadership. Of course, the timing of these meetings is not proof of China's sole desire to promote economic ties with Pyongyang; however, both the timeline and content of these exchanges is telling of China's perception of the economic benefits that will come from a partnership with North Korea.

China stands to benefit from North Korea's focus on its economy through increasing bilateral trade with both North Korea and South Korea. China has extended efforts to bring North Korea into the Belt and Road Initiative (BRI), which critics argue may "cast shadow over UN sanctions" on North Korea.[49] If North Korea's focus on the economy results in a BRI partnership with China, this will mean even more influence and strategic economic importance in the region for China as well as a direct route for land transportation of goods to South Korea.[50] Moreover, it further highlights the consequences of Beijing's relationship with Pyongyang—effective undermining of U.S. and international pressures on the regime.

Furthermore, North Korea has both known and predicted oil and gas reserves that could further benefit China's growing energy needs. In 2002, the Singapore-based company Sovereign Ventures announced the discovery of 10 million barrels of oil reserves in North Korea across the Tumen River touching the Chinese border.[51] In a report for the Woodrow Wilson International Center for Scholars, Selig Harrison affirmed that on a trip to Pyongyang in 2005, DPRK Petroleum Ministry officials informed him that estimates of potential oil reserves in the seabed west of Anju totaled 12 billion barrels.[52] In a stable North Korean state focused on economic development, China has a lot to gain both in terms of economic growth and energy security from a good relationship with the North Korean regime.

Concluding Remarks and Policy Recommendations

For almost four decades the United States has called upon the People's Republic of China to exert pressure on the Democratic People's Republic of Korea in response to the threat of nuclear proliferation. Despite this continued reliance on China, U.S. and international pressure on Pyongyang has proven ineffective, and the North Korean regime remains a large threat to the international community. Effectively, U.S. insistence on Chinese pressure towards North Korea resulted in more leverage for the Chinese state over broader American diplomatic efforts, reinforced to China that a relationship with North Korea ensures American lenience and distraction towards unfavorable Chinese actions, and granted China potential increases in economic and energy security. U.S. policymakers must understand why such tactics have failed in the past and move to understand and respond to China's modern incentive structure.

With the understanding that China has strong positive incentives for which to support North Korea in addition to the negative incentives to help perpetuate the regime, the United States can engage with China in more productive ways. In regard to economic incentives, for example, U.S. policymakers may consider engaging in bilateral and multilateral economic frameworks—such as the forgone TPP—that increase the United States' presence in Asia while simultaneously benefitting China's economy. An intertwined global network, especially one in which the

United States does not have a diminishing economic presence in Asia compared to China, gives the United States more leverage over China's economy as well as over North Korea's illicit trade routes.

Other policy recommendations include, as discussed above, strictly focusing the scope of Sino-U.S. discussions that do not inherently revolve around North Korea. In retroactively adding North Korea–related issues to discussions on trade and intellectual property, among other topics, the United States is effectively ensuring China leniency on all other matters of international relations as long as there exists a North Korea contingency to solve. With an understanding that difficult negotiations with the United States can be ameliorated by a hint at future help against North Korea, what Chinese leader would want to end the problem and take away the country's greatest bargaining chip with the United States?

Finally, given that China benefits from its increasing importance to the United States in the region, U.S. policymakers may benefit from intentionally downplaying the U.S. expectation of China's success in dealing with North Korea. In publicly referencing China as a solution to the problem in both media and academic literature, the United States is in fact perpetuating China's desire to help maintain the North Korean regime—with free press declaring the country to be an essential player in the international fight against a rogue nuclear state, what Chinese leader would in fact want to end the problem and cease its stream of positive international media?

About the Author:

Naomi Garcia is an alumna of the School of Advanced International Studies at Johns Hopkins University. She currently works as an editorial assistant at the National Bureau of Asian Research.

Endnotes

1. Person, James, "Chinese-North Korean Relations: Drawing the Right Historical Lessons," *The Wilson Center*, October 2017, www.wilsoncenter.org/article/chinese-north-korean-relations-drawing-the-right-historical-lessons
2. Ibid. and Joel S. Wit, Daniel B. Poneman, Robert L. Gallucci, *Going Critical - The First North Korean Nuclear Crisis* (Washington, D.C.: Brookings Institution Press, 2004).
3. Eleanor Albert, "The China–North Korea Relationship," *The Council on Foreign Relations*, March 2018, www.cfr.org/backgrounder/china-north-korea-relationship; Hui Zhang, "The North Korean Nuclear Test: The Chinese Reaction," *Bulletin of the Atomic Scientists*, *Harvard Kennedy School Belfer Center for Science and International Affairs*, 2009, www.belfercenter.org/publication/north-korean-nuclear-test-chinese-reaction.
4. Assistant Secretary Marshall S. Billingslea, "Testimony of Assistant Secretary Marshall S. Billingslea Before House Foreign Affairs Committee on Threat Posed by North Korea," U.S. *Department of the Treasury*, September 12, 2017, https://home.treasury.gov/news/press-release/sm0156.
5. U.S. Department of State, "Risks for Businesses with Supply Chain Links to North Korea," July 23, 2018, www.treasury.gov/resource-center/sanctions/Programs/Documents/dprk_supplychain_advisory_07232018.pdf.
6. The Chinese name of the company is 延边银星网络科技有限公司.
7. U.S. Department of the Treasury, "Treasury Targets North Korea-Controlled Information Technology Companies in China and Russia," September 13, 2018, https://home.treasury.gov/news/press-releases/sm481.
8. U.S. Department of the Treasury, "Treasury Targets Shipping Industry and Other Facilitators of North Korea United Nations Security Council Violations," August 15, 2018, https://home.treasury.gov/news/press-releases/sm458.
9. United Nations Security Council, "Report of the Panel of Experts established pursuant to resolution 1874," February 27 2017, http://www.un.org/ga/search/view_doc.asp?symbol=S/2017/150 (p 76).
10. "The Observatory of Economic Complexity," Massachusetts Institute of Technology, https://atlas.media.mit.edu/en/visualize/tree_map/hs92/export/prk/show/all/2016/ and https://atlas.media.mit.edu/en/visualize/tree_map/hs92/import/prk/show/all/2016/. Wit, et. al., 392.
11. Korea Trade-Investment Promotion Agency, 2015 Annual Report, 14, https://news.kotra.or.kr/user/globalBbs/kotranews/11/globalBbsDataView.do?setIdx=249&dataIdx=151201
12. Ibid.
13. "China-DPRK border trade zone opens," *Xinhua*, 2015, www.xinhuanet.com//english/2015-10/15/c_134717510.htm.
14. Kelsey Davenport, "Chronology of U.S.-North Korean Nuclear and Missile Diplomacy," *The Arms Control Association,* November 2018, www.armscontrol.org/factsheets/dprkchron.
15. "Section 5: China's Evolving North Korea Strategy," *U.S.-China Economic and Security Review Commission*, 2016, p. 414, www.uscc.gov/sites/default/files/Annual_Report/Chapters/Chapter%203%20Section%205-%20China%27s%20Evolving%20North%20Korea%20Strategy_0.pdf.
16. Ibid., 421.
17. Marcus Noland, Stephan Haggard, Kent Boydston, "UN Security Council Resolution 2375," *The Peterson Institute for International Economics*, September 12, 2017, https://piie.com/blogs/north-korea-witness-transformation/un-security-council-resolution-2375. Eleanor Albert, "The China–North Korea Relationship," *The Council on Foreign Relations*, March 2018, www.cfr.org/backgrounder/china-north-korea-relationship.
18. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (Washington, D.C.: Office of the Secretary of Defense, 2018), 113.
19. "The China–North Korea Relationship."
20. Hazel Smith and Timothy Hildebrandt, "Uneasy Allies: Fifty Years of China-North Korea Relations," *The Woodrow Wilson International Center for Scholars*, September 2003, 3.

21. Wang Lu, "Expert Opinion: Facing the North Korean Situation, Anti-War Attempts Still Need Preparations for War," *People's Daily*, March 2017, http://military.people.com.cn/n1/2017/0321/c1011-29158448.html.
22. The full text of the leaked document can be found at ABC news Australia, "China Mobile Refugee Camp Document," December 14, 2017, https://www.abc.net.au/news/2017-12-14/china-mobile-refugee-camp-document/9258494.
23. Oriana Skylar Mastro, "Why China Won't Rescue North Korea: What to Expect if Things Fall Apart," *Foreign Affairs*, 2017, https://www.foreignaffairs.com/articles/asia/2017-12-12/why-china-wont-rescue-north-korea
24. Ibid.
25. *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, 114.
26. Fu Ying, "The Korean Nuclear Issue: Past, Present, and Future: A Chinese Perspective," *Brookings Institution*, 2017.
27. Richard C. Bush, "China's Response to Collapse in North Korea," *Brookings Institution*, January 2017, https://www.brookings.edu/on-the-record/chinas-response-to-collapse-in-north-korea/.
28. Anny Boc, "North Korea and China, Friends Again?" *The Diplomat*, 2018, thediplomat.com/2018/06/north-korea-and-china-friends-again/.
29. Wit, et. al., 404.
30. Ying, 17.
31. Wit, et. al., 405.
32. "Chronology of U.S.-North Korean Nuclear and Missile Diplomacy."
33. Chen Cheng, "North and South Meetings Bring a New Era for Peace on the Korean Peninsula," *People's Daily*, 2018, http://military.people.com.cn/n1/2018/0428/c1011-29956466.html.
34. "Expert Opinion: Facing the North Korean Situation, Anti-War Attempts Still Need Preparations for War."
35. Wit, et. al. 405.
36. "Why China Won't Rescue North Korea: What to Expect if Things Fall Apart."
37. Anna Fifield, "North Korea tries to play Beijing and Washington against each other- and come out the winner," *The Washington Post*, September 10, 2018, www.washingtonpost.com/world/asia_pacific/north-korea-is-trying-to-play-off-beijing-and-washington--and-come-out-the-winner/2018/09/10/11a0cdaa-b4dc-11e8-b79f-f6e31e555258_story.html?utm_term=.45e623b65d1a; and Ana Swanson and Alan Rappeport, "Trump Delays a Tariff Deadline, Citing Progress in China Trade Talks," *New York Times*, Feb. 24, 2019, https://www.nytimes.com/2019/02/24/us/politics/us-china-trade-truce.html.
38. "A different kind of decoupling — China Tip Sheet June 18, 2019," *Trivium China*, 2019, https://triviumchina.com/2019/06/18/a-different-kind-of-decoupling-china-tip-sheet-june-18-2019/.
39. Jennifer Lind, "Will Trump's hardball tactics work on China and North Korea?" *CNN*, August 7, 2017, https://www.cnn.com/2017/08/07/opinions/china-north-korea-opinion-lind/index.html.
40. Maximilian Mayer, "Rethinking the Silk Road: China's Belt and Road Initiative and Emerging Eurasian Relations," (Palgrave Macmillan, 2018), 274.
41. Michael Heng, "If the US military withdraws from Korea, China will be a big loser," *South China Morning Post*, 2018, scmp.com/comment/insight-opinion/united-states/article/2151584/if-us-military-withdraws-korea-china-will-be
42. Tang Lu and Zhang Xin, "Zhou Enlai Twice Warned Japan Against Revitalization of the Military," *People's Daily*, 2018, http://zhouenlai.people.cn/n1/2018/1015/c409117-30342543-2.html. Zhang Ling Bo, "South Korea's next-generation fighter design, expected to fly in 2022, looks exactly like the F-22," 2018, http://military.people.com.cn/n1/2018/0702/c1011-30100217.html.

43. Mark Landler, "Trump Orders Pentagon to Consider Reducing U.S. Forces in South Korea." *New York Times*, 2018, https://www.nytimes.com/2018/05/03/world/asia/trump-troops-south-korea.html.
44. "The Observatory of Economic Complexity."
45. Kim Jong-un, "New Year's Day," *Rodong News*, 2018, rodong.rep.kp/ko/index.php?strPageID=SF01_02_01&newsID=2018-01-01-0001.
46. Steven Lee Myers and Jane Perlez, "Kim Jong-un Met With Xi Jinping in Secret Beijing Visit," *New York Times*, 2018, https://www.nytimes.com/2018/03/27/world/asia/kim-jong-un-china-north-korea.html
47. Xiang Bo, "Xi Jinping, Kim Jong Un hold talks in Beijing," *Xinhua*, 2018, http://www.xinhuanet.com/english/2018-03/28/c_137070598.htm.
48. Yun Sun, "The State of Play in Sino-DPRK Relations," *38 North*, 2018, https://www.38north.org/2018/09/ysun090518/. "China's President Xi completes state visit to North Korea: China state media," *Reuters*, June 2019, https://www.reuters.com/article/us-northkorea-china-xi/chinas-president-xi
-completes-state-visit-to-north-korea-china-state-media-idUSKCN1TM0LE.
49. Shi Jiangtao, "North Korea's invitation to China's Belt and Road summit 'may cast shadow over UN sanctions,'" *South China Morning Post*, 2017, https://www.scmp.com/news/china/diplomacy-defence/article/2093622/north-korea-join-chinas-belt-and-road-summit
50. Bonnie S. Glaser and Lisa Collins, "China's Rapprochement with South Korea," *Foreign Affairs*, 2017, https://www.foreignaffairs.com/articles/china/2017-11-07/chinas-rapprochement-south-korea
51. Selig S. Harrison, "Seabed Petroleum in Northeast Asia: Conflict or Cooperation?" *The Woodrow Wilson International Center for Scholars*, 2005, 44.
52. Ibid., 13.

It's Time to Cyberattack China: New Approaches in Offensive Cyber Operations

Melodie Ha

21st century modern warfare has evolved past the realm of conventional warfare to encompass the information domain. The People's Republic of China recognized the importance of information warfare and cybersecurity in the late 1990s, and has been developing its military to conduct malicious activities in cyberspace in pursuit of its national objectives, including gaining economic advantages through industrial espionage, gathering military intelligence, and garnering influence through coercive means. This article examines the nature of cyberspace as it fits into the greater strategic competition between China and the United States and seeks to explain limited warfare and escalation in cyberspace. It argues that current U.S. postures in cyber defense and deterrence are not enough to change Chinese behavior and prompts alternative offensive approaches from the United States in order to keep its strategic edge in the information competition. The article proposes multiple offensive approaches in dealing with Chinese adversaries in cyberspace and considers the benefits and the costs of U.S. state-sponsored cyber-attacks.

Introduction

China and the United States have entered an unprecedented era of strategic competition in the 21st century that covers the gamut of military, economic, diplomatic, and information domains. As China seeks to gain influence, it has started to utilize the cyber domain in pursuit of its national objectives, with the ultimate goal of vitiating the United States's influence across the globe. As the world grows increasingly connected through globalization and networks, information has become a currency for power and influence. Since the 1990s, the People's Republic of China (PRC) has recognized the centrality of information warfare and network operations in modern conflict. The center of gravity in war has shifted into the cyber and information domains, and China has ambitions to not only catch up to, but also surpass, countries like the United States in cyber capabilities. In the past decade, the PRC has worked to reform and modernize its military with a focus on informationization, a holistic framework that aims to transform China from an industrial society into an information society through the development of information and communications technology industries and applications, information resources, infrastructure, and security.[1]

This article examines the nature of cyberspace as it fits into the greater strategic competition between the United States and China. It examines what China hopes to accomplish in terms of national objectives through the cyber domain, including gaining economic advantages through industrial espionage, gathering military intelligence, and garnering influence through coercive means. First, it is important to understand how China's capabilities and actions align with its strategy and goals. Given that China's goals in cyberspace do not align with U.S. goals, it is difficult to cooperate within this space. Previous attempts at bilateral diplomacy have not been fruitful, and if it is impossible to change China's behavior through cooperation, alternative approaches are necessary.

Within the cyber domain, China has gained an advantage while the United States is falling behind. Previous and current U.S. actions in this space have not deterred or changed Chinese actions in

any significant way. Current strategies put forth by the Executive Branch and the Department of Defense focus on mitigating threats and defending networks and critical infrastructure. Moreover, approaches to offensive or defensive engagement with adversaries lack operational detail and do not elaborate upon the risks of persistent engagement.

I seek to analyze how the United States can take multiple offensive approaches in dealing with adversaries in cyberspace. I hypothesize that a new strategic offensive campaign will be the most effective in countering China and pushing it to moderate its activities, providing the United States with an edge in its strategic competition. However, there are also limitations and risks in taking an offensive posture. Currently, the United States does not have a strategy for offensive cyber operations. Consequently, there is significant value in developing a range of options for enhancing American flexibility and strategic options in cyberspace. This paper offers multiple escalatory approaches and analyzes the benefits and the costs of the different options. It also explains how these approaches might advance U.S. objectives in the competition and hypothesize how China will respond.

In addition to laying out clear policy options for offensive cyber operations, the paper seeks to address the following questions: How can we effectively conduct limited warfare in the cyber domain? Will cyber operations be enough to change and alter China's behavior in this space? And what are the laws of war for dealing with this space?

Key Terms

This essay relies on several key terms. Though there is no common definition for cyber terms used by states and nations,[2] the narrowly defined terms below provide a useful framework for this paper because it considers the U.S. perspective and the damages specific to the U.S. and its citizens.

Cyberspace: The interdependent network of information technology infrastructure which includes the internet, telecommunications networks, computer systems, and embedded processors and controllers.[3] A completely man-made shared domain in the global commons. Used interchangeably with "cyber domain" or "cyber realm." Activities occurring in cyberspace are termed "cyber operations."

Cyber attack: Officially referred to as "offensive cyber operations" (OCO). A cyber operation taken to undermine the functions of a computer network for a political or national security purpose. A cyber-attack may be carried out by means of any action, including hacking, bombing, cutting, infection, but must aim to undermine or disrupt the function of a computer network.[4]

Cyber espionage: A cyber operation to obtain unauthorized access to sensitive information through covert means.[5] Acts of cyber espionage allow the systems to function normally and do not alter or disrupt the computer networks themselves.[6]

Economic or Industrial Espionage: Stealing a trade secret or proprietary information; appropriating, taking, carrying away, concealing, or by fraud, artifice, or deception obtaining, a trade secret or proprietary information without the authorization of the owner. Copying, duplicating, downloading, uploading, destroying, transmitting, delivering, sending, communicating, or conveying a trade secret or proprietary information without the authorization of the owner.[7]

Attribution Dilemma: The inherent covert and deceptive nature of

all cyber operations, which makes identifying the perpetrator behind the operation extremely difficult. There are certain ways to technologically identify perpetrators, either through analyzing the complexity of the operation or the code, as well as identifying the resources necessary to have executed the operation.

Literature Review

Literature on the cyber domain generally suggests that deterrence is difficult due to attribution challenges, the ease at which non-state and state actors can engage in cyber-attacks, difficulties in establishing a red line against cyber aggression, limitations in states' ability to set and enforce international norms, and challenges with escalation control.[8] But despite these challenges, some scholars still believe that cyber deterrence can be achieved through specific and targeted deterrence. Buchanan argues for applying different deterrence models against different actors. Against Chinese hackers associated with Chinese military and intelligence, he supports a restrictive deterrence model, which encourages actors to moderate their behavior to reduce the likelihood of consequences. Chinese actors' exploits are far less disastrous than strategic computer network attacks, as the majority of Chinese attacks involve information gathering and theft.[9] Thus, the credible threat of a retaliatory strike is enough, and an equivalent of a kinetic counter strike is not essential.

Denning similarly argues for specific models of deterrence for different classes of cyberweapons, and deterrence through established regimes. She looks at the Tallinn Manual sponsored by NATO as an international legal framework for establishing rules in cyberspace.[10] However, even these targeted deterrence models and the establishment of international frameworks are difficult to apply against a state like China, which has a nuanced view of deterrence, and simply ignores international law.

Scott Harold, Martin Libicki, and Astrid Stuth Cevallos point out that the Chinese thinking differs from the Western conception of deterrence, which focuses on the fear of potential consequences. China, on the other hand, sees deterrence as a measure of strategic ambiguity designed to magnify the weaker state by expanding the zone of uncertainty about what actions may trigger a response.[11] Adam Segel points out that Chinese military writings suggest cyberattacks have a deterrent effect due to the United States' dependency on banking, critical networks, and telecommunication. Thus, Chinese intrusions are used as a warning to keep the United States out of regional conflicts such as the South China Sea and Taiwan.[12] As such, it is difficult to apply strategies of cyber deterrence to actors like China who perceive it as an entirely different action.

Scholars have countered replacing strategies of cyber deterrence with cyber offense, noting the traditional theory of offense-defense balance. Robert Gilpin argues that offense and defense are distinguished through an economic cost-benefits framework, where developments in favor of the offense means fewer resources will be expended in order to overcome the defense.[13] This is especially true in the cyber domain, where investing in defensive and deterrent capabilities are expensive and not ever guaranteed to work simply because it is impossible to protect the entirety of the internet. Offensive advantages, however, are typically more effective and cheaper. Arquilla notes that the 2007 Estonian cyberattacks cost the perpetrators very little but had a high payoff in terms of disrupting the Estonian government. Krepinevich asserts that cyber weapons, like nuclear weapons, favor the offense due to their extremely compressed timeline and the rapidity at which an attack can be delivered, which places immense stress on the defense.[14]

Some scholars go further to argue that not only is cyber defense and deterrence expensive but also too difficult to achieve. Thus, offensive cyber operations

serve as a better approach for cyber deterrence. Michael Sulmeyer argues that the United States, in seeking to deter its enemies, is falling behind and should be pursuing a more active policy aimed at disrupting their capabilities. Deterrence is insufficient in getting actors to change their behavior. However, he points out that attacks do not need to be aggressive or destructive; they should merely disrupt the hacker's capability to attack.[15]

The Trump Administration has recently embraced an aggressive vision for the cyber domain. The new 2018 Cyber Strategy released by the U.S. Department of Defense envisions a more offensive-minded campaign, with constant, disruptive, "short of war" activities against foreign computer networks. The aim is to engage dangerous adversary activities before they can exploit American networks' vulnerabilities. The Cyber Strategy is a step forward in establishing a new national security framework that acknowledges the proactive use of offensive cyber capabilities, but there are still gaps in both literature and policy addressing the different models of offensive approaches as well as the consequences of attack. Through international frameworks, legal countermeasures exist. One example is the Articles on State Responsibility, which define countermeasures as "measures that would otherwise be contrary to the international obligations of an injured state vis-à-vis the responsible state." However, these countermeasures have primarily been focused on diplomatic actions such as sanctions, and they have not yet been applied to the cyber domain.

My project aims to fill these analytical gaps within offensive cyber approaches, as I seek to differentiate among offensive operations against a nation-state adversary like China. Insofar as Chinese cyber-attacks targeting the United States will not cease in the future, I argue that it is to the United States's advantage to use offensive cyber-attacks against China in this greater strategic competition.

China's Perspective on Cyber War

It is important to establish that China and the U.S. view the concept of "cyber warfare" through different lenses. Interestingly, the Chinese do not even have an equivalent word for "cyber" in Mandarin, often using the English loanword *saibo*. Instead, China focuses on the significance and power of information, seeing cyberspace as a domain in which to conduct operations to maintain dominance over information.

The Chinese view themselves as what is best translated as a "cyber superpower" (网络强国). This term stems from the fundamental principles of Confucian social thought, which prioritizes the power of the state and society over those of the individuals.[16] Confucianism asserts that the rightful power of the government knows no formal restraints vis-a-vis its citizens, and a government restrained by law is a threat to the regime.[17] China utilizes this traditional framework to view the cyber domain as another space where it can apply its form of governing with Chinese characteristics. Chinese leaders see their primary responsibility as controlling information in this domain. From their perspective, the significance of information goes far beyond the cyber realm; it is about establishing "information dominance."[18] In order to establish information dominance, the Chinese believe they need to wage information warfare, of which cybersecurity is only a small subset. Information warfare encompasses a whole range of information and military options, from electronic warfare, network warfare, to psychological warfare.

This strategic concept is applied to the way the People's Liberation Army (PLA) envisions the future of cyber operations. The Gulf War served as a wake-up call for China to push for military modernization. America's high-tech weaponry raised the effectiveness of their use to previously unimagined levels through precision guidance, computer grids, and information networks.[19] China was shocked at the level of joint operations the U.S. was able

to achieve and quickly realized that the Chinese armed forces needed to rapidly upgrade their air defenses, networks, and technical capabilities not only to compete with the rest of the world but also to defend their country.

The PLA recognized how important networked and joint operations were in modern warfare and started developing a future force that is capable of conducting "local wars under informationized conditions" and able to "secure dominance" in the electromagnetic domain.[20] To that end, the PLA has established the PLA Strategic Support Force (SSF), an entity that envisions operations under the umbrella of integrated network electronic warfare (INEW).[21] The force would be in charge of combined use of cyber operations, electronic warfare, information operations, and kinetic strikes in adversary's C4ISR.[22] In essence, SSF serves as the leader and organizer for Chinese information warfare. It serves as a central command and control mechanism that consolidates and enhances all the different objectives the PLA is looking to achieve. This integration of information warfare capabilities is not only consistent with PLA doctrine, but also reflects China's rapidly improving capability to conduct integrated joint operations.[23]

China wages information warfare through a concept called the "Three Warfares" (三站); public opinion warfare, psychological warfare, and legal warfare (or lawfare). Psychological warfare exploits information by drawing upon political, economic, and cultural elements of power. Legal warfare builds psychological support among bystanders and seeks to constrain an opponent's will by limiting his or her options. Public opinion warfare persuades audiences of China's objectives and the righteousness of Beijing's cause while, at the same time, undermining China's adversaries.[24] All three forms of warfare seek to take various types of information to exploit and manipulate in order to achieve China's political objectives and gain an advantage. This is why the cyber domain is crucial to winning China's initiatives both domestically and abroad.

Chinese literature suggests that cyber deterrence cannot be achieved unless there is centralized management, a high degree of command and control, and effective organization. These objectives provided the impetus for the creation of the SSF in 2015.[25] In addition, Chinese literature puts forth the idea that, if an enemy initiates an attack, China should immediately and effectively retaliate through a targeted strike, such as penetrating adversary telecommunications networks, flooding networks with Chinese propaganda, and attacks against critical infrastructure. Moreover, successful deterrence would be enacted both during peacetime and wartime.[26] This literature reveals several aspects of Chinese perspectives. First, China has already created the conceptual framework of how offensive cyber-attacks will serve deterrence purposes. Second, the use of propaganda aligns with Chinese notions of "information warfare" to include psychological operations to influence public opinion. Finally, China believes the United States and its cyber capabilities are the most threatening and destabilizing to the CCP regime. Snowden's leak put America's significant cyber capabilities into perspective, compelling the Chinese to develop a strong, offensive cyber force.[27]

The other noteworthy aspect of China's information warfare campaign is its vision of a closed internet. Beijing refers to this as "national cyber sovereignty," where it believes countries should "choose their own path of cyber development, model of cyber regulation, and internet public policies."[28] In other words, the Chinese believe in controlling cyberspace like any other domain or territory. Furthermore, their approach stipulates that the cyber domain must be monitored and controlled carefully in order to protect the rule of the Chinese Communist Party (CCP) and preserve domestic stability and national security.[29] Not only does the Chinese leadership need to counter

foreign influence and interference but they also need to prevent domestic opponents from creating and spreading unrest, which means monitoring social media platforms to prevent the spread of potential protests.[30] Further objectives in this space include effectively propagandizing achievements of the CCP in economic and development areas, using technologies to guide online public opinion, preventing mass incidents and public opinion from becoming online ideological patterns and issues, and making the space cleaner.[31] All of these objectives are the result of the CCP highly policing citizens' actions and communications in the cyber domain, which demonstrates a strong leadership and a top-down governmental approach.

As China seeks to push this vision forward domestically, it is also attempting to operationalize its concept of cyber sovereignty at an international level. This is most prevalent in the Shanghai Cooperation Organization's 2015 letter to the United Nations on cyber norms, where member states, including China and Russia, rejects NATO's cybersecurity framework in place of an alternative framework. The language in the letter cleverly uses the UN Declaration on Human Rights to mask China's definitions and intentions within the cyber domain, which stipulate that no country should intervene in another country's sovereignty and attempt to influence a country's regime. This is, in effect, China's way of using lawfare to change the global conceptualization of cyberspace to favor the restrictive Chinese model of "cyber sovereignty."[32]

The Chinese believe that Western notions of democratization and liberalization are a constant threat to China's political security and the CCP's hold on power. This is especially prevalent in the Chinese conception of "political warfare," where information dominance is essential. Political warfare is waged through strategic communication tools, including radio, the internet, news organizations, and television.[33] It uses information to coerce and attack opponents, impose psychological pressure, and influence perceptions. As modern technologies continue to blur the lines between peacetime and wartime, informationized warfare has also reached into the civilian realm in society, domestic and abroad.

American Perspective on Cyber War

The United States views cyber power from a very different perspective than the Chinese. Whereas the Chinese are preoccupied with the notions of central command and highly regulated control of the space, the U.S. derives its concepts from its values as a western liberal democracy, which prioritizes freedom of speech, expression, and privacy.[34] The U.S. envisions an open and free internet, and actively works to protect the economic and social values of the internet without stifling innovation, and to promote an interoperable, reliable, and secure space. This fundamental contrast in principles shifts the way the U.S. thinks about operations in this space.

First, the U.S. has a much narrower view of what cybersecurity encompasses; it separates cyber warfare from electronic warfare and information warfare and develops different strategic doctrines for each form of warfare. The U.S. believes cybersecurity generally means protecting communications and other critical networks from unauthorized access,[35] and it is primarily focused on threat mitigation. U.S. Cyber Command's vision to achieve cyberspace superiority is defined as efforts to "defend forward as close as possible to the origin of adversary activity, and persistently contest malicious cyberspace actors." This would include scaling to the magnitude of the threat, working quickly, and maneuvering to counter adversaries.[36] This sets aside a strategy for employing offensive and defensive engagement with adversaries, but the vision elaborates very little on what these engagements look like operationally, and what the risks of "persistent engagement" entail.

Second, the U.S. holds a disjointed vision on operations, where it will integrate only some conflicts into joint operation planning if necessary. Organizationally, the U.S. is not as streamlined or as integrated as the Chinese. For example, Cyber Command was elevated to be independent of NSA under the Trump administration, and soon the "dual-hatted" leadership will be split into two different leading individuals. The newly elevated Cyber Command removes Strategic Command from the formal line of communication between the secretary of defense and the commander of Cyber Command.[37] This organizational move is meant to increase efficiency and speed in reporting or responding to a cyber-attack. However, the different organizations still maintain separate and parallel chains of command. Unlike China's SSF, which consolidates the PLA's military capabilities of new-type force development, space, cyber, and electronic warfare, U.S. organizations have no overarching command center to oversee and control all activities in this space.[38]

Third, the U.S. highly values individual privacy in its cybersecurity strategy. Technology companies work to protect users' privacy and communications online, and privacy rights are recognized under the U.S. Constitution, resulting in multiple cases of big American tech companies bumping heads with the U.S. government over issues of national security and individual privacy.[39] In contrast, the ruling of the CCP is deeply woven into the institutional fabric of the Chinese economy; the government forces all Chinese technology companies to cooperate with it, allowing for streamlined civil-military fusion and access. Chinese civil-military fusion blurs the distinction between defense and commercial activities and boosts the involvement of Chinese private companies in national defense, where many Chinese cyber militias are comprised of IT companies, scientists, and network engineers.

Finally, the reason the U.S. approaches cyber security from such a technical standpoint, unlike China, is because it does not want to subsume everything under the umbrella of information warfare. This is also the reason why the U.S. struggles to formulate responses to adversary aggression in the cyber domain. The narrow perspective by which the U.S. views cybersecurity prevents it from developing an effective way to respond to cyber-attacks.[40]

The Failure of Cyber Diplomacy

The United States and China have fundamentally different principles and values when it comes to approaching strategy in the cyber domain. As discussed above, the U.S. values freedom, access, and privacy. China values leadership and control. Consequently, the strategic doctrine stemming from both countries in using cyberspace to achieve political objectives is also vastly different. However, because the domain of cyberspace is a shared commons, countries must inevitably work together and cooperate. Is diplomacy in this space possible, and how can two countries with contrasting values work together to develop international norms?

While the U.S. envisions a space where everybody plays under fair and reasonable rules, China believes that the U.S. holds an unfair advantage in governing the space; China frequently complains that the U.S. holds complete control over formulating and managing internet standards of all international organizations and core industries.[41] Beijing stresses that every individual country has its own right to develop a model of regulation in cyberspace, and that no country should pursue cyber hegemony, interfere in other countries' internal affairs, or undermine other countries' national security.[42] In part, Beijing is using this to justify its own actions in policing domestic cyberspace, but it is also pushing back against the Western efforts on cyber norms development. Beijing's end goal is to eliminate threats to regime legitimacy and to extend Chinese influence globally in this domain.

Washington and Beijing have engaged in multiple rounds of cyber diplomacy to establish norms. At the World Internet Conference in 2015, China voiced its view that the world needed new rules on internet governance. Ideas of sovereignty, authority, non-interference, and quality were all discussed. However, the U.S. and China still need to engage in the issue of Chinese hacking into U.S. companies to carry out IP theft. Washington consistently seeks to persuade Beijing to acknowledge and enforce norms against state-sponsored commercial cyber theft. Beijing's initial strategy was to deny U.S. accusations of IP theft, but when Edward Snowden disclosed classified information on U.S. spying practices, it gave China an opportunity to criticize the U.S in turn.

Finally in 2015, U.S. President Barack Obama and Xi reached an agreement that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property."[43] Cyber espionage, it was decided, was accepted as a norm since espionage has always been a part of a country's military operations going back in history. IP theft and economic and industrial espionage to gain advantage in one's own industry, however, was deemed egregious. Despite this agreement serving as a huge step forward for China and the U.S. to come to terms with the same principles in the cyber domain, both Chinese IP theft and cyber-attacks have continued to this day. U.S. accusations and indictments of continued Chinese cyberattacks have prevented the two countries from producing effective dialogue on the subject, lending further credence to the notion that diplomacy within this space is fruitless and difficult, if not impossible.

The Strategic Competition: Why China Hacks

Since opening to foreign trade and investment in 1979, China has seen unprecedented growth and development. China is on its way to surpass the United States as the largest economy in the world, and it boasts the world's largest military. Its gross domestic product growth rates averaged 9.5% through 2017, and China has been able to successfully lift 800 million people out of poverty. As China's economy grows and becomes more interlinked with the global economy, China also sees a need to expand its military to protect its economic interests. China argues that its naval expansion out in the Indian Ocean Rim and its militarization of the South China Sea are all to protect its maritime trade routes. To do this, China sees the necessity of modernizing its military capabilities to attain a blue water navy and highly capable information technology. The United States and its allies and partners in the region, however, perceive China's increased military spending and aggressive military actions as a threat to the stability of the Indo-Pacific. In a classic manifestation of the security dilemma, the United States perceives China's rapid military modernization as an attempt by Beijing to displace the U.S. world order. 2018 marked the 40-year anniversary of China's opening up to the world, and its current leader, Xi Jinping, is intent on continuing China's growth trajectory. In particular, he is prioritizing high technology and innovation for furthering economic and military growth. National strategic plans such as Made in China 2025, China's plan to build the world's most advanced and competitive economy through innovative manufacturing technologies like artificial intelligence, and Xi's ambitions for the PLA to be a fully informationized and world class military by 2050 all depend on China's ability to modernize and use cutting-edge technology.[44]

There are three main drivers behind China's cyber operations that explain China's strategy in the greater competition: 1) China's desire to close the technology gap between itself and the United States, 2) its goal to rapidly modernize its military platforms, and 3) its desire leverage in information warfare.

China's desire to advance technologically derives from its interpretation of U.S. activity in cyberspace. Beijing truly believes that there is a race to develop a centralized command structure in this domain, and they see U.S. Cyber Command as a destabilizing progression towards a new Cold War mindset, which is also why they see such urgency behind the need to informationize.[45] Thus, this information competition is also the prime reason China relentlessly engages in intellectual property theft, because Beijing does not want to get caught in the technology trap. At the same time, due to China's desire to decrease its dependency on other countries, China is making great strides in areas such as quantum computing and artificial intelligence. However, most Chinese producers are still not able to produce high-tech products. [46] As a result, China relies on tools in the cyber domain to maintain that edge in technological innovation—through economic and industrial espionage.

China's push to obtain advanced military platforms is hindered by the fact that the country still struggles with producing advanced technology indigenously. Stealing information gives China the potential to acquire technology or platforms that the United States is unwilling to sell.[47] As a result, China specifically targets U.S. defense contractors that produce military platforms for the U.S. military for IP theft. PLA hacking groups like Unit 61938 and 61486 have reportedly stolen information from dozens of Defense Department weapons programs, including the Patriot missile system and the U.S. Navy's littoral combat ship.[48] In 2009, Chinese hackers spear phished Boeing employees and stole 630,000 files from Boeing related to the C-17 military transport aircraft, with research and development costs of up to $3.4 billion USD.[49] The information stolen included detailed drawings, measurements of the plane, outlines of electric systems, and flight test data. Most notably, China's J-31 stealth fighter, which looks eerily similar to Lockheed Martin's F-35, is believed to have been partly derived from the plans of the U.S. warplane, which was obtained by Chinese hackers.[50] Though attribution for these cases is still difficult, China remains a prime suspect.

China also sees big data collection and surveillance as a form of leverage in the greater information war. The CCP's control over information is not only pervasive in its domestic politics but also serves as the primary objective in China's activities on the international level. Though China internally monitors its own citizens in an attempt to control them, China believes the same strategy of controlling information applies internationally. It is one of the prime reasons Beijing conducts cyber espionage operations—to gather data that it can eventually use as leverage. In April 2015, the U.S. Office of Personnel Management (OPM) realized that a foreign agent had infiltrated and stole millions of files, including Standard Form 86, a 127 page questionnaire for federal security clearances that detail very probing questions for some of the government's most secretive jobs, personnel files of over 4.2 million employees, and 5.6 digital images of government employee fingerprints.[51] Cybersecurity experts analyzed the malware used in the attack and recognized the program as one that is commonly deployed by Chinese-speaking hacking units. This program has also consistently shown up on computers used by enemies of the Chinese government, including Hong Kong and Tibetan dissidents.[52] Computer security experts are fairly confident in attributing the OPM hack to China, but have refused to acknowledge China officially. More importantly, the U.S. does not know what the hackers' intentions are with the stolen data, which remain a massive security threat. Some theories involve Chinese plots to recruit agents, to blackmail government operatives, and more. Either way, the Chinese can put this information to use in the future as leverage against the United States.

Finally, one would be remiss to not consider China's pursuit of cyber

capabilities to degrade U.S. warfighting capabilities in times of conflict. Though there is little direct knowledge of the kinds of operations the Strategic Support Force would lead during times of war, it can be assumed that the SSF would have a major role in supporting the rest of the PLA military services. The Joint Staff Department's Network-Electronic Bureau, now under the SSF, seems to be pushing the INEW concept, likely overseeing force development and warfighting efforts in the SSF, other services, and theater commands.[53] These could include disabling adversary communications' systems, degrading adversary military networks, and more.

Current U.S. Approaches

The United States has addressed the importance of cybersecurity in various published strategy documents and in policy implementation in current and previous administrations. The Trump Administration in the 2018 National Security Strategy and National Defense Strategy has, for the first time, specifically called out China and Russia as strategic competitors, something that previous administrations have not done. [54] Moreover, the Cyber Strategy released by the Department of Defense in October 2018 focuses on building a more lethal force to move toward offensive cyber operations. Despite these recent strategic shifts, much of U.S. cyber strategy focuses on deterrence and defense. It does not provide a framework for responses to cyber-attacks.

By aiming to only broadly deter its enemies, the United States will constantly be one step behind in the cyber domain. Deterrence does not work in the cyber realm as it does in the physical domains of war; state-sponsored cyber attackers especially often operate with virtual impunity.[55] For deterrence to work, the enemy must be denied success or at least perceive costs to outweigh the benefits of acting, which means establishing defenses in networks. However, in the cyber domain, an insurmountable defense is impossible, as an attacker will always find a way to penetrate the network.[56] In addition, deterrence does not apply in a domain where the attackers are conducting long-term persistent campaigns, especially espionage campaigns that are cloaked in deniability.[57] Thus, something apart from defending networks must be done in order to form a successful deterrent strategy.

For the first time, the United States has publicly announced successful OCO on adversaries. Prior to the midterm elections, the Pentagon launched a cyber-attack to deter Russian interference. U.S. Cyber Command targeted Russian operatives, including military hackers and trolls financed by Russian oligarchs, and informed them that the U.S. military was actively tracking their activities. This semi-covert messaging was intended to inject friction and fear into the ranks of Russian operatives to not take action during the elections.[58] U.S. military officials stated that new authorities approved last year to allow Cyber Command be more aggressive and effective in what they privately say was an apparent success at deterring Russian operatives.[59]

General Paul M. Nakasone, currently the dual-hatted commander of both Cyber Command and the NSA, has stated that the United States needs to shift from a posture of waiting for adversaries to come to it and instead work to actively defend, conduct reconnaissance, and understand its adversaries' capabilities and intents.[60] Furthermore, Nakasone posits that if the United States wants to have an impact on an adversary, it would have to *persistently engage* with that adversary. Persistent engagement requires that the United States be in constant contact with its adversaries in cyberspace. Success is determined by how it enables and acts. The concept of persistent innovation involves the maintaining of tools, tradecraft, and techniques to keep pace with adversaries.[61] Of these concepts, persistent engagement would

mark the shift of U.S. cyber strategy into offensive operations.

This engagement would also need to be tailored in ways to impose costs based on the particular adversary, which would include a combination of deterrence, defense, prevention, and resilience. The most important aspect of successful OCO is signaling within the domain, which is strategically difficult to accomplish because it is impossible to know how American adversaries are interpreting the signal.[62] However, the fact that new U.S. documents and public announcements state U.S. offensive capabilities is already changing the way American adversaries perceive the U.S. in the cyber domain. As such, it is necessary to expand on these capabilities to send the clear message to American adversaries what the United States military is willing to accomplish in this space. The next section expands upon the different types of offensive approaches to take within this space, ranging from degrading adversary capabilities to targeted espionage and leak campaigns.

A New OCO Playbook for China

Currently, America's OCO track record is limited to successfully disrupting Russian interference. In the case of China, a vastly different adversary, the U.S. has not been able to signal clearly its intent nor its capability. The Chinese would categorize the U.S. cyber-attack on Russia as a provocative "active defense" attack, with the intent of protecting U.S. objectives by use of offensive capability, which in turn deter Russian actions.[63] Though a recent unnamed U.S. official has stated that U.S. intelligence and cyber soldiers have begun to conduct cyber-counterattacks against Chinese military and intelligence targets, details on operations remain classified.[64]

The strategy I will put forth here is primarily along the concept of "active defense," with the two aims being 1) getting China to change their actions in the space by using OCO and 2) using OCO to degrade Chinese capabilities through denial. This strategy would have elements of both deterrence and compellence, but differs from a warfighting cyber strategy, which would aim to inflict as much damage as possible on an adversary. Thus, approaches in an active defense strategy would aim to keep the conflict under the threshold of all-out war and seek to avoid escalation into the realm of conventional or nuclear warfare. However, because these approaches are highly escalatory and provocative towards China, there are still risks that engagement that may go beyond low-intensity conflict due to misperceived signals or fear within the domain.

In addition, these approaches would be limited to the national strategy level, focused on how the United States as a nation-state would conduct operations on China and change the calculus of the CCP. U.S. actors would thus primarily be military, including the NSA, Cyber Command, and the service branches' own cyber commands. Because cyber as a domain is understood to be easily accessible by individuals and groups, a national strategy aimed at changing the actions of Chinese individual hackers, for example, will not be very effective. These approaches will serve as a response and broad guidance for cyber-attacks carried out by China on a nation-state level. Attacks perpetrated by nation-states, such as the OPM hack, are relatively easy to discern from a technical standpoint due to the complexity of attacks and the advanced source codes. So far, nation-states are the only actors that have the time, money, and talent that is needed to plan and execute advanced and sophisticated cyber-attacks.

Finally, the key is to keep in mind who the U.S. adversary is and how the United States can inflict the most effective amount of damage while sustaining minimal damage to itself. In order to successfully inflict asymmetric harm, considering what China and the CCP value politically will be important. Given these caveats, I

offer a few approaches on how the United States can tailor OCO against China.

The "Beijing Papers"

This approach would be akin to the "Panama Papers," a leak consisting of 11.5 million files that detail how rich individuals from all over the world exploited secretive offshore tax regimes. Twelve national leaders were implicated, including Vladimir Putin, the president of Russia.[65] Nominally, this approach would be classified as primarily cyber espionage.

The U.S. intelligence community would work together to gather financial information on the CCP's senior officials and leading executives in China's business world, specifically seeking out individuals who are involved in corruption scandals including fraud, tax evasion, embezzling government funds, etc. Once enough information is gathered through traditional cyber espionage methods, the "Beijing Papers" could be released to independent media outlets around the world, as well as multiple channels in the Chinese media and on the Chinese internet.

A leak on this scale could have several effects. First, on the international stage, it would discredit the CCP and Chinese leadership. Similarly, on the domestic stage, it would foster distrust between the CCP and the people. Second, under Xi Jinping's own anti-corruption campaign launched in 2012,[66] the Beijing Papers could spur an even more robust crackdown on corrupt officials, or at least bring to the public eye who these people are. This would be especially pertinent if the Beijing Papers could reveal corrupt officials who are currently being protected by the CCP leadership, particularly Xi loyalists.

The objective of this type of leak is not to bring Xi Jinping or the CCP regime down, but to inject doubt into the Chinese leadership and force transparency from the notoriously opaque CCP. The question now remains, will the Chinese populous actually care about a scandal like this, and would it have an impact? Scholars argue that Xi's anticorruption campaign has already made the Chinese public deeply suspicious of the leadership.[67] Moreover, the Tiananmen Papers released in 2001 have already gone this route; the papers detailed decision-making at the highest levels of government, particularly during the 1989 Tiananmen crackdown, and revealed the battles between the reformers and the ideologues in the Party.[68] The Tiananmen Papers were not particularly effective in causing domestic unrest as the book was denounced as fake by the CCP and banned in China. Based on these facts, it is unclear what kind of domestic unrest the Beijing Papers would foment, and how much of a disturbance it would actually cause.

Finally, would the Beijing Papers actually achieve U.S. objectives of changing China's behavior? For one, the timing of the leak could be strategic as a deterrent factor. Donald Trump has accused the Chinese of influencing and meddling in the November 2018 midterm elections through propaganda in newspapers.[69] If Chinese influence remains a concern in future U.S. elections, a well-timed leak prior to elections would serve as a strong message to the CCP that any interference would be unacceptable, not to mention the leak would create a distraction and force the CCP to focus on domestic issues at hand. Though a leak might not ultimately change Chinese behavior in the long run, it at least sends a strong message that the United States is capable of gathering sensitive information and that it holds leverage. Similar to the cyberattack against the Russian operatives prior to the 2018 midterm elections, this approach would serve as an "active defense" measure.

Though the Beijing Papers approach may not prove to be very effective, it holds fewer escalatory risks. The biggest risk is the attribution factor; in order to effectively send a deterrent signal, the United States would have to own up to the leak. This may result in backlash from China, who may deem it necessary to escalate horizontally and hit back with economic

sanctions, visa restrictions, or other punishments outside the realm of cyber. Alternatively, the Chinese could hit the U.S. back with a "leak" of their own, based on all the information they have acquired on U.S. citizens from the various hacks they have perpetrated. The other option, of course, is to keep the attribution vague. However, then the United States would not be able to send a message or achieve its objective of changing how the Chinese interact with the United States in cyberspace.

The Fall of the Great Firewall

This approach would be classified as a cyber-attack, as U.S. cyber forces would aim to penetrate, disrupt, and undermine Chinese censorship networks. Specifically, this would mean attacking the Ministry of Industry and Information Technology, which controls and licenses all internet service providers in China, and thus monitors and manipulates all content in and out of China.[70] As noted earlier, the CCP uses the Great Firewall to keep out foreign influence, specifically Western ideologies, but they also utilize it to quash domestic dissent and criticism.

Executing an attack like this would strike China in a critical area where it maintains a tight hold. The Great Firewall is integral to the CCP's control over the country, and taking it down would be akin to undermining the regime's control and leadership. An attack like this would send a stronger political message than it would have an operational effect. It is preposterous to assume that by bringing down the Great Firewall, Chinese internet users will suddenly embrace democratic values and believe the truth of what happened at Tiananmen in 1989 by consuming western news media. Thus, the significance of this attack would be sending a clear political message to the CCP—that the United States is attacking the legitimacy of the regime. However, it must also be made clear that an attack like this is not supposed to bring down the communist regime, as that is not an American objective. This attack denies Chinese censorship capabilities and sends a strong signal that the United States can strike China where it hurts and will do so again if China continues to perpetrate cyber-attacks.

This approach follows a compellence and deterrence strategy, where the United States inflicts punishment on China to force it to change its behavior. The continued tacit threat that the United States is capable of attacking the Great Firewall again in the future could also deter China from bad behavior. There is a greater possibility that we would observe a shift in Chinese calculus in the cyber domain due to harm that the CCP incurs in an attack like this. However, there is also an increased risk of horizontal and vertical escalation or an offensive cyber response from China. Both risks and change are only possible if the United States again owns up to the attack.

"Fighting Fire with Fire"

The age-old adage, "an eye for an eye," best describes this approach. It is time to do exactly what China has repeatedly done to the United States—conduct economic and industrial espionage and target Chinese companies through OCO. In 2016, the Council of Economic Advisers estimated that the United States lost between $57 and $109 billion in damages due to malicious cyber activity. These attacks are both conducted by Chinese state-owned enterprises and the Chinese government. It is estimated that the U.S. economy loses over $300 billion of revenue to IP theft annually, with China perpetrating 50-80% of all IP theft cases.[71]

China has been developing advanced technology in multiple areas, including quantum computing and artificial intelligence. In 2017, China was able to successfully use quantum particles to send secure messages from a satellite to its ground stations, a huge stepping stone in virtually unbreakable communications networks and eventually, a space-based quantum internet.[72] The United States,

on the other hand, has been lagging in quantum technology; only last year Congress was urged to pass bills that would establish new federal programs to advance quantum technologies.[73] The United States could infiltrate the networks of Chinese technology companies and government institutions working on quantum technology and steal sensitive project information and data. This information could be used to not only further U.S. innovation within these fields but also provide insight into what the Chinese are working on. Using this information, the U.S. could determine methods to preempt those technologies in the future. Apart from advanced technology, other fields the United States could possibly investigate are more traditional forms of military technology, including China's hypersonic missile technology, and the new short range anti-ship ballistic missiles, the CM-401.[74] Taking data from these military technologies could also help the United States understand Chinese capability, and in turn inform its strategies to counter for example Chinese A2/AD in the South China Sea.

While conducting economic and industrial espionage to better understand Chinese military capability and strategy absolutely gives the U.S. military an edge, stealing information to advance America's own technologies can lead to a series of other issues regarding operations security (OPSEC)[75], and competition between U.S. private companies. Because the U.S. defense industrial base is dominated by private businesses, it is not the role of the government to provide classified information to specific businesses to further their profits.[76]

Finally, according to the Department of Defense's Law of War Manual, because "cyber espionage resembles traditional peacetime intelligence and counterintelligence activities, such as unauthorized intrusions into computer networks solely to acquire information, such cyber operations would likely be treated similarly under international law."[77] Thus, hacks such as OPM are illegal, but because they are classified as cyber espionage, nation states file it under the laws for intelligence and espionage. IP theft, on the other hand, most certainly is a federal crime under U.S. laws.[78] However, the way to circumvent this is the attribution dilemma; the United States could simply deny any involvement.

This approach is different from the previous two in that there is no overt political signaling involved. In fact, the United States would not want to admit these acts unless it wants to face international backlash on violating its own laws and principles. The significance of this approach lies at the core of the strategic competition—the United States has already identified China as a strategic competitor on the national level, and this approach serves as a more aggressive tool for the United States to maintain the upper edge in terms of both civilian and military technology and development.

While there are fewer risks of horizontal escalation with this approach, we can be sure that China will respond, either through publicized accusations or threats. However, insofar as the attribution dilemma in this scenario protects the United States, as long as China does not have proof that the attack links back to the United States, deniability will provide protection from backlash.

On the other hand, this approach does not offer a solution to the persistent problem of economic and industrial espionage at all, but rather escalate the rate at which IP theft occurs between both nations. The only real way to mitigate this problem is to put the burden and responsibility of responding to IP threats on U.S. private companies themselves. Currently, U.S. companies are afraid to come forward about Chinese cyberattacks or hacks due to business interests in China. Thus, companies will often complain to the government about Chinese attacks, but also prevent the government from responding to them.[79] It is possible for the U.S. government to pass a law and significantly raise the costs for

these companies, which could provide the necessary incentive for private companies to actually care about and invest in network defenses.[80]

The "Stuxnet" Approach

This final approach is the most aggressive form of OCO, which would involve physical damage from a cyber-attack. Potential targets could include critical infrastructure, such as the electricity grid, water supply, public transportation, and more. Sweeping attacks that cause real-world damage are not unheard of, but they are extremely rare. For example, in 2010, reports of the Stuxnet virus were uncovered. This computer worm was designed to specifically infiltrate and attack the centrifuges in Iran's nuclear facility at Natanz. Due to its sophistication and complex code, it was originally suspected that the United States and Israel were behind the attack. This was confirmed eventually through a series of leaks from senior U.S. officials.[81] In another instance in December 2015, suspected Russian groups hacked into the Ukranian power grid by remotely taking control of the facilities' SCADA systems, effectively shutting off electricity for over 200,000 consumers.[82]

The Stuxnet worm proves that the United States possesses the offensive capability to take down critical infrastructure through cyber-attacks. If these capabilities are aimed at China, the United States would be able to cause real damage. Targeting China's transportation system in urban areas could potentially disrupt and even destroy lives. Cities like Beijing and Shanghai that have populations of over 25 million people could be prime targets. However, it is unlikely that the United States would execute an attack of such scale against China. Realistically, the United States could target known military facilities, particularly those of the SSF and specific hacking units to *degrade* their capabilities continuously over time to prevent China from continuing the APT. If the United States can execute this strategy of denial well enough, it will sufficiently incapacitate Chinese offensive capability, which means China will not be able to fight back in cyberspace. This kind of targeted approach is most similar to Stuxnet.

An approach like this falls more into the "warfighting" category than the "deterring and compelling" category, which increases risks of escalation exponentially. Conflict would no longer be limited to the cyber domain and could easily cross over the threshold of all-out war. Under the United States's own definitions in the Law of War Manual, cyber operations that "trigger physical effects would be regarded under traditional uses of force in *jus ad bellum*." Moreover, "operations that cripple military's logistics systems and the ability to conduct and sustain military operations are also considered a use of force."[83] Thus, it is very likely that China could respond in a physical manner as well, either through conventional forces or though the cyber domain.

To this day, we have yet to see cyber-attacks on critical infrastructure escalate to conventional war. The result of Stuxnet led to a cyberattack on U.S. banking institutions from Iran, but nothing more severe than that.[84] This is partially due to the fact that we have yet to see cyberattacks that have caused loss of life and the fact that many effects of cyberattacks, albeit physical, are still short-term effects. As a result, it is reasonable to assume that a carefully targeted cyberattack on Chinese military facilities aimed at degrading Chinese military networks and capabilities would not escalate into armed conflict. It is also possible that the Chinese simply do not have the offensive capabilities to launch a similar cyberattack against U.S. critical infrastructure or military networks, and thus respond in other horizontally escalating measures.

The objective of an attack like this would not necessarily be to change Chinese behavior in cyberspace, but rather to work to continuously incapacitate Chinese cyber capabilities. If the United States is

relatively certain that China does not possess the same offensive capabilities and it is able to keep the conflict from escalating outside the realm of cyber, this would be the most effective approach at getting China to stop its cyber operations.

Cyber Espionage

Finally, the United States should continue its intelligence and counter-intelligence activities in cyberspace. Under the Law of War Manual, these cyber operations would be treated similarly under international law to traditional intelligence methods, with the understanding that these operations can be considered as hostile acts.[85] Thus, these cases are not illegal, but could increase bilateral tensions if breaches are detected, as occurred in the OPM hack.

While the United States did not formally respond to this case, it is possible for the U.S. to take countermeasures on Chinese cyber espionage under international law. The Articles on State Responsibility define countermeasures as "measures that would otherwise be contrary to the international obligations of an injured state vis-à-vis the responsible state . . ."[86] The United States could formally identify China as the state responsible for the OPM hack and the resulting damages. Then, the U.S. may use active defense as a countermeasure, which can take the form of sanctions or a withdrawal of trade. This offers an official remedy through the use of countermeasures, though it is potentially more politically risky. The few reasons why the United States would not formally name China are, in fact, political. First, the U.S. administration may not want to increase tensions in the already delicate bilateral relationship. Second, state-on-state espionage is still acceptable and different from economic industrial espionage. Third, by not naming the attack, the United States can secretly retaliate in a similar cyberattack without having to worry about political blowback.

Conclusion

After analyzing five different approaches on how the United States could actively engage with China in the cyber domain, it is difficult to determine whether conducting offensive cyber operations will ultimately change Chinese behavior in this space. We see many nuanced arguments as to how more offensive operations can cause more damage and send a stronger political message. These are all effective compellence strategies, using punishment to impose costs and force an adversary to change its behavior. Once the behavior changes, the punishment would also stop, but the threat and capability to inflict damage in the future would serve as a deterrent to future bad behavior as well. These strategies are not new, but merely adapted to the cyber domain. Taking down the Great Firewall and attacking China's military facilities all fit within this strategy. However, there are also clear drawbacks in terms of horizontal and vertical escalation in very single scenario.

Despite significant frictions, the U.S.-China relationship is still one of the most important bilateral relationships that the United States maintains, as the two countries are interdependently linked through the global economy. Any attack would come at a political and economic cost, and the United States needs to carefully weigh the cost of a cyberattack in relation to how effective the attack would be. Granted, there are also ways for the United States to mitigate those costs through unclear messaging and denial of attribution. This would also undoubtedly decrease the ultimate effectiveness of a compellence and deterrence strategy.

On the other hand, this paper provides multiple approaches under the umbrella of cyber espionage. It is even less clear that these operations would force China to change its behavior, but they would at least help maintain the United States's edge in the broader information war. Finally, it needs to be acknowledged that all these

operations could already be occurring within cyberspace, and the public simply may be unaware. There is already some evidence that the United States is conducting such operations against the Chinese, but the cyber operations remain covert and highly classified. The only reason we even know of cyberattacks like Stuxnet is due to leaks to the media.

In conclusion, I advocate a two-pronged strategy for conducting offensive cyber operations against China. First, acts such as degrading Chinese military capabilities in cyberspace and obtaining intelligence would effectively provide an edge for the United States in the greater strategic competition. Second, the combined political signaling behind these actions could push China back to the negotiating table where both countries can work together to establish norms and a framework for dealing with this conflict, although this may be difficult due to fundamentally different perceptions on cyber norms.

It is widely acknowledged and accepted that China and the United States do not want to go to war, and any form of escalation in armed conflict would be devastating. The United States should thus adopt this strategy as a less-risky option for pushing back against China. There are also several reasons as to why the United States should not pursue, or at least carefully consider, an offensive cyber campaign. First, an offensive strategy in any domain has escalation risks, and there are chances of miscommunication and misinterpretation that could spill over to negatively affect the bilateral relationship outside the cyber domain, such as in trade and diplomacy. Second, at the risk of OCO being discovered by the public, tools such as the use of disinformation could greatly distort the public's perception of cyber-attacks, which are already considered secretive operations conducted by nation-states. China, which has experience using propaganda and disinformation to sway people at home and abroad has a clear advantage in controlling these narratives in this domain.[87] Using any of the above strategies to attack China will almost certainly result in China responding, often to the detriment of the U.S.-China bilateral relationship.

It is also important to emphasize China's fundamental goals and beliefs in collecting information for power. OCO alone would probably not deter China from continuing its actions in cyberspace. China could receive the political message loudly and clearly and continue retaliating, if not escalating, in this domain. However, it is important to consider OCO as a tool for the United States in this broader strategic competition with China, and how it serves as a complement for other tools in the U.S. foreign policy toolkit in the diplomatic, economic, and conventional military spheres. To that end, this paper establishes a framework of what OCO can achieve for the United States, and outlines what persistent engagement just below the threshold of conflict could look like in cyberspace.

About the Author:

Melodie Ha is an alumna of the Security Studies Program at Georgetown's Edmund A. Walsh School of Foreign Service. She received her B.A. in Political Science and Chinese Language and Culture from Wellesley College and currently works as a federal consultant in Washington D.C. Previously, she worked as a research assistant at the Center for the Study of Chinese Military Affairs at National Defense University and served as a Boren Fellow to China.

Endnotes

1. Amy Chang, "Warring State, China's Cybersecurity Strategy," *Center for a New American Security*, December 2014, 13.
2. This acknowledges that the NATO Cooperative Cyber Defence Center of Excellence has a glossary to provide a picture on how different states and institutions interpret their approaches to cyber." NATO Cooperative Cyber Defence Centre of Excellence," https://ccdcoe.org/cyber-definitions.html; the Shanghai Cooperation Organization holds its own concept of "international information security," which differs from the Western consensus. "Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security," December, 2, 2008, http://www.ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf.
3. National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace," 2018. https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.
4. Oona A. Hathaway and Rebecca Crootof, "The Law of Cyber Attack," *Faculty Scholarship Series* Paper 3852, 826 (2012), http://digitalcommons.law.yale.edu/fss_papers/3852.
5. "Russia-U.S. Bilateral On Cybersecurity, Critical Terminology Foundations," *EastWest Institute*, Issue 1 (April 2011), https://www.files.ethz.ch/isn/130080/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20(2)-1.pdf.
6. Oona A. Hathaway and Rebecca Crootof, "The Law of Cyber Attack."
7. National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace," 2018, https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.
8. Will Goodman, "Cyber Deterrence: Tougher in Theory Than in Practice," *Strategic Studies Quarterly* (Fall 2010): 102-135 and David Elliott, "Deterring Strategic Cyberattack," *IEEE Security & Privacy,* September/October 2011.
9. Ben Buchanan, "Cyber Deterrence Isn't MAD; It's Mosaic," *Georgetown Journal of International Affairs,* International Engagement on Cyber IV (2014), https://www.jstor.org/stable/43773656?seq=1#page_scan_tab_contents.
10. Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Force Quarterly,* Issue 77 (2015), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_8-15_Denning.pdf.
11. Scott W. Harold, Martin C. Libicki, Astrid Stuth Cevallos, *Getting to Yes with China in Cyberspace* (Santa Monica, California: RAND Corporation, 2016.
12. Adam Segel, "How China is preparing for cyberwar," *The Christian Science Monitor*, March 20, 2017, https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar.
13. Robert Gilpin, *War and Change in World Politics* (Cambridge, England: Cambridge University Press, 1981).
14. Andrew Krepinevich, *Cyber Warfare—A Nuclear Option?* (Washington, D.C.: Center for Strategic and Budgetary Assessment: 2012).
15. Michael Sulmeyer, "How the U.S. Can Play Cyber-Offense," *Foreign Affairs,* March 22, 2018, https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense.
16. *Getting to Yes with China in Cyberspace*, 22.
17. Ibid.
18. Dean Cheng, *Cyber Dragon, Inside China's Information Warfare and Cyber Operations* (Santa Barbara, California: Praeger, 2017) 15-16.
19. Ellis Joffe and International Herald Tribune, "China: Learning from Iraq," *New York Times,* April 14, 2003, https://www.nytimes.com/2003/04/14/opinion/china-learning-from-iraq.html.
20. Jake Bebber, "Beijing's views on norms in cyberspace and cyber warfare strategy pt. 1," *Center for International Maritime Security*, June 26, 2017, http://cimsec.org/beijings-views-norms-cyberspace-cyber-warfare-strategy-pt-1/33099.

21. Michael Raska, "China's evolving cyber warfare strategies," *Asia Times*, March 8, 2017, http://www.atimes.com/article/chinas-evolving-cyber-warfare-strategies/.
22. Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance.
23. Elsa Kania, "PLA Strategic Support Force: The 'Information Umbrella' for China's Military," *The Diplomat*, April 1, 2017, https://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military/.
24. *Cyber Dragon, Inside China's Information Warfare and Cyber Operations*, 44.
25. Yuan Yi, "Analysis on the Characteristics, Types and Application Points of Network Space Deterrence 浅析网络空间威慑的特征 类型和运用要点," *Academy of Military Sciences of the Chinese People's Liberation Army*, November 2015.
26. Ibid.
27. Jiang Yamin, "Whoever strengthens the construction of network deterrent power is a powerful country in the information age, 加强网络威慑力量建设是信息时代的强国之策," *Academy of Military Sciences of the Chinese People's Liberation Army*, November 2015.
28. ,《国家网络空间安全战略》, 国家互联网信息办公室, 2016年12月27日, Central Network Security Leading Group, "National Cybersecurity Strategy," *National Internet Information Office*, December 27, 2016, http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.
Elizabeth C. Economy, "China's New Revolution," *Foreign Affairs*, May 2018, https://www.foreignaffairs.com/articles/china/2018-04-17/chinas-new-revolution?cid=int-fls&pgtype=hpg.
29. Adam Segal, "How China is preparing for cyberwar," *The Christian Science Monitor*, March 20, 2017, https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar.
30. *Cyber Dragon, Inside China's Information Warfare and Cyber Operations*, 53.
31. Elsa Kania, Samm Sacks, Paul Triolo, Graham Webster, "China's Strategic Thinking on Building Power in Cyberspace," *New America*, September 25, 2017, https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/.
32. Author interview, February 20, 2019.
33. *Cyber Dragon, Inside China's Information Warfare and Cyber Operations,* 41.
34. Jeffrey A. Eisenach, Claude Barfield, James K. Glassman, Mario Loyola, Ariel Rabkin, Jeremy Rabkin, Shane Tews, "An American Strategy for Cyberspace: Advancing Freedom, Security, and Prosperity," *American Enterprise Institute*, June 2016, http://www.aei.org/spotlight/american-strategy-for-cyberspace/?utm_source=paramount&utm_medium=email&utm_campaign=mediaeisenachgis&utm_content=report#2.
35. Adam Segal, "Chinese Cyber Diplomacy in a New Era of Uncertainty," *Hoover Working Group on National security, Technology, and Law Aegis Paper Series* No. 1703 (June 2017), 3.
36. Jason Healey, "Triggering the Forever War, in Cyberspace," *The Cipher Brief*, April 1, 2018, https://www.thecipherbrief.com/triggering-new-forever-war-cyberspace.
37. Michael Sulmeyer, "Getting to Ground Truth on the Elevation of U.S. Cyber Command," *War on the Rocks*, August 31, 2017 https://warontherocks.com/2017/08/getting-to-ground-truth-on-the-elevation-of-u-s-cyber-command/.
38. Joe Costello and John McReynolds, "China's Strategic Support Force: A Force for a New Era," *China Strategic Perspectives* 13 (October 2018), 492.
39. Bruce Schneier, "Why you should side with Apple, not the FBI, in the San Bernardino iPhone case," *The Washington Post,* February 18, 2016, https://www.washingtonpost.com/posteverything/wp/2016/02/18/why-you-should-side-with-apple-not-the-fbi-in-the-san-bernardino-iphone-case/?utm_term=.5c0a2379bc03.
40. Sarah Kreps and Jacquelyn Schneider, "Should the U.S. try to deter cyberattacks by promising nuclear retaliation," *The Washington Post,* January 29, 2018, https://www.washingtonpost.com/news/monkeycage/wp/2018/01/29/should-the-u-s-try-to-deter-cyberattacks-by-promising-nuclear-retaliation/?noredirect=on&utm_term=.9e2137e5fb23.
41. "Chinese Cyber Diplomacy in a New Era of Uncertainty," 4.
42. "Chinese Cyber Diplomacy in a New Era of Uncertainty," 10.

43. Robert D. Williams, "Cyberspace Norms and U.S. China Relations: Addressing the Challenge of 'China, Inc.+,'" *Lawfare*, February 26, 2018, https://www.lawfareblog.com/cyberspace-norms-and-us-china-relations-addressing-challenge-china-inc.
44. Lei Zhao,, "PLA to be a world class force by 2050," *China Daily,* October 27, 2017, https://www.chinadaily.com.cn/china/2017-10/27/content_33756453.htm; Mirjam Meissner Wübbeke, Max J. Zenglein, Jaqueline Ives, Björn Conrad, "Made in China 2025, The making of a high-tech superpower and consequences for industrial countries," *Merics*, December 2016, https://://www.merics.org/sites/default/files/2017-09/MPOC_No.2_MadeinChina2025.pdf.
45. "Warring State, China's Cybersecurity Strategy," 27.
46. "Is China winning race with the U.S. to develop quantum computers?" *South China Morning Post*, April 9, 2018, http://www.scmp.com/news/china/economy/article/2140860/china-winning-race-us-develop-quantum-computers; Elsa Kania, "China's AI Agenda Advances," *The Diplomat*, February 14, 2018, https://thediplomat.com/2018/02/chinas-ai-agenda-advances/.
47. Phil Saunders and Joshua K. Wiseman, "Buy, Build, Steal: China's Quest for Advanced Military Aviation Technologies," *China Strategic Perspectives* 4 (National Defense University: December 2011).
48. "How China is preparing for cyberwar."
49. Adam Segal, "Why China hacks the world," *The Christian Science Monitor*, January 31, 2016, https://www.csmonitor.com/World/Asia-Pacific/2016/0131/Why-China-hacks-the-world.
50. "How China is preparing for cyberwar."
51. Brendan I. Koerner, "Inside the cyberattack that shocked the U.S. government," *Wired*, October 23, 16, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.
52. "Inside the cyberattack that shocked the U.S. government."
53. "China's Strategic Support Force: A Force for a New Era," 26-27.
54. *National Defense Strategy of the United States of America* (Washington, D.C.: United States Department of Defense, 2018) and Michael Sulmeyer, "How the U.S. Can Play Cyber-Offense," March 22, 2018, *Foreign Affairs*, https://www.foreignaffairs.com/articles/world/2018-03-22/how-us-can-play-cyber-offense.
55. Clint Hinote, "How to Stop the Next Hack," January 4, 2015, *Foreign Affairs*, https://www.foreignaffairs.com/articles/2015-01-04/how-stop-next-hack
56. Ibid.
57. Robert Bebber, "There is No Such Thing as Cyber Deterrence. Please Stop," *Cipher Brief*, April 1, 2018, https://www.thecipherbrief.com/column_article/no-thing-cyber-deterrence-please-stop.
58. Ellen Nakashima, "Pentagon launches first cyber operation to deter Russian interference in midterm elections," *Washington Post,* October 23, 2018.
59. Ellen Nakashima, "U.S. cyber force credited with helping stop Russia from undermining midterms, *Washington Post,* February 14, 2019.
60. "An Interview with Paul M. Nakasone," *Joint Forces Quarterly,* Vol 92. No 1. (2019)
61. Ibid.
62. "Interview with Michael Sulmeyer."
63. Author interview, February 20, 2019.
64. Bill Gertz, "U.S. Hits Back Against Chinese Cyberattacks," *Washington Examiner,* March 6, 2019, https://www.washingtontimes.com/news/2019/mar/6/us-counters-china-cyberattacks/.
65. Luke Harding, "What are the Panama Papers? A guide to history's biggest data leak," *The Guardian*, April 5, 2016, https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers.
66. Gerry Shih, "In China, investigations and purges become the new normal," *The Washington Post,* Ocotber 22, 2018, https://www.washingtonpost.com/world/asia_pacific/in-china-investigations-and-purges-become-the-new-normal/2018/10/21/077fa736-d39c-11e8-a275-81c671a50422_story.html?noredirect=on&utm_term=.cada59e53189.

67. Interview with Christopher K. Johnson, *Center for Strategic and International Studies*, https://www.youtube.com/watch?v=0USIKN0mqo0&feature=youtu.be&start=317&autoplay=1&rel=0
68. Andrew J. Nathan, "The Tiananmen Papers," *Foreign Affairs*, January/February 2001, https://www.foreignaffairs.com/articles/asia/2001-01-01/tiananmen-papers.
69. "Trump accuses China of election 'meddling' against him," *BBC News*, September 26, 2018, https://www.bbc.com/news/world-us-canada-45656466.
70. Wei Chun Chew, "How It Works: Great Firewall of China," *Medium,* May 1, 2018, https://medium.com/@chewweichun/how-it-works-great-firewall-of-china-c0ef16454475.
71. Blair, et al. "The Report on the Commission of the Theft of American Intellectual Property" May 2013.
72. Gabriel Popkin, "China's quantum satellite achieves 'spooky action' at record distance," *Science Mag*, June 15, 2017, https://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance
73. Aaron Stanley, "Is the U.S. Getting Its Act Together on Quantum Computing?" *Forbes*, June 26, 2018, https://www.forbes.com/sites/astanley/2018/06/26/is-the-u-s-getting-its-act-together-on-quantum-computing/#6387bd6a704f.
74. Joseph Trevithick, "China Reveals Short-Range Anti-Ship Ballistic Missile Designed to Dodge Enemy Defenses," *The Drive*, November 5, 2018, https://www.thedrive.com/the-war-zone/24699/china-reveals-short-range-anti-ship-ballistic-missile-designed-to-dodge-enemy-defenses.
75. Operations Security (OPSEC) is the process by which nations protect critical information, whether it is classified or unclassified, that can be used against them. It focuses on preventing our adversaries' access to information and actions that may compromise an operation. As defined by https://www.cdse.edu/catalog/operations-security.html.
76. Author personal interview, April 10, 2019.
77. *Law of War Manual* (Washington, D.C.: Department of Defense, June 2015), 994.
78. H.R.3723 - Economic Espionage Act of 1996, 104th Congress, 1995. https://www.congress.gov/bill/104th-congress/house-bill/3723
79. Laura Sullivan, "As China Hacked, U.S. Businesses Turned A Blind Eye," *NPR*, April 12, 2019. https://www.npr.org/2019/04/12/711779130/as-china-hacked-u-s-businesses-turned-a-blind-eye
80. Author interview, April 17, 2019.
81. Kim Zetter, "An Unprecedented Look at Stuxnet, The World's First Digital Weapon," *Wired*, November 3, 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/; Elias Groll, "'Obama's General' Pleads Guilty to Leaking Stuxnet Operation," *Foreign Policy*, October 17, 2016, https://foreignpolicy.com/2016/10/17/obamas-general-pleads-guilty-to-leaking-stuxnet-operation/.
82. Donghui Park, Julia Summers, and Michael Walstrom, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks," *University of Washington*, October 11, 2017, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.
83. *Law of War Manual*, 994-995.
84. Dustin Volz and Jim Finkle, "U.S. indicts Iranians for hacking dozens of banks, New York dam," *Reuters*, March 24, 2016, https://www.reuters.com/article/us-usa-iran-cyber/u-s-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF.
85. *Law of War Manual*, 994-996.
86. Ibid.
87. Emily Feng, "How China Uses Twitter And Facebook To Share Disinformation About Hong Kong," *NPR*, August 20, 2019, https://www.npr.org/2019/08/20/752668835/how-china-uses-twitter-and-facebook-to-share-disinformation-about-hong-kong.

Al Qaeda and ISIS' Online Propaganda and Jihadist Lone-actor Terrorism in the United States Post-9/11

Daniel Zhang

This paper examines the trend and developments of jihadist lone-actor attacks in the U.S. after the 9/11 attack and its relationship with the online propaganda by al-Qaeda and ISIS. With a quantitative analysis of 37 jihadist lone-actor (attempted or completed) attacks in the United States in the post 9/11 era, the research found that 1) jihadist lone-actor attacks peaked in 2010 and 2016 in the U.S. but are generally declining; 2) lone-actor attacks in the past 18 years are mostly inspired by al-Qaeda considering that the rise of ISIS starts only after 2013, but al-Qaeda-inspired attacks dramatically decreased after 2014 when ISIS-inspired attacks arose; 3) among those attacks inspired by al-Qaeda, an overwhelming majority cited influences from one of al-Qaeda's branches, al-Qaeda in the Arabian Peninsula (AQAP), or its senior member Anwar al-Awlaki.

Introduction

On June 27, 2019, Europol released the 2019 European Union Terrorism Situation and Trend Report (TE-SAT). The Report highlighted that all seven completed jihadist terrorist attacks in Europe in 2018 "were perpetrated by lone actors,"[1] which resulted in 13 casualties and 46 injured. For several years, both al-Qaeda and the so-called Islamic State of Iraq and Syria (ISIS) have used various forms of online propaganda to call on supporters in the West to perpetrate terrorist attacks on their own initiative. While groups perpetrate the majority of terrorist attacks,[2] a series of lone-actor terrorism in Western countries suggest that such phenomenon continues to grow and poses a great danger to international security.[3] As one of the biggest targets for jihadist terrorism, the United States has suffered multiple lone-actor terrorist incidents. On June 12, 2016, Omar Mateen, an ISIS-inspired lone actor opened fire on customers at Pulse, a gay nightclub, in Orlando, Florida, resulting in 50 deaths and 53 injuries—the second-deadliest mass shooting by a single shooter in the U.S. history.[4]

This paper provides a detailed analysis of 37 jihadist lone-actor attacks (both completed attacks and attempted but unsuccessful terrorist plots) in the United States in the post-9/11 era. Specifically, the research aims to analyze the trends and developments of jihadist lone-actor attacks as well as their relationship with the online propaganda by al-Qaeda and ISIS, based on data from the Global Terrorism Database (GTD) by the National Consortium for the Study of Terrorism and Responses to Terrorism (START).

The research found that 1) jihadist lone-actor attacks peaked in 2010 and 2016 in the United States but are generally declining; 2) lone-actor attacks in the past 18 years are mostly inspired by al-Qaeda considering that the rise of ISIS starts only after 2013, but al-Qaeda-inspired attacks dramatically decreased after 2014 when ISIS-inspired attacks arose; 3) among those attacks inspired by al-Qaeda, an overwhelming majority cited influences from one of al-Qaeda's branches, al-Qaeda in the Arabian Peninsula (AQAP), or its senior member, Anwar al-Awlaki. The paper begins with a literature review and then proceeds to introduce the dataset, followed by an examination of trends and developments of lone-actor terrorism in the United States after 9/11.

Literature Review

Lone-Actor Terrorism

It is first important to define lone-actor terrorism, as it determines the scope of the research. There is no consistent definition of lone-actor terrorism across past literature. Publications on lone-actor terrorism offer multiple definitions of the crime that emphasize various key points, which Spaaij and Hamm point out "has often made the definitional conundrum more complex, more arbitrary, and more contradictory."[5] Those definitions vary mostly in two areas: the motivations of lone actors and the number of terrorists included in the research.

On motivations, Becker defines lone-actor terrorism as "ideologically driven violence, or attempted violence, perpetrated by an individual who plans and executes an attack in the absence of collaboration with other individuals or groups."[6] Becker's definition focuses on an ideologically-driven motivation, and similar emphasis can be found in Bates' study that includes " . . . violent acts to promote a cause or support a belief system."[7] Such definitions are different from Simon and Jenkin's definition that extends the motivation to " . . . purely personal or financial gain."[8] Spaaij, nevertheless, provides a rather narrow definition—one that emphasizes terrorists themselves and avoids specifying political, religious, or social aims.[9]

Past literature also disagrees on the number of terrorists included in the definition. Spaaij, for example, points out that only attacks carried out by persons who operate individually qualify and "terrorist attacks carried out by couples or by very small terrorist cells, do not, strictly speaking, qualify as lone wolf terrorism."[10] Multiple terrorist experts adopt such definition in their lone-actor terrorism research, including Weimann[11] and Schuurman et al.[12] Simon and Jenkins, on the other hand, counts individuals "acting alone or with minimal support from one or two other people" as lone-actor terrorists.[13] There is, however, some consistency as most definitions agree that lone-actor terrorism is distinguished from terrorist incidents conducted by (part of) terrorist organizations or state bodies.[14] The most expansive definition of lone-actor terrorism that includes multiple motivations and counts multiple perpetrators as what he called "lone wolf pack" is Pantucci's definition. Pantucci, who focuses on Islamist lone-actor attacks, said that terrorist goals could be "either driven by personal reasons or their belief that they are part of an ideological group" and "the term Lone Wolf is expanded out to Lone Wolf pack when referring to small isolated groups pursuing the goal of Islamist terrorism together under the same ideology . . ."[15] As a result of various definitions existed in lone-actor terrorism literature, it is difficult to compare studies across the board, as the subject of research may vary depending on those aforementioned factors.

Lone-actor Terrorism in the United States

The landscape of literature on lone-actor terrorism has changed within the past decade with an increasing amount of data-driven studies that provide important insights into the lone-actor terrorists and related attacks.[16] Three major empirical studies have focused on lone-actor terrorism in the United States.

Spaaij published research in 2010 that assesses a total of 74 cases of lone-actor terrorist attacks in fifteen countries that occurred between 1950 and 2007. The study identifies a "markedly [increasing]" trend of lone-wolf terrorism in the United States that was not observed in other countries, and six out of 30 cases in the United States. are driven by the Islamist ideology.[17] Deloughery et al. published a Department of Homeland Security report in 2013 that compares lone-actor terrorism to two other forms of violence, group-based terrorism and violent hate crimes that took place in the United States between 1992 and 2010. They found that while lone-actor terrorism shared some similarities on year-to-year

changes and target selection with group-based terrorism, it tends to occur more in less populous states than the other two types of crimes.[18] Finally, Teich published a study in 2013 that seeks to identify trends and developments of lone-wolf terrorism in Western countries (1990-2013). The research discovered that the United States was the most targeted country among the list, and there are an increased number of countries targeted by lone-actor terrorists as well as an increased success rate of U.S. law enforcement in apprehending lone actors before they can conduct attacks.[19]

Lone-actor Online Propaganda

As past research suggests, the Internet plays an important role in promoting jihadist agenda and especially lone-actor terrorism. Pantucci argues that "the Internet is clearly the running theme between most of the [lone-actor] plots . . . and it appears to be a very effective tool" that "provides [the terrorists] with direct access to a community of like-minded individuals around the world with whom they can connect and in some cases can provide them with further instigation and direction to carry out activities."[20] Due to the loss of senior leadership and territories as well as sustained military pressure that discouraged sympathizers from traveling to conflict zones, both al-Qaeda and ISIS have thrown their efforts into promoting lone-actor terrorism with online platforms.[21] Those platforms include blogs, online lectures, online Internet forums, magazines, social media, mobile messenger applications, etc.

Al-Qaeda

Many attributed al-Qaeda's strategic shift towards a decentralized approach and the adaptation of the global jihadist movement, especially the rise of lone-actor terrorism, to Abu Musab al-Suri, al-Qaeda's leading theoretician.[22] His 2004 book, *Call to Global Islamic Resistance*, promotes a phenomenon later labeled by Sageman as "leaderless jihad."[23] Specifically, al-Suri urges recruits to stay under the radar with "small, completely separate non-central cells" and perform the "leaderless jihad" from wherever they are, including the Western soil.[24]

Al-Qaeda's early forms of lone-actor propaganda online included articles on extremist forums by prominent members or Salafi writers, such as Abu Jihad al-Masri, who authored a text in 2006 titled "How to Fight Alone."[25] It also circulated English-language videos, including one in 2011 that clearly emphasizes lone-actor operations with the title "Do Not Rely on Others, Take the Task Upon Yourself," and another one in 2012 that promotes the same message.[26] Those videos call on Muslims living in the United States to purchase weapons—such as fully automatic weapons—to carry out deadly one-man terrorist attacks.

Al-Qaeda has also published various online magazines, including *Resurgence* by al-Qaeda in the Indian Subcontinent (AQIS) and *Al-Risalah* by the former al-Nusra Front. The one that has been vocal in encouraging lone-actor terrorism is *Inspire* (2010-2016) by al-Qaeda in the Arabian Peninsula (AQAP). Each edition of the magazine contains a section called "Open Source Jihad" that introduces tools and instructions for jihadists to conduct attacks without traveling to the recruitment camps.[27] *Inspire*'s very first issue included an article, titled "How to Make a Bomb in the Kitchen of your Mum" that was referenced multiple times by terrorists in their attempts to carry out attacks in the West, including the 2009 Fort Hood shooting (and Boston Bombing).[28] Sivek argued that the power of the magazine method that "[unifies] audiences through the construction of communities around topics and through the medium's distinctive mode of address"[29] makes *Inspire* a successful example of online propaganda.

Moreover, Anwar al-Awlaki, a popular US-born AQAP senior member who Brachman and Levine describe as the "al-Qaeda Idol"[30] set up websites to

mobilize sympathizers, incite terrorist actions, and urge followers to become "internet mujahideen."[31] Nevertheless, al-Qaeda leaders Osama bin Laden disapproved the notion of lone-actor terrorism that could potentially kill Muslims and damage the public image of al-Qaeda.[32] His successor Ayman al-Zawahiri also published an article in 2013 that urged al-Qaeda members and followers to "understand the boundaries of 'useful' violence."[33]

ISIS

Compared to al-Qaeda, ISIS does not shy away from the use of indiscriminate violence.[34] Its notorious use of social media, including Facebook, Twitter, and YouTube, to promote violence quickly became a successful method for recruiting fighters.[35] Although there is no empirical analysis on specific ISIS social media content that advertises lone-actor attacks, literature suggests that such use has contributed to the increase of lone-actor terrorists.[36]

Both ISIS's online magazines, *Dabiq* (2014-2016) and *Rumiyah* (2016-2017), while aiming to incite every Muslim to engage in violence against Islam's enemies, contain language that promotes lone-actor terrorism.[37] In the forward of *Dabiq*'s 6th issue in 2014, the magazine argues that lone-actor terrorism in the West avenges Western violence against Muslims, and it is "strategically important as a way of 'flanking the crusaders on their own streets and bringing the war back to their own soil."[38] An empirical study conducted by Wignell et al. that examines the changes in ISIS magazines suggests that after the ISIS-controlled town of Dabiq came under attack from the Turkish-led coalition forces, the group changed its magazine from Dabiq to Rumiyah and shifted focus to advertise lone-actor terrorism, especially in the United States.[39] Rumiyah, or Rome in English, is a reference to a hadith by Prophet Muhammad that said Muslims would conquer Constantinople and then Rome.[40]

Past research has also touched on the role of messenger applications in lone-actor attacks. Shehabat et al. used a digital ethnography approach to observe the information flow on four of the most celebrated IS Telegram channels—created by IS members and affiliates to enhance communications among them and strengthen the propaganda machine—between 2015 and 2016.[41] They found that such a platform plays an important role in "personal communication between potential recruits and dissemination of propaganda," and it is often used to encourage lone actors to carry out attacks in the west.[42]

Research Method

The research adopts Pantucci's definition of lone-actor terrorist mentioned above as those "individuals pursuing Islamist terrorist goals alone, either driven by personal reasons or their belief that they are part of an ideological group."[43] While past research has used various terms to describe lone-actor attacks, such as "leaderless resistance", "phantom cell networks," etc.,[44] this paper avoids using one of the most frequently cited terms, "lone-wolf" terrorism and adopts "lone-actor" instead. As Schuurman et al. and Joosse point out, "[the term] is sensationalist rather than descriptive, hampering a dispassionate assessment of the phenomenon."[45] Bakker and de Graff also argue that using the term "lone wolf" suggest the standalone and isolated nature of the perpetrator, which "[neglects] the ideological connections individuals might have with other networks or organizations, either through personal contacts or inspirational content on the internet."[46] As many cases in this paper suggest, lone-actor terrorists are often inspired by online propaganda or in touch with figures in a terrorist organization. Thus, the term "lone actor" is more appropriate to describe those terrorists.

The research is based on a dataset compiled by searching the GTD and LexisNexis databases for terrorist incidents from September 12, 2001, to December

31, 2018. Only jihadist-inspired terrorist attacks by lone-actors that took place in the United States are included in the database. The dataset includes the date, place, summary, the type of attacks, the weapons used in the attack, along with information of whether such an attack is inspired by al-Qaeda, AQAP/Anwar al-Awlaki, or ISIS. The terrorist incidents in this dataset include completed and attempted terrorist incidents. Completed terrorist acts refer to cases in which the terrorists are identified and apprehended after such an act has been carried out. Attempted cases refer to those in which the terrorists are caught before conducting a terrorist act. Moreover, if the same perpetrator conducts more than one attack, all attacks are registered separately in the database.

It is important to note that the START database lists the number of perpetrators of each accident and labels "unknown" for the affiliated organization to signal that such an incident might be a lone-actor attack. However, the database is not particularly clear on whether each terrorist incident listed is identified specifically as a lone-actor act or not or whether the terrorists are influenced by Al Qaeda or Islamic State propaganda. Moreover, the START database lacks thwarted terrorist attacks. As a result, this research uses LexisNexis database to search news sources with terms such as "lone-wolf terrorist," "lone-actor terrorist," "leaderless jihad," etc. and also cross-check the news with U.S. Department of Justice (DOJ) records to 1) ensure that the terrorist incident listed in the START database is in fact a lone-actor attack; 2) identify unlisted attempted jihadist lone-actor attacks; and 3) look for signs of al-Qaeda, AQAP/al-Awlaki, and ISIS influence in the investigation of the terrorists.

Research Result & Analysis

Between September 12, 2001, and December 31, 2018, there have been 37 jihadist lone-actor terrorist attacks on the U.S. soil by 30 jihadist lone-actor terrorists. Among them, 16 are attempted attacks, and 21 are completed attacks. Washington Metropolitan Area and New York Metropolitan Area were among the most targeted areas in the United States that account for a total of 38% of all the attacks. Moreover, the 21 completed attacks caused 87 deaths and 304 non-fatal injuries. Of the 37 attacks, 16% of them targeted military personnel, and 84% targeted civilians, which also include six planned or completed attacks on various branches of the U.S. government.

Means of attacks also vary. Explosives (54%) and firearms (32%) are two of the most frequently used weapons, followed by melee (11%) and vehicle (3%). This result is different from Becker's study in 2014 that identifies firearms as "disproportionately [used]"[47] means of attack for lone actors. It is important to note however, that Becker includes lone-actor terrorists motivated by various ideologies. Jihadist terrorists, in the case of this research, use explosives more than firearms to conduct violence.

As shown in Figure 1, the number of lone-actor terrorist attacks peaked in 2011 and 2016. This is because one lone actor, Yonathan Melaku, conducted five separate attacks in Northern Virginia in 2010, and Ahmad Khan Rahami conducted four separate attacks in New York and New Jersey in 2016. The United States saw the largest number of lone-actor terrorist attacks between 2009 and 2012, and overall, the number of lone-actor terrorists decreased after 2015.

According to Figure 2, among the 30 jihadist lone-actor terrorists, more than half were inspired by al-Qaeda and 27% of them cited ISIS as their sources of inspiration. There are two cases (7%) in which the terrorists claimed they were inspired by both al-Qaeda and ISIS propaganda. Those two were Zale Thompson who was responsible for attacking a police patrol with a hatchet in New York city in 2014, and Abdul Razak Ali Artan, who drove a vehicle into a group of students and stabbed bystanders at Ohio State University in 2016.

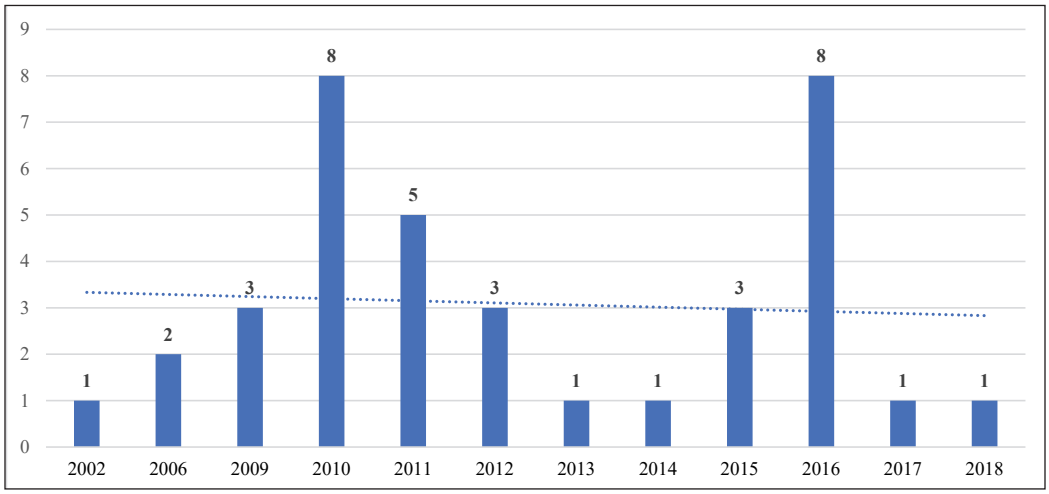


Figure 1: Number of Jihadist Lone-actor Terrorist Attacks in the United States post-9/11, by Year

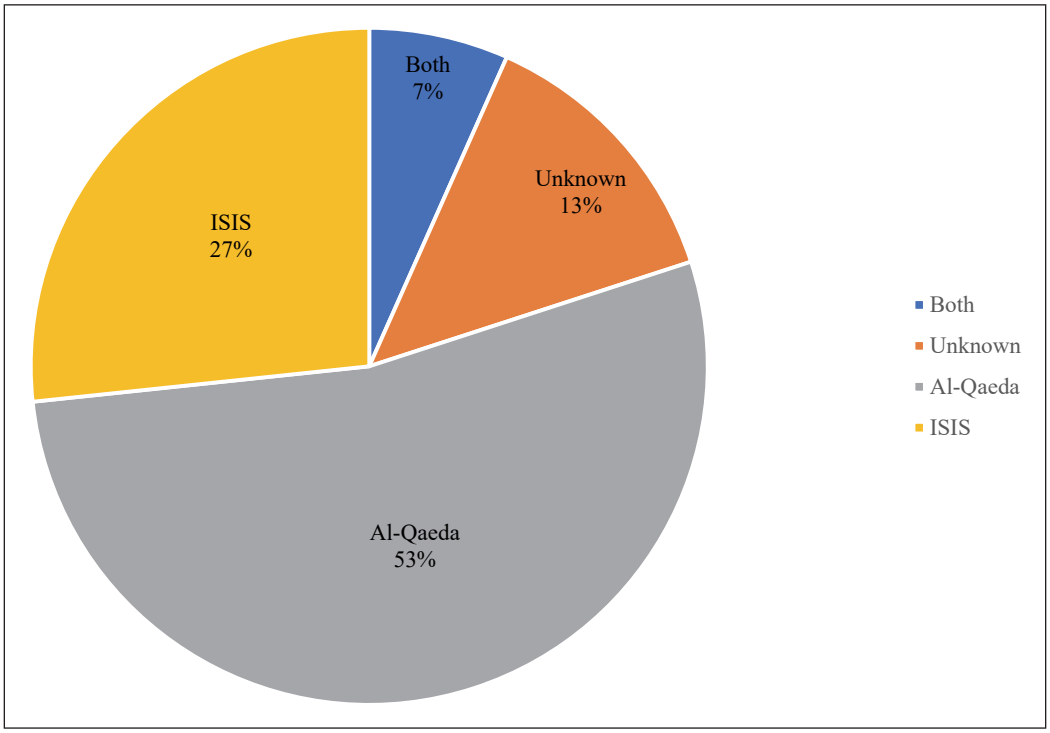


Figure 2: Terrorist Organization that Inspired Jihadist Lone-actor Terrorists in the United States post 9/11

In most cases, terrorists told investigators that they were influenced by online materials published by extremist organizations and participated in online discussions on social media. For example, Jose Pimentel, who was charged of attempting to build and detonate bombs in New York in 2011, said that he took inspirations from *Inspire*, the AQAP online magazine.[48] Moreover, two gunmen who tried to ambush a public event in Garland, Texas in 2015—later credited as the first ISIS-claimed attack in the United States—pledged allegiance to ISIS hours before the attack.[49]

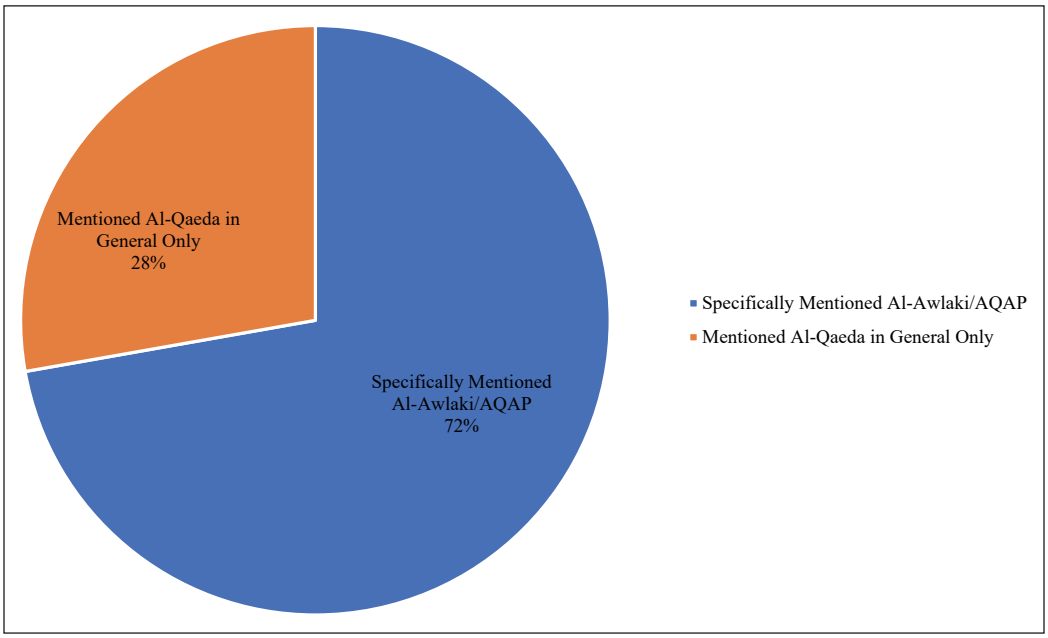


Figure 3: Al-Qaeda Branches that Inspired Jihadist Lone-actor Terrorists in the United States post-9/11

According to Figure 3, among the 18 jihadist lone actors inspired by al-Qaeda, investigations showed that 72% of the terrorists specifically mentioned that they were inspired by AQAP or its senior member, Anwar al-Awlaki. Quasi Nafis, who attempted to bomb the Federal Reserve Bank in New York in 2013 "[carried] instructions on how to make a bomb out of household items, as well as audio recordings of Anwar al-Awlaki," according to the New York Times.[50] In another case, the Fort Hood attacker, Nidal Malik Hasan, had communicated directly with Anwar al-Awlaki."[51] The remaining 28% of terrorists did not reveal any specific references to the propaganda of AQAP or al-Awlaki.

Figure 4 shows the distribution of those terrorist organizations that inspired jihadist lone-actor terrorists over the years. The number of terrorists inspired by al-Qaeda increased from four before 2010 to 11 between 2010 and 2014. Such a dramatic increase can be attributed to two factors. First, AQAP was established in January 2009, and one of its leaders, Anwar al-Awlaki, used English-language propaganda to promote the use of lone-actor terrorism. The fact that he was born and has lived in the United States, and his videos are in English, made him a popular terrorist figure.[52] Secondly, AQAP started to publish its online English-language magazine *Inspire* in 2010 that has not only advertised lone-actor terrorism but also carried instructions on how to make a bomb.

Moreover, the overall al-Qaeda-influenced lone-actor terrorists decreased after 2014. The only major al-Qaeda attack in the West after 2014 is the shooting of 12 people at Charlie Hebdo newspaper office in Paris by the Kouachi brothers.[53] The rise of ISIS and al-Qaeda's shifted focus could explain such a decline. The rise of ISIS and its focus on attacking the West gained the sympathy of lone-actor terrorists who would have carried out attacks in the name of al-Qaeda.[54] ISIS' intention to position itself as the new leader of the global jihadist movement could have weakened al-Qaeda's power. Also, ISIS' crusade against the West could disincentivize al-Qaeda to continue targeting the West. Al-Qaeda intended to position itself as the less extreme

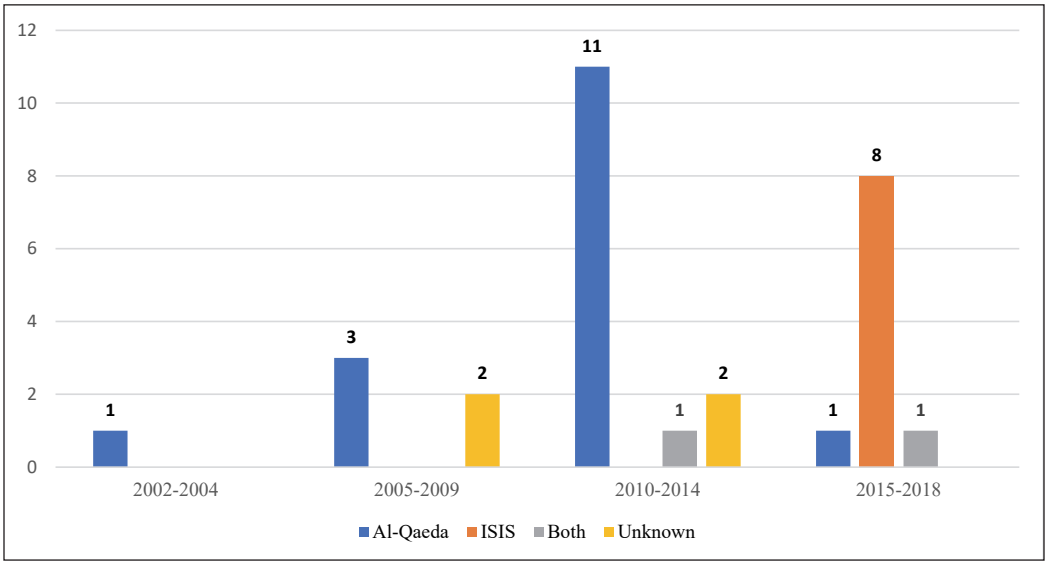


Figure 4: Terrorist Organization that Inspired Jihadist Lone-actor Terrorists in the United States post 9/11, by Year

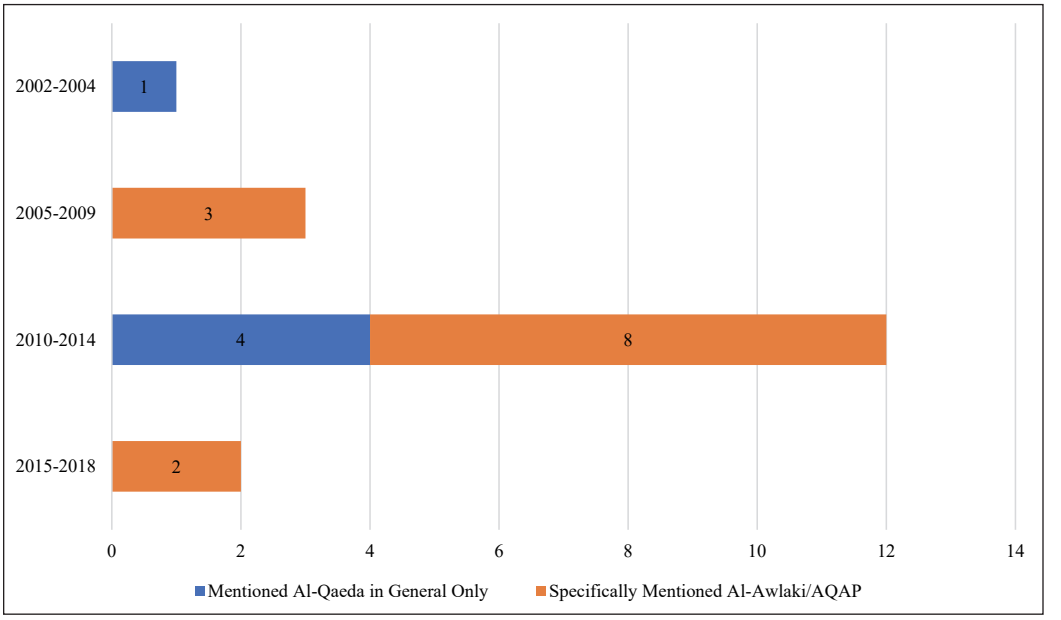


Figure 5: Al-Qaeda Branches that Inspired Jihadist Lone-actor Terrorists in the United States post-9/11, by Year

and the more tolerable group compared to ISIS to win the support of moderate Muslims living in its area.[55]

After 2014, ISIS surpassed al-Qaeda as the organization that most frequently inspired lone-actor terrorists. While the official establishment of ISIS' predecessor, the Islamic State of Iraq (ISI), occurred in 2006, ISIS proclaimed itself a worldwide caliphate in 2014, which explains the abrupt number of lone-actor terrorists that emerged from 2015 onwards. Moreover, the consistent use of advertisement in ISIS' two online magazines, as well as the promotion of violence on social media and mobile messenger applications,

also speaks to the increase in ISIS-inspired lone-actor terrorist attacks.

More importantly, the difficulty to travel to the Caliphate may prompt both an increase in lone-actor propaganda and attacks. Turkey, under the Western pressure, started to seal its border and arrest suspected militants along its border in early 2015.[56] When it became too challenging for wannabe jihadists to travel to the Caliphate—which would be the ideal situation, they start to carry out attacks in their homelands.

According to Figure 5, 13 out of 18 lone-actor terrorists inspired by al-Qaeda have referenced AQAP or al-Awlaki as sources of inspirations. It is important to note that all three attacks between 2005 and 2009 took place in 2009, meaning before 2009 or the establishment of AQAP, there was only one terrorist attack that was inspired by al-Qaeda. The number of AQAP/al-Awlaki-influenced terrorists increased to eight between 2010 and 2014, and such a timeframe aligns with the start of AQAP's publication, *Inspire*.

Conclusion

There are three key findings in this research. First, the number of lone-actor attacks reached the highest points in the United States after 9/11 in 2010 and 2016, and in general, the number of such attacks is decreasing. Secondly, while most lone-actor attacks are perpetrated by terrorists inspired by al-Qaeda, those attacks dramatically decreased after 2014 due to the rise of ISIS. Finally, AQAP or its senior member Anwar al-Awlaki has had a much stronger influence on lone-actor terrorists than other al-Qaeda branches.

The paper also observes a few weaknesses. First, the dataset may not be comprehensive considering the potential selection bias of START database towards the most newsworthy type of terrorist attacks.[57] While outside research is conducted through the LexisNexis database and DOJ records, the insignificant lone-actor attacks or the un-disclosed thwarted terrorist attempts may not be included. Moreover, the paper attempts to link the trend of terrorist attacks inspired by al-Qaeda in general, AQAP, and ISIS with the times of the establishment of those organizations and the publication of their respective online magazines. However, although those times of establishment may match with the trend, they do not speak to the actual reasons behind the trend. Future research should extend the dataset to include lone-actor terrorist attacks in other western countries to observe whether such times still align with the trends, thereby increasing the validity of this research. Finally, the research assumes that the influence of al-Qaeda in general, AQAP, and ISIS is derived from those organization's online propaganda. Such an assumption is based on the notion that terrorist organizations' recruitment in the west often relies solely on online propaganda. Even though investigations of these lone actors revealed that they were influenced by certain jihadist organizations to an extent, these lone actors could also be influenced by other materials, such as the portrayal and description of jihadism in Western media. Critics has argued the Western portrayal of ISIS in mass media—especially the circulation of brutal killings— incites sympathizers and research shows that such media coverage of violence could also trigger further attacks.[58]

While the research suggests a decreasing trend in lone-actor terrorist attacks in the United States, it does not indicate that the threat of lone-actor attacks should be taken lightly. Evidenced by the 2013 Boston bombings and the 2016 Orlando attack, weakly connected and even relatively unskilled individuals are able to carry out deadly attacks with instructions from jihadist online propaganda. Only less than half of the jihadist lone-actor terrorist attacks in this research were thwarted by the U.S. security services, and the U.S. government should therefore continue to proactively monitor the online propaganda distributed by terrorist organizations with

combined law enforcement, intelligence, and community efforts and avoid alienating Muslim communities to prevent isolated lone-actor terrorist attacks.

About the Author:

Daniel Zhang is a second-year Master candidate pursuing a degree in Security Studies concentrating on Technology and Security, and a certificate in International Business Diplomacy at the Georgetown University Walsh School of Foreign Service. Prior to Georgetown, he worked in education policy conducting research on Montessori education and supporting development efforts at a veteran affairs nonprofit. Daniel graduated from Furman University with a B.A. in politics & international affairs and film studies. His interests include cybersecurity, artificial intelligence, and private sector risk assessment. He can be reached at (864) 915-5143 or at qz105@georgetown.edu.

Endnotes

1. Europol, "Terrorism Situation and Trend Report 2019 (TE-SAT)," Europol, accessed July 8, 2019, https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat.
2. Ramon Spaaij, *Understanding Lone Wolf Terrorism: Global Patterns, Motivations and Prevention* (Springer Science & Business Media, 2011), 4.
3. Bart Schuurman et al., "Lone Actor Terrorist Attack Planning and Preparation: A Data-Driven Analysis," *Journal of Forensic Sciences* 63, no. 4 (July 1, 2018): 1191, https://doi.org/10.1111/1556-4029.13676.
4. Lizette Alvarez and Richard Pérez-Peña, "Orlando Gunman Attacks Gay Nightclub, Leaving 50 Dead," *The New York Times*, June 12, 2016, sec. U.S., https://www.nytimes.com/2016/06/13/us/orlando-nightclub-shooting.html.
5. Ramón Spaaij and Mark S. Hamm, "Key Issues and Research Agendas in Lone Wolf Terrorism," *Studies in Conflict & Terrorism* 38, no. 3 (March 4, 2015): 168, https://doi.org/10.1080/1057610X.2014.986979.
6. Michael Becker, "Explaining Lone Wolf Target Selection in the United States," *Studies in Conflict & Terrorism* 37, no. 11 (November 2, 2014): 960, https://doi.org/10.1080/1057610X.2014.952261.
7. Rodger Bates, "Tracking Lone Wolf Terrorists," *The Journal of Public and Professional Sociology* 8, no. 1 (August 25, 2016): 2, https://digitalcommons.kennesaw.edu/jpps/vol8/iss1/6.
8. Jeffrey D. Simon and Brian Michael Jenkins, *Lone Wolf Terrorism: Understanding the Growing Threat*, Reprint edition (Amherst, New York: Prometheus, 2016), 67.
9. Ramón Spaaij, "The Enigma of Lone Wolf Terrorism: An Assessment," *Studies in Conflict & Terrorism* 33, no. 9 (August 16, 2010): 856, https://doi.org/10.1080/1057610X.2010.501426.
10. Spaaij, 856.
11. Gabriel Weimann, "Lone Wolves in Cyberspace," *Contemporary Voices: St Andrews Journal of International Relations* 3, no. 2 (September 22, 2012), https://doi.org/10.15664/jtr.405.
12. Schuurman et al., "Lone Actor Terrorist Attack Planning and Preparation."
13. Simon and Jenkins, *Lone Wolf Terrorism*, 266.
14. Spaaij, "The Enigma of Lone Wolf Terrorism," 856.
15. Raffaello Pantucci, *A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists* (International Centre for the Study of Radicalisation and Political Violence, 2011), 8.
16. Schuurman et al., "Lone Actor Terrorist Attack Planning and Preparation," 1191.
17. Spaaij, "The Enigma of Lone Wolf Terrorism."
18. Kathleen Deloughery, Ryan D. King, and Victor Asal, "Understanding Lone-Actor Terrorism: A Comparative Analysis with Violent Hate Crimes and Group-Based Terrorism | START.Umd.Edu," Final Report to the Resilient Systems Division, Science and Technology Directorate (College Park, MD: U.S. Department of Homeland Security, 2013), https://www.start.umd.edu/publication/understanding-lone-actor-terrorism-comparative-analysis-violent-hate-crimes-and-group.
19. Sarah Teich, "Trends and Developments in Lone Wolf Terrorism in the Western World An Analysis of Terrorist Attacks and Attempted Attacks by Islamic Extremists," 2013, /paper/Trends-and-Developments-in-Lone-Wolf-Terrorism-in-Teich/fe951d78e86ac364ad9b8bdcca56b23b666a1650.
20. Pantucci, *A Typology of Lone Wolves*, 34.
21. Weimann, "Lone Wolves in Cyberspace."
22. M.W. Zackie, "An Analysis of Abu Mus'ab al-Suri's 'Call to Global Islamic Resistance,'" *Journal of Strategic Security* 6 (March 1, 2013): 1–18, https://doi.org/10.5038/1944-0472.6.1.1; Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-First Century*, 1st edition edition (Philadelphia: University of Pennsylvania Press, 2008).
23. Sageman, *Leaderless Jihad*.
24. Laura Scaife, *Social Networks as the New Frontier of Terrorism: #Terror* (Taylor & Francis, 2017), 40.

25. Weimann, "Lone Wolves in Cyberspace."
26. Weimann.
27. Robert J. Bunker and Pamela Ligouri Bunker, *Radical Islamist English-Language Online Magazines: Research Guide, Strategic Insights, and Policy Response* (CreateSpace Independent Publishing Platform, 2018), 13.
28. Weimann, "Lone Wolves in Cyberspace."
29. Susan Currie Sivek, "Packaging Inspiration: Al Qaeda's Digital Magazine in the Self-Radicalization Process," *International Journal of Communication* 7, no. 0 (January 30, 2013): 5.
30. Jarret M. Brachman and Alix N. Levine, "You Too Can Be Awlaki Feature," *Fletcher Forum of World Affairs* 35 (2011): 31.
31. Martin Rudner, "'Electronic Jihad': The Internet as Al Qaeda's Catalyst for Global Terror," *Studies in Conflict & Terrorism* 40, no. 1 (January 2, 2017): 11–12, https://doi.org/10.1080/1057610X.2016.1157403.
32. Barak Mendelsohn, "ISIS' Lone-Wolf Strategy," August 25, 2016, https://www.foreignaffairs.com/articles/2016-08-25/isis-lone-wolf-strategy.
33. Mendelsohn.
34. Mendelsohn.
35. Daniel Byman, *Al Qaeda, the Islamic State, and the Global Jihadist Movement: What Everyone Needs to Know* (Oxford University Press, 2015).
36. Ramón Spaaij, "Lone Wolf Terrorism," in *The SAGE Encyclopedia of Political Behavior*, 2 vols. (Thousand Oaks,: SAGE Publications, Inc., 2017), 453–54, https://doi.org/10.4135/9781483391144; Weimann, "Lone Wolves in Cyberspace."
37. Tyler Welch, "Theology, Heroism, Justice, and Fear: An Analysis of ISIS Propaganda Magazines Dabiq and Rumiyah," *Dynamics of Asymmetric Conflict* 11, no. 3 (September 2, 2018): 186–98, https://doi.org/10.1080/17467586.2018.1517943.
38. Haroro J. Ingram, "An Analysis of Islamic State's Dabiq Magazine," *Australian Journal of Political Science* 51, no. 3 (July 2, 2016): 473, https://doi.org/10.1080/10361146.2016.1174188.
39. Peter Wignell et al., "A Mixed Methods Empirical Examination of Changes in Emphasis and Style in the Extremist Magazines Dabiq and Rumiyah," *Perspectives on Terrorism* 11, no. 2 (2017): 18.
40. Michael Weiss, "An ISIS Plot to Blow Up Notre Dame Cathedral—and Rule the World?," *The Daily Beast*, September 8, 2016, sec. world, https://www.thedailybeast.com/articles/2016/09/08/an-isis-plot-to-blow-up-notre-dame-cathedral-and-rule-the-world.
41. Ahmad Shehabat, Teodor Mitew, and Yahia Alzoubi, "Encrypted Jihad: Investigating the Role of Telegram App in Lone Wolf Attacks in the West," *Journal of Strategic Security* 10, no. 3 (2017): 27–53.
42. Shehabat, Mitew, and Alzoubi.
43. Pantucci, *A Typology of Lone Wolves*.
44. Paul Joosse, "Leaderless Resistance and the Loneliness of Lone Wolves: Exploring the Rhetorical Dynamics of Lone Actor Violence," *Terrorism and Political Violence* 29, no. 1 (January 2, 2017): 52, https://doi.org/10.1080/09546553.2014.987866.
45. Joosse, "Leaderless Resistance and the Loneliness of Lone Wolves"; Schuurman et al., "Lone Actor Terrorist Attack Planning and Preparation," 1191.
46. Edwin Bakker and Beatrice de Graaf, "Preventing Lone Wolf Terrorism: Some CT Approaches Addressed," *Perspectives on Terrorism* 5, no. 5–6 (July 12, 2011): 44, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/preventing-lone-wolf.
47. Becker, "Explaining Lone Wolf Target Selection in the United States," 970.
48. Joseph Goldstein and William K. Rashbaum, "Jose Pimentel Is Charged in N.Y.C. Bomb Plot," *The New York Times*, November 20, 2011, sec. N.Y. / Region, https://www.nytimes.com/2011/11/21/nyregion/jose-pimentel-is-charged-in-new-york-city-bomb-plot.html.
49. Anderson Cooper, "60 Minutes Investigates First ISIS-Claimed Attack in U.S. and What the FBI Knew," March 26, 2017, https://www.cbsnews.com/news/terrorism-in-garland-texas-what-the-fbi-knew-before-the-2015-attack/.

50. Mosi Secret, "30-Year Prison Sentence in Plot to Bomb U.S. Bank," *The New York Times*, August 9, 2013, sec. New York, https://www.nytimes.com/2013/08/10/nyregion/30-year-sentence-for-man-who-tried-to-bomb-federal-reserve.html.
51. David Johnston and Scott Shane, "Fort Hood Suspect Communicated With Radical Cleric, Authorities Say," *The New York Times*, November 9, 2009, sec. U.S., https://www.nytimes.com/2009/11/10/us/10inquire.html.
52. Brachman and Levine, "You Too Can Be Awlaki Feature."
53. Rukmini Callimachi and Jim Yardley, "From Amateur to Ruthless Jihadist in France," *The New York Times*, January 17, 2015, sec. World, https://www.nytimes.com/2015/01/18/world/europe/paris-terrorism-brothers-said-cherif-kouachi-charlie-hebdo.html.
54. Tore Hamming, "Jihadi Competition and Political Preferences," *Perspectives on Terrorism* 11, no. 6 (December 18, 2017): 76, http://www.terrorismanalysts.com/pt/index.php/pot/article/view/657.
55. TORE REFSLUND HAMMING, "With Islamic State in Decline, What's Al-Qaeda's Next Move?," *War on the Rocks*, April 27, 2018, https://warontherocks.com/2018/04/with-islamic-state-in-decline-whats-al-qaedas-next-move/.
56. Tim Arango and Eric Schmitt, "A Path to ISIS, Through a Porous Turkish Border," *The New York Times*, March 9, 2015, sec. World, https://www.nytimes.com/2015/03/10/world/europe/despite-crackdown-path-to-join-isis-often-winds-through-porous-turkish-border.html.
57. Spaaij, *Understanding Lone Wolf Terrorism*, 10.
58. Michael Jetter, "Terrorism and the Media," *Institute of Labor Economics*, IZA Discussion Paper, no. 8497 (September 2014), https://www.iza.org/publications/dp/8497/terrorism-and-the-media; Charlie Winter, "ISIS Is Using the Media Against Itself," *The Atlantic*, March 23, 2016, https://www.theatlantic.com/international/archive/2016/03/isis-propaganda-brussels/475002/.

Reciprocal Radicalization: A New Framework for Analysis and the Case of al-Muhajiroun and the English Defence League in Britain

Christopher Morris

Reciprocal radicalization has captured academic and policymaker attention over the past decade with its assertion that group interaction can independently generate extreme beliefs and behaviors. However, it remains an ambiguous concept with unclear causal mechanisms, which prevents it from effectively guiding policy. To address these shortcomings, this article draws on the psychological Social Identity Approach (SIA) to develop a new framework called the Social Identity Theory of Reciprocal Extremism (SITRE). *Fusing group and individual processes, SITRE proposes that extremist groups contribute to each other's recruitment through practices that (1) create identity crises that push individuals toward joining each other's groups; and (2) reinforce each other's narratives and their persuasive ability to pull individuals toward extremism. To examine SITRE's explanatory potential, the article examines a crucial case of reciprocal radicalization in Britain: the far-right English Defence League (EDL) and Islamist al-Muhajiroun (ALM). Using interview data and content analysis, the article finds strong support for SITRE's two pathways with EDL and ALM practices driving identity crises, strengthening narratives, and reciprocally driving each other's recruitment. Based on these findings, practitioners can disrupt violent reciprocal radicalization with two key strategies: intra-group targeting, e.g. prototypical leadership removal, and inter-group process targeting, e.g. controlling group contact. With the recent release of EDL and ALM leadership from prison and the far-right's resurgence, understanding reciprocal radicalization is a pressing task for academia and policy, and SITRE offers a powerful framework for those upholding order and security.*

Reciprocal Radicalization: A New Framework for Analysis and the Case of al-Muhajiroun and the English Defence League in Britain

"I am just a regular White man . . . who decided to take a stand to ensure a future for my people," wrote Brenton Tarrant before he walked into two New Zealand mosques and shot 50 people.[1] In response, al-Qaeda condemned the attacks as a "heinous crime committed by a group of racist crusaders" while Islamic State media urged retaliation: "We advise you to attack in churches or discotheques and other open places."[2] The following month, two Islamist groups unleashed a devastating attack against Sri Lanka's churches and hotels with nine suicide bombers killing over 250 people.[3] These tit-for-tat attacks, from New Zealand to Sri Lanka, highlight the growing importance of an under-appreciated dynamic: reciprocal radicalization between extremist groups where Islamists and the far-right reinforce each other's ideologies and fuel a spiral of violence.

Interest in reciprocal radicalization has burgeoned over the past decade with the media, government, and academia emphasizing its importance, but it remains a nebulous concept and provides unclear policy guidance.[4] Bridging the chasm between individual and structural causes, reciprocal radicalization captures how radicalization often emerges in a relationship where extremist groups symbiotically develop each other's beliefs and actions.[5] However, significant ambiguity remains concerning reciprocal radicalization's precise causal mechanisms, intra-group dynamics, and outcome indicators. Such conceptual weakness permits deterministic arguments of endless violence spirals that overlook the

historical record and countervailing factors. Consequently, reciprocal radicalization in its current state could amplify risk, inform ineffective policy, and paradoxically reinforce radicalization by confirming extremist narratives.

To address these challenges, this article develops a reciprocal radicalization framework called the *Social Identity Theory of Reciprocal Extremism (SITRE)*. SITRE proposes that extremist groups contribute to each other's recruitment through practices that (1) create identity crises that *push* individuals toward joining each other's groups; and (2) reinforce each other's narratives and their persuasive ability to *pull* individuals toward extremism. For example, Brenton Tarrant reveals that the Islamic State's 2017 Stockholm attack threatened his identity and *pushed* him toward extremism: "The first event that begun the change was the terror attack in Stockholm . . . They were attacks on my people . . . attacks on my soul."[6] Subsequently, Tarrant viewed far-right material online that used Islamist attacks to justify white nationalism, and he affirms these narratives were persuasive and *pulled* him "further and further into the belief of violence over meekness."[7] Such reciprocal processes play out daily worldwide and become tragically apparent when they erupt in violence.

The article proceeds by first reviewing reciprocal radicalization's literature, conceptual weaknesses, and policy implications. Next, the article draws on a strand of psychology called the Social Identity Approach (SIA) to develop SITRE and its two causal push-pull pathways. To evaluate SITRE, the article applies it to a crucial case of reciprocal radicalization in the United Kingdom. By examining interactions between the far-right English Defence League and Islamist al-Muhajiroun, the article finds significant empirical support for SITRE's two pathways. Lastly, the article concludes with SITRE's policy implications and avenues for future research.

Reciprocal Radicalization: Origins, Shortcomings, and Implications

Over the past decade, the phenomenon of reciprocal radicalization has garnered academic and practitioner interest, but it remains an ambiguous concept and risks informing counterproductive policy. Theorizing on reciprocal radicalization can be traced to Eatwell's 2006 article on "cumulative extremism" where he proposed "one form of extremism can feed off and magnify other forms."[8] Subsequent studies have termed this process "tit-for-tat radicalization," "cumulative radicalization," and "co-radicalization," but "reciprocal radicalization" has emerged as the most commonly used term.[9] Empirically, reciprocal radicalization receives support from studies that find terrorism spurs retaliatory hate crimes, tactical encounters increase inter-group extremism, and extremist groups construct mirror-image narratives.[10] Such academic research has proven influential; for example, the U.K.'s *CONTEST* strategy now recognizes that "Islamist and extreme right-wing groups have at times reinforced . . . each other."[11] Given these policy consequences, reciprocal radicalization should be conceptually precise and its causal mechanisms explicit, yet it remains undertheorized and cannot presently guide effective policy.

Reciprocal radicalization's unclear outcome indicators, causal mechanisms, and operating parameters yield conceptual ambiguity; consequently, practitioners receive inconsistent guidance for intervention. Radicalization is already a vigorously contested concept, and its reciprocal generation amplifies debate over whether it should be measured by extreme beliefs or violence.[12] While violence could provide a rough measure, most radicalized individuals are non-violent; thus, an accurate indicator must also capture extreme beliefs.[13] However, even if studies utilized an accurate indicator, the causal pathways behind reciprocal radicalization are underspecified. Direct extremist encounters

likely facilitate reciprocal radicalization, but Busher and Macklin emphasize that it could also operate through narratives and by shaping communities and societal perceptions.[14] Thus, studies need to span multiple levels, from extremist engagements to their broader national contexts, to capture reciprocal radicalization's intertwined pathways. These higher-level contexts further compound the challenge since studies must also examine processes over extended periods of time that tie together extremist encounters.

Most problematically, reciprocal radicalization's ambiguity and mechanical inter-group escalation permit arguments of inevitable violence that validate extremist narratives and provide questionable policy guidance. For example, Ebner predicts a "spiraling violence effect" between extremist groups "where one side's action increasingly leads to a retaliatory reaction."[15] Such arguments overlook contrary evidence and moderating factors like inter-group coupling patterns and intra-group processes. During the 1990s, for instance, Britain's fascist (BNP) and anti-fascist (AFA) groups deescalated because BNP leadership shifted from violence to electoral politics.[16] Furthermore, Bartlett and Birdwell highlight that groups are often asymmetrically coupled with unequal radicalization and violence can shock group members to deescalate.[17] This latter point highlights the "internal brakes" on reciprocal radicalization, which range from strategic shifts to weak cohesion.[18] For example, violence between Combat 18 fascists and AFA dissipated in late-1990s Britain because Combat 18 imploded from internal feuding. Claims of spiraling violence overlook these moderating factors and draw policy implications that amplify risk; paradoxically, they may fuel reciprocal radicalization by influencing policies that confirm extremist narratives.

Evidently, reciprocal radicalization is a complex phenomenon, but influential theoretical approaches, from Eatwell in 2006 to Ebner in 2017, provide insufficient clarity and potentially counterproductive policy guidance. Thus, a new framework for analysis is required that specifies outcomes, mechanisms, and inter/intra-group factors. Busher and Macklin suggest one potential framework is "competitive escalation" from Social Movement Theory (SMT), but they also conclude that research "would benefit from approaches that combine group-level analysis with analysis of individual participation."[19] Therefore, this article develops a framework from the Social Identity Approach (SIA), which integrates theories of individual and group behavior, and directly answers Busher and Macklin's call for a robust theory of reciprocal radicalization.

A New Framework: The Social Identity Approach and Reciprocal Radicalization

The Social Identity Approach (SIA) offers a powerful lens to examine reciprocal radicalization's group processes, since it descends from a European tradition of social psychology that stresses the interplay of groups and individuals.[20] Accordingly, the SIA aims to "account for when and how social structures and belief systems impact on what people do" and provides explanations across multiple levels by fusing sociology with cognitive science.[21] Individuals are the proximal actors who pull the trigger, and their mindsets are important, but the SIA affirms these actors are shaped by social groups, their wider context, and in turn, their actions reshape society. By leveraging the SIA's flexible analytical lens and emphasis on group dynamics, a new framework can be forged to capture reciprocal radicalization's processes and guide interventions.

Two theories constitute the SIA and provide the foundation for a new framework: Social Identity Theory (SIT) and Self-Categorization Theory (SCT). SIT asserts that individuals possess social identities based on group memberships from which they derive self-esteem; thus,

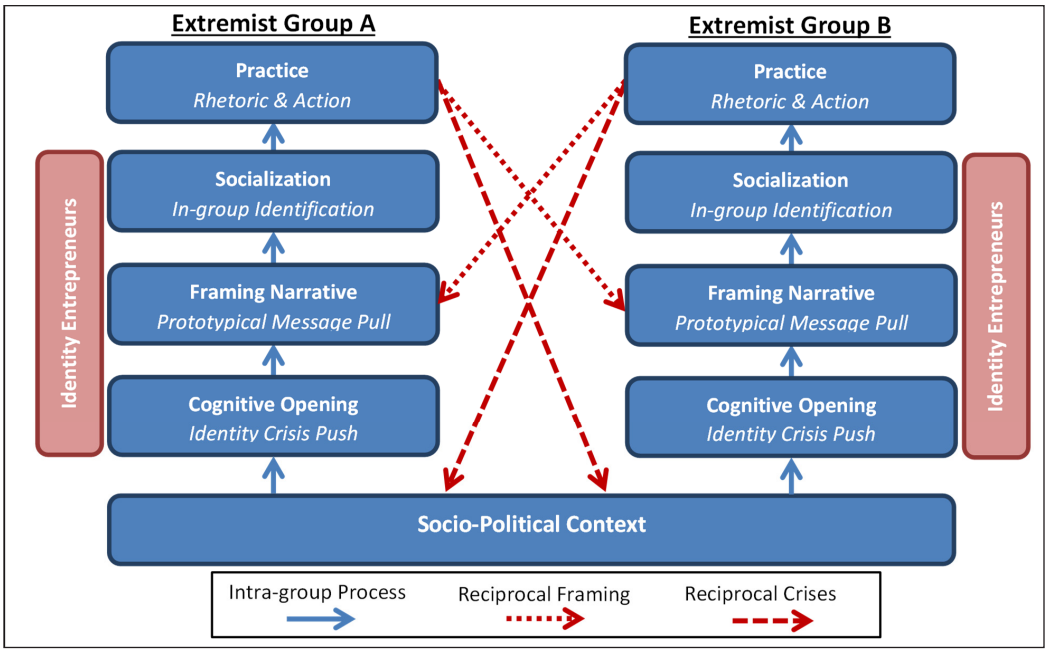


Figure 1: Social Identity Theory of Reciprocal Extremism (SITRE) Framework

group threats motivate collective behavior to restore positive identity.[22] Synergistically, SCT states that individuals automatically self-categorize into groups based on their social context, and this process underpins group phenomena, from social influence to collective violence.[23] Given these theories' far-reaching implications, interest in the SIA has surged in terrorism studies with scholars applying it to extremism, radicalization, and terrorist disengagement.[24] Reciprocal radicalization, however, has yet to be comprehensively analyzed through the SIA's dual theories, which is a significant gap in the literature that can be filled with a new theoretical framework.

Drawing from the SIA, this article proposes a new reciprocal radicalization framework called the *Social Identity Theory of Reciprocal Extremism (SITRE)*. SITRE proposes that tightly coupled extremist groups contribute to each other's recruitment through practices that (1) create identity crises that *push* individuals toward joining each other's groups; and (2) reinforce each other's narratives and their persuasive ability to *pull* individuals toward extremism.

The framework deliberately adopts reciprocal *extremism* to sharpen the outcome of reciprocal radicalization as socialization of individuals into extremism. Following J.M Berger, extremism is "the belief that an in-group's success or survival can never be separated from the need for hostile action against an out-group."[25] This definition avoids bias from defining extremism in relation to a mainstream, emphasizes *belief* content, and does not predetermine violence. The SITRE framework draws on Wiktorowicz's four-stage radicalization model to structure SIA processes in one group and mirrors this structure to create an extremist group dyad with reciprocal processes (Figure One, overleaf).[26]

As illustrated above, SITRE's framework encompasses the socio-political context, intra-group radicalization, and two reciprocal radicalization mechanisms: framing and identity crises. Beginning with the potential recruit, radicalization requires a "cognitive opening" to alternate beliefs and "frame alignment" with an extremist narrative.[27] SITRE proposes identity crises create cognitive openings while prototypical message framing increases

frame alignment. These two stages are the reciprocal inputs between extremist groups, and the article elaborates them in subsequent sections. After frame alignment, individuals undergo "socialization" where they adopt extremist beliefs, which SITRE specifies as self-categorization, de-personalization, and adoption of a new social identity.[28]

Throughout this process, extremists who are prototypical (representative) of the group act as "identity entrepreneurs" and define "who we are" and "what we should do."[29] Such entrepreneurs shape radicalization by stirring crises, crafting persuasive narratives, and guiding socialization. Once individuals self-categorize into extremist groups, they conform to group stereotypes, follow prototypical members, and engage in collective behavior.[30] Crucially, these group practices are outputs that provide inputs into other extremist groups' cognitive openings and framing narratives, which ultimately drives the process of reciprocal radicalization.

Push Factor: Reciprocal Generation of Identity Crises

Extremist groups generate cognitive openings for each other's recruits when their practices shape society, distort salient group categories, and prompt identity crises. According to Wiktorowicz, "a crisis can produce a 'cognitive opening' that . . . renders an individual more receptive to the possibility of alternative views."[31] Crises range from the economic to the personal, but SITRE focuses on Wiktorowicz's socio-cultural category and proposes extremist practices cause identity crises and cognitive openings. Specifically, identity crises occur when extremist actions and rhetoric make a threatened social identity salient for the recipient. SCT indicates that this process is automatic because self-categorization into social groups occurs based on salient categories in a given social context.[32]

While SCT captures how extremists fuel crises by making threatened identities salient, SIT suggests individuals are then motivated to seek alternate views by the need for identity and self-esteem. SIT states that individuals derive self-esteem from their social identity; thus, group threats motivate behaviors to restore positive identity through diverse strategies.[33] Extremism is one seductive solution because its maximal inter-group differentiation provides clear purpose, identity, and self-esteem. Not all individuals with identity crises become extremists, however, since not all encounter extremist narratives. From SITRE, the following hypothesis is derived:

> **H_1:** Extremist practices make a threatened identity salient for recipients and raise the likelihood of them pursuing alternate beliefs like extremism to restore self-esteem.

Pull Factor: Reciprocal Generation of Persuasive Frames

When extremist groups confirm each other's narratives with their actions, they boost narrative credibility and their capacity to persuade recruits into adopting their worldviews. Wiktorowicz proposes that recruitment relies on belief or "frame" alignment between extremists and recruits, and closing the gap between these beliefs depends on persuasive narratives.[34] Since extremist beliefs are often conspiratorial and patently false, extremist narratives must strongly "resonate" with recruits and persuade them to adopt new beliefs.[35] SCT indicates such narratives persuade by influencing the recruit's perceived context, making salient conflictual inter-group relations, and encouraging the recruit to self-categorize into the same group as the extremists.

Recruiters facilitate this persuasive process by acting as "identity entrepreneurs" and craft narratives that portray extremists as the true defenders of the recruit's social group against out-group threats.[36] Once recruits self-categorize into the same group as the extremists, they look to the most prototypical or representative

extremists for guidance on what to believe and how to act, which provides these members with influence over recruits. Such influence enables further indoctrination and generates extremist ringleaders' *charismatic leadership* not as a personal trait but as a group-level attribute bestowed on prototypical members by their followers.[37]

Persuasive framing becomes reciprocal when the actions of one extremist group increase the narrative and speaker prototypicality of another extremist group. SCT indicates that when an extremist group confirms the external threat claimed by another group, inter-group difference sharpens and makes extremist group leaders appear more representative and influential. For example, when a social group led by moderate leaders faces a credible out-group threat, the inter-group comparison shifts the group's most prototypical member in an opposite direction to the threat and moderates lose their social influence.[38] Extremists leverage this process and invoke narratives with threatening out-groups to increase their influence; however, their actions can reciprocally empower another group's extremist factions and generate a cycle of inter-group extremism. SITRE provides a hypothesis for assessment:

> **H_2:** Extremists increase the persuasiveness of their narratives by using each other's practices to construct threatening out-groups in relation to in-groups that envelop target recruits.

Methodology

To assess SITRE and its hypotheses, this article employs a crucial case design with a single most-likely case of reciprocal radicalization. Such a design is suitable for initial theory-testing and provides moderate theoretical leverage if the theory holds, which would justify more resource-intensive designs like structured comparisons with negative cases.[39] Given reciprocal radicalization's relational basis, a single most-likely case requires examination of two extremist groups in dynamic interaction where SITRE's conditions and variables are strongly satisfied. After surveying extremist dyads, the author selected the English Defence League and al-Muhajiroun in Britain due to their tight coupling, overt interaction, and persistent hostility. To examine reciprocal recruitment pathways, the article utilizes structured interviews from prior ethnographic studies. This data is combined with content analysis of extremist leadership rhetoric to assess reciprocity of extremist narratives and their persuasiveness. If the evidence supports SITRE's framework, then intensive primary research will be justified for future studies.

Reciprocal Radicalization in Britain: Islamist and Far-Right Extremists

The hostile relationship between the English Defence League (EDL) and al-Muhajiroun (ALM) provides a rich case of reciprocal identity crises and framing narratives that have fueled a wave of British far-right and Islamist extremism. EDL and ALM members frequently cite each other's practices as out-group threats that push them into high-risk activism while their leaders use each other's practices to justify their ideologies and maximize persuasive pull. While EDL and ALM activities are forceful but largely non-violent, both groups are connected to individuals who have committed terrorism, e.g. Jo Cox's 2016 assassination and the 2017 London Bridge attack. To better understand these processes and outcomes, the article first introduces each group and their basic interaction and then examines their reciprocal mechanisms in-depth through SITRE's lens.

Founded in London in 1996, ALM predates the EDL and was established by Omar Bakri Muhammed, a Syrian-born immigrant, as an offshoot of the Islamist group Hizb ut-Tahrir. Committed to a Salafi-Jihadi ideology, ALM locates sovereignty in Allah, rejects democracy and free-markets, and works through activism

to establish the *Sharia* (law) under a global *Khilafah* (caliphate). ALM qualifies as an extremist group where in-group success is inseparable from out-group hostile action because its members believe all *kuffar* (non-believers) must convert to their brand of Islam or burn in hellfire.[40] ALM received increased scrutiny post-9/11, but it has proven resilient and established at least 11 front organizations between 2004 and 2014.[41] During this period, Anjem Choudary replaced Bakri and provided ideological coherence, but his recognition of ISIS's caliphate in 2014 resulted in his arrest and a leadership vacuum. ALM has gained notoriety as a "conveyor-belt" to terrorism with its members linked to 24% of U.K. terrorism cases.[42] However, most members do not radicalize to violence; rather, its 250-350 activists conduct provocative activism, which in 2009 led outraged Luton residents to create the EDL.[43]

The EDL formed in June 2009 in response to an ALM demonstration in Luton against the British Army and sparked the beginning of Britain's mass "Counter-Jihad" movement. Outraged by ALM, a group of Lutonians created the EDL and Tommy Robinson (Stephen Yaxley-Lennon) emerged as the EDL's figurehead. While it initially focused on Islamist extremism, the EDL quickly came to espouse an Islamophobic, cultural nationalist ideology that upholds "the English tradition" against the "rape jihad" of "global Islamification."[44] Thus, EDL's ideology differs from the neo-fascism of the BNP and National Front, but it clearly registers as extremist since its members believe their group's survival requires action against an insidious Islamic out-group.[45]

From 2009 to 2015, the EDL established 90 local and issue-based divisions, gained over 100,000 Facebook followers, and held 10-15 demonstrations of up to 2,000 people each year.[46] EDL rallies and their anti-Muslim hooliganism, however, spurred ALM protests and plots to bomb soldiers in 2011 and EDL's Dewsbury rally in 2012.[47] In turn, as EDL growth stalled, the May 2013 beheading of Lee Rigby by former ALM members reinvigorated the EDL with their rallies again attracting 2,000 people.[48] Nevertheless, the EDL eventually fragmented in late-2013 due to BNP infiltration, factionalism, and Robinson's imprisonment and surprise resignation.

The EDL persists as a diminished group, but its ideology has proven influential by inspiring new Counter-Jihad groups, from Britain First to Robinson's PEGIDA UK.[49] While the EDL has never directly supported terrorism and posed more of a public order challenge, its materials have inspired right-wing terrorists, from Anders Breivik in 2011 to Darren Osborne in 2017.[50] Given the consequences of EDL-ALM interaction, their potential to reignite and inspire, and their similarity to contemporary Islamist and far-right interaction, understanding EDL-ALM reciprocal pathways is a vital task for both academia and policy.

EDL-ALM Reciprocal Identity Crises

SITRE's first hypothesis suggests that EDL and ALM practices generate cognitive openings for each other's recruits by creating identity crises and searches motivated by self-esteem. Starting with ALM, multiple push factors exist from friendship to crime, but Michael Kenney concludes after five years of fieldwork that ALM's "strategy is tailored to young men and women who seek identity and belonging."[51] In the words of one ALM recruit, he was "a young Muslim . . . who felt racism and discrimination around me" and had a "lack of self-esteem," but "Choudary and his group made me feel wanted."[52] Perceived out-group racism and low self-esteem generate identity crisis and search, and this process became reciprocal when the EDL generated out-group threats.

According to the West Midlands Counter-Terrorism Unit, the EDL's demonstrations created a more receptive environment for ALM recruiters who could say: "this is the way white Western

society sees us."[53] One of the most significant consequences of this EDL-driven identity threat and push toward extremism was the failed ALM-linked plot to attack the EDL's June 2012 Dewsbury rally. Six individuals who witnessed EDL rallies and sought out guidance from ALM travelled to the rally but arrived late, and only a traffic stop uncovered their IED, weapons cache, and a retaliation letter to the EDL.[54] Through their lawyers, the men reveal that the EDL rallies were "intimidating, they are insulting" and they were pushed toward Islamist extremism out of "fear and loathing about their communities being attacked" by the EDL's followers.[55]

EDL rallies deliberately marched through Muslim communities and provided a salient out-group threat which, combined with ALM accessibility, pushed individuals into extremism. The EDL's February 2011 rally in Luton proved particularly consequential with its anti-Muslim violence serving as the out-group threat that helped radicalize locals Zahid Iqbal and Khalid Masood. Immediately after the rally, Iqbal stated that "he wanted to shoot EDL," contacted ALM, and led the failed September 2011 Toy Car Bomb plot. Similarly, Masood yelled "if they were to come to my town again I'd kill them," sought ALM material, and later conducted the 2017 Westminster Bridge attack.[56] Since none of these individuals were Islamists prior to the EDL rallies and were well-integrated, it is unlikely they would have radicalized at that moment without the EDL. In turn, these incidents became the threats that pushed people toward the EDL.

As with ALM recruitment, there are multiple pathways to the EDL, but identity crisis and search is the common thread that runs through the accounts of activists. Based on her three-year field study, Hilary Pilkington asserts that most EDL recruits are "converts" without a background in far-right activism or racism.[57] Identity is a major conversion component, which Joel Busher's two-year field study affirms is "common to every activist's account of their journey into EDL."[58] Busher further notes that activists almost always cited fear and outrage over perceived Islamist threats to a traditional British identity from the aforementioned ALM incidents.[59] Indeed, EDL membership surged after ALM's initial 2009 Butchers of Basra protest, the 2010 ALM Remembrance Day poppy burning, and the ALM-linked Lee Rigby beheading in 2013.[60] While these high-level trends suggest Islamist out-group threats generate identity crisis and push individuals to the EDL, interviews with members provide more granular and revealing evidence.

Examination of several EDL activist interviews supports the argument that ALM served as an out-group threat, which sparked identity crisis, and pushed them toward the EDL. As true "converts," none of the interviewees were far-right until after encountering the ALM. Ivan Humble, a former EDL organizer, states: "it all started for me when the radical Islamic preacher Anjem Choudary . . . interrupted a homecoming parade" which made him "angry and frustrated," so he searched online and "joined the EDL for what they stood for . . . against the radical hate."[61]

Former member Darren Carroll also cites the parade protest but elaborates that "I felt threatened. You hear Anjem Choudary . . . I started to fear. Fear for my kids, for my family . . . it felt like al-Qaeda's gonna jump out the woodwork." Wanting his "heritage to always remain" but feeling "disenfranchised," Darren sought out an early EDL rally in 2009 where "I might get listened to," but the growing presence of neo-Nazis at rallies made him feel "like I had lost my identity" and he disengaged by 2011.[62] Lastly, Chris Skellorn, a former member, similarly reiterates out-group threat "of Muslims taking over . . . the way I felt in a white working class community . . . I saw them burning poppies and it angered me." After ALM's 2010 poppy burning, Chris searched for a platform and went with friends to EDL's Leeds rally

where he "felt like I was getting heard," but he admits "you just going along with what's there at the time, it's a sheep mentality."[63] These three accounts illustrate ALM's reciprocal push of EDL activists, but such pushes were only sufficient with SITRE's second factor: persuasive narratives.

EDL-ALM Reciprocal Framing Narratives

SITRE's second hypothesis suggests that EDL and ALM practices increase the recruiting 'pull' of each other's narratives by helping their leaders construct out-group threats to target audiences, which enhances their charisma and persuasiveness. Beginning with the EDL, Tommy Robinson emerged as its figurehead because his "typical bloke off a council estate" demeanor made him a highly prototypical group member. In contrast to his unassuming personality and strained speech, Robinson's position in the group endowed him with influence and generated his group-specific charisma. Robinson resonated with audiences, and the more he maximized inter-group difference by highlighting out-group Islamist threats, the more his audiences roared "Tommy! Tommy!"[64] Robinson pulled new members in with his charismatic influence, and members compared him to Nelson Mandela for "speaking up for the people" and enduring hardship.[65] ALM injected reciprocal influence into this process when their practices increased the credibility of Robinson's narratives and enabled him to increase intergroup difference and his persuasive pull on followers.

From 2009 to 2013, Robinson's live and recorded speeches attracted and mobilized thousands of individuals, drew on ALM practices to justify out-group threats, and demonstrated an uncanny interdependence with ALM speeches. ALM's repeated declaration of coming *Sharia* became a centerpiece of Robinson's performances that enabled him to weave ALM's extremism into a wider Islamic threat. This conflation yielded an England vs. Islam dynamic that increased the narrative's pull for people pushed toward the EDL.

For example, Robinson's 2010 Christmas message begins by highlighting ALM's earlier Remembrance Day protest where they burned symbolic poppies. Outraged, Robinson exclaims: "Choudary is swanning round this country causing mayhem . . . every single member of the British public are incited." Having established the ALM hook, Robinson defines the in-group: "we want to protect this country . . . this is about protecting our way of life." Finally, he uses ALM to construct a threatening Islamic out-group to justify his call to action: "the whole world is looking to the EDL who are rising up against the oppression of Islam."[66] Over the years Robinson refined his narrative and delivered an impassioned speech at the July 2013 EDL Birmingham rally where he opened with Lee Rigby's murder and the EDL bomb plot. Robinson warns "what happened to Lee Rigby will happen again" and ties this ALM-linked act to Muslims when he asks "why are they not integrating?" He further widens the out-group to inept politicians and Antifa, and wields influence with call-responses of "Whose streets? Our streets!"[67] Clearly, Robinson's speeches and influence benefited from ALM actions that confirmed the out-group threat claimed by EDL.

When EDL rallies produced street violence against Muslims, they reciprocally provided ALM with further material to justify its *Khilafah* and for Choudary and his associates to bolster their persuasive influence. Kenney's fieldwork indicates that recruits felt Choudary represented them and therefore found him charismatic.[68] By drawing extreme inter-group comparisons of all the *kuffar* against the ALM, Choudary maximized his group prototypicality, which increased his charismatic influence. EDL practices aided Choudary's construction of ALM narratives by providing specific examples of *kuffar* activity that he used to justify a large *kuffar* out-group threat and need for *sharia*. For example,

Choudary proclaimed during a street proselytizing speech (*da'wah)* that "In Western Europe you can see the plague of right-wing fascism . . . the EDL are taking the hearts of the youth. Why?" In response, he ties the EDL and right-wing groups into a wider failure of liberal democracy and the need for *sharia*: "because of frustration with the government not providing basic needs. The solution to this is . . . *Sharia*. I urge you to come forward . . . Let us discover the truth together."[69] Evidently, ALM benefited from EDL actions in crafting persuasive narratives just as the EDL benefited from ALM practices.

Conclusion: Findings and Implications

The Social Identity Theory of Reciprocal Extremism (SITRE) offers a new framework to capture interaction between extremist groups, and it demonstrated its explanatory power in the case of al-Muhajiroun and the English Defence League. As postulated by SITRE's first causal pathway of reciprocal identity crises, EDL and ALM practices served as out-group threats for each other's recruits, which pushed them toward extremism. Moreover, as SITRE's second causal pathway of reciprocal narratives suggested, EDL and ALM practices helped each other's leaders construct prototypical narratives that maximized their persuasive pull of recruits. Combined, these two reciprocal pathways facilitated radicalization into extremism by increasing the probability that a recruit would experience a cognitive opening and encounter a sufficiently persuasive narrative.

By specifying outcomes, mechanisms, and conditions, SITRE provides a framework that addresses several challenges within the reciprocal and wider radicalization literatures. Using the SIA lens, SITRE captures the interplay of individuals with group processes and wider society in a structurationist model, which balances agency and context. Moreover, SITRE's meso-level framework, informed by the SIA, generalizes beyond idiosyncratic cases of radicalization and provides greater insight than structural root causes. Answering the question of why some but not others radicalize, SITRE emphasizes contingency and suggests individuals who do not face identity crisis, encounter a framing narrative, and find that narrative persuasive, are unlikely to become extremists. Despite these strengths, SITRE could be critiqued for privileging identity and confounding reciprocal and exogenous radicalization. SITRE recognizes identity is not the only radicalization cause but, following Sageman, it asserts identity is pervasive and often the most important factor.[70] Moreover, SITRE's interplay of reciprocal and exogenous radicalization is a key framework strength that illuminates their relative prevalence and captures social complexity.

Beyond theory development, SITRE offers several policy insights contingent on further empirical verification of the framework. Beginning in the United Kingdom, Choudary's release from prison in October 2018 and Robinson's pursuit of a mainstream political platform could increase far-right and Islamist reciprocal radicalization. However, Choudary and Robinson would need to activate SITRE's pathways by employing renewed rhetoric of out-group threats and practices that threaten communities. As long as Choudary's stringent two-year release conditions are enforced and Robinson learns from his EDL experience and tempers his rhetoric, reciprocal radicalization is unlikely. More broadly, for countering-violent extremism (CVE) policies, SITRE indicates governments can deescalate reciprocal radicalization with two types of intervention. Targeting intra-group processes, governments can attempt to remove prototypical leaders like with Choudary, which can collapse one half of the dyad. Alternatively, governments can target reciprocal narratives by blocking extremist content and avert reciprocal crises by limiting group contact and movement.

Nonetheless, governments must proceed with caution to avoid becoming

a third actor and exacerbating reciprocal radicalization. This latter point suggests that future research would benefit from broadening SITRE to capture reciprocal processes between three or more groups. Furthermore, future research needs to test SITRE with negative cases to establish wider generalizability. By integrating multiple levels, reciprocal mechanisms, and intra-group processes, SITRE offers a new framework for understanding reciprocal radicalization that can help practitioners prevent the worst consequences of extremism.

About the Author:

Christopher Morris is a graduate student in Georgetown's Security Studies Program and has worked for Senate Leadership and the Committee on Homeland Security and Governmental Affairs. Prior to Georgetown, Chris graduated from the University of St Andrews, Scotland, with a First Class M.A. (Hons) degree in International Relations. Chris's interests span radicalization, emerging threats, and transatlantic relations, and he is currently directing an international study on extremist leadership in far-right and Islamist groups. All views expressed are his and not necessarily those of any affiliated organization. He can be reached at 202-599-7952 or at cjm294@georgetown.edu.

Endnotes

1. Quote from manifesto see Brenton Tarrant, "The Great Replacement," March 2019, 7.
2. Muntasir Media, *They Are of One Religion Islam Is the Target*, 2019; Al-Andalus, "Statement of Condolences" (AQIM, March 18, 2019).
3. While planning for the Sri Lanka bombings likely predated Tarrant's attacks, the influence of his actions on subsequent events cannot be ruled-out see Dilrukshi Handunnetti, "Sri Lanka Attack 'retaliation' for NZ Massacre: Minister," *Al Jazeera News*, April 23, 2019.
4. For sector examples see Nikita Malik, "The Real Terrorist Risk in Europe Is 'Reciprocal Radicalisation,'" *The Independent*, December 22, 2016; Raffaello Pantucci, "A View from the CT Foxhole: Neil Basu UK Counterterrorism Chief," *CTC Sentinel* 11, no. 2 (February 2018); Seamus Hughes, "Prepared Testimony for Hearing: Allies Under Attack" (HFAC, June 27, 2017), 6–7.
5. For structural vs. individual explanation issues see Tore Bjorgo, ed., *Root Causes of Terrorism* (London: Routledge, 2005).
6. Quote from manifesto see Tarrant, "The Great Replacement," 10.
7. Quotes from manifesto see Tarrant, 8, 17.
8. Roger Eatwell, "Community Cohesion and Cumulative Extremism in Contemporary Britain," *The Political Quarterly* 77, no. 2 (2006): 205.
9. For tit-for-tat radicalization see Paul Jackson and Michael Feldman, "The EDL: Britain's New 'Far-Right' Social Movement" (University of Northampton, 2011); for cumulative radicalization see Jamie Bartlett and Jonathan Birdwell, "Cumulative Radicalization: A Review of Evidence" (Demos, November 2013); for co-radicalization see Douglas Pratt, "Islamophobia as Reactive Co-Radicalization," *Islam and Christian–Muslim Relations* 26, no. 2 (2015): 205–18; for reciprocal radicalization see Donald Holbrook, "Far Right and Islamist Extremist Discourses: Shifting Patterns of Enmity," in *Extreme Right Wing Political Violence and Terrorism*, by Max Taylor, PM Currie, and Donald Holbrook (London: Bloomsbury, 2013).
10. Kathleen Deloughery, Ryan D. King, and Victor Asal, "Close Cousins or Distant Relatives? The Relationship Between Terrorism and Hate Crime," *Crime & Delinquency* 58, no. 5 (September 1, 2012): 663–88; Gavin Bailey and Phil Edwards, "Rethinking 'Radicalisation,'" *Journal for Deradicalization* 0, no. 10 (March 28, 2017): 255–81; Julia Ebner, *The Rage: The Vicious Circle of Islamist and Far Right Extremism* (London: I.B. Tauris, 2017), 155.
11. HM Government, "CONTEST: The United Kingdom's Strategy for Countering Terrorism" (Stationary Office, June 2018), 16.
12. Peter R. Neumann, "The Trouble with Radicalization," *International Affairs* 89, no. 4 (2013): 873–93; Alex Schmid, "Radicalisation, De-Radicalisation, Counter-Radicalisation" (ICCT, March 2013), 5–19.
13. For cognitive versus behavioral radicalization see Randy Borum, "Radicalization into Violent Extremism I: A Review of Social Science Theories," *Journal of Strategic Security* 4, no. 4 (2011): 8–9; Marc Sageman, *Misunderstanding Terrorism* (Philadelphia: University of Pennsylvania Press, 2016), 90; see also John Horgan, *The Psychology of Terrorism*, 2nd ed. (Abingdon, Oxon: Routledge, 2014).
14. Joel Busher and Graham Macklin, "Interpreting 'Cumulative Extremism': Six Proposals for Enhancing Conceptual Clarity," *Terrorism and Political Violence* 27, no. 5 (October 20, 2015): 892–94.
15. Ebner, *The Rage*, 152.
16. Graham Macklin and Joel Busher, "The Missing Spirals of Violence," *Behavioral Sciences of Terrorism* 7, no. 1 (2015): 53–68.
17. Bartlett and Birdwell, "Cumulative Radicalization: A Review of Evidence," 9–10.
18. Joel Busher, Donald Holbrook, and Graham Macklin, "The Internal Brakes on Violent Escalation: A Typology," *Behavioral Sciences of Terrorism and Political Aggression* 11, no. 1 (2019): 3–25.
19. Busher and Macklin, "Interpreting 'Cumulative Extremism,'" 899; For competitive escalation see Donatella della Porta, *Clandestine Political Violence* (Cambridge: Cambridge University Press, 2013), 70–113.

20. For European versus North American social psychology see Klaus R. Scherer, "Two Faces of Social Psychology: European and North American Perspectives," *Social Science Information* 32, no. 4 (December 1, 1993): 515–52.
21. Stephen Reicher, Russell Spears, and Alexander Haslam, "The Social Identity Approach in Social Psychology," in *The SAGE Handbook of Identities*, by Margaret Wetherell and Chandra Mohanty (London: SAGE, 2010), 45–46.
22. Henry Tajfel and John Turner, "An Integrative Theory of Intergroup Conflict," in *The Social Psychology of Intergroup Relations*, by W Austin and S Worchel (Monterary: Brooks/Cole, 1979); Henri Tajfel et al., "Social Categorization and Intergroup Behaviour," *European Journal of Social Psychology* 1, no. 2 (1971): 149–78.
23. John C. Turner et al., *Rediscovering the Social Group: A Self-Categorization Theory* (Cambridge, MA, US: Basil Blackwell, 1987).
24. J.M. Berger, *Extremism*, 1 edition (Cambridge, MA: The MIT Press, 2018); Marc Sageman, *Turning to Political Violence: The Emergence of Terrorism* (Philadelphia: University of Pennsylvania Press, 2017); Sigrid Raets, "The We in Me. Considering Terrorist Desistance from a Social Identity Perspective.," *Journal for Deradicalization* 0, no. 13 (2017): 1–28; for a strong reciprocal radicalization study that draws on SIT but engages less with SCT and wider SIA literatures see Fathali M. Moghaddam, *Mutual Radicalization* (Washington, DC: APA, 2018).
25. Berger, *Extremism*, 44; for contrasting view of extremism's inherent violence see Alex Schmid, "Violent and Non-Violent Extremism: Two Sides of the Same Coin?" (ICCT, May 2014); for policy implications see Jamie Bartlett, Jonathan Birdwell, and Michael King, "The Edge of Violence" (Demos, 2010).
26. The four stages in Wiktorowicz's model are "cognitive opening," "religious seeking," "frame alignment," and "socialization" see Quintan Wiktorowicz, "Joining the Cause: Al-Muhajiroun and Radical Islam" (Rhodes College Research Paper, 2004), 7–11.
27. Wiktorowicz, 7–9.
28. Social identity is a socially-structured field within the individual see Michael Hogg and Graham Vaughan, *Social Psychology*, 5th ed. (Milan: Pearson, 2008), 646; de-personalization is the shift from personal to social identity and is not a loss of self as Zimbardo proposes under deindividuation see Joanne Smith and Alex Haslam, *Revisiting the Classic Studies* (LA: SAGE, 2012), 126–42.
29. Stephen Reicher, S. Alexander Haslam, and Nick Hopkins, "Social Identity and the Dynamics of Leadership," *The Leadership Quarterly*, Leadership, Self, and Identity, 16, no. 4 (2005): 547–68; Niklas K. Steffens et al., "Leadership as Social Identity Management," *The Leadership Quarterly* 25, no. 5 (October 1, 2014): 1001–24.
30. Turner et al., *Rediscovering the Social Group*, 44–46; see also John Turner, *Social Influence* (California: Brooks/Grove, 1991).
31. Wiktorowicz, "Joining the Cause: Al-Muhajiroun and Radical Islam," 8.
32. Reicher, Spears, and Haslam, "The Social Identity Approach in Social Psychology," 54; Turner et al., *Rediscovering the Social Group*, 54.
33. Tajfel and Turner, "An Integrative Theory of Intergroup Conflict," 40–45; for uncertainty rather than self-esteem reduction see Michael A. Hogg and Barbara-A. Mullin, "Joining Groups to Reduce Uncertainty: Subjective Uncertainty Reduction and Group Identification," in *Social Identity and Social Cognition* (Malden: Blackwell Publishing, 1999), 249–79.
34. Wiktorowicz, "Joining the Cause: Al-Muhajiroun and Radical Islam," 9.
35. Robert D. Benford and David A. Snow, "Framing Processes and Social Movements: An Overview and Assessment," *Annual Review of Sociology* 26 (2000): 619–21; see also Dennis Chong and James N. Druckman, "A Theory of Framing and Opinion Formation in Competitive Elite Environments," *Journal of Communication* 57, no. 1 (2007): 99–118.
36. S. Alexander Haslam, Stephen D. Reicher, and Michael J. Platow, *The New Psychology of Leadership: Identity, Influence and Power* (New York: Psychology Press, 2010), 86–91; see also J.M. Berger, "Extremist Construction of Identity:" (ICCT, April 2017).

37. Daan van Knippenberg, Nathalie Lossie, and Henk Wilke, "In-Group Prototypicality and Persuasion," *British Journal of Social Psychology* 33, no. 3 (1994): 289–300; Michael A. Hogg, "A Social Identity Theory of Leadership," *Personality and Social Psychology Review* 5, no. 3 (2001).
38. This process is based on the meta-contrast principle see John C. Turner et al., "Self and Collective: Cognition and Social Context," *Personality and Social Psychology Bulletin* 20, no. 5 (October 1, 1994): 454–63.
39. Jack S. Levy, "Case Studies: Types, Designs, and Logics of Inference," *Conflict Management and Peace Science* 25, no. 1 (2008): 12–13; For structured comparisons see Alexander L. George et al., *Case Studies and Theory Development in the Social Sciences*, Fourth Printing edition (Cambridge, Mass: The MIT Press, 2005); for substantively significant cases see Gary Goertz and James Mahoney, *A Tale of Two Cultures: Qualitative and Quantitative Research in the Social Sciences* (Princeton, N.J: Princeton University Press, 2012), 184–85.
40. Quintan Wiktorowicz, *Radical Islam Rising: Muslim Extremism in the West* (Lanham, Md: Rowman & Littlefield Publishers, 2005), 57–59; Catherine Raymond, "Al Muhajiroun and Islam4UK: The Group behind the Ban" (ICSR, May 2010), 18–19.
41. Al-Muhajiroun's key aliases are Al Ghurabaa and the Saved Sect (2004-2006), Islam4UK (2008-2010), Muslims Against Crusades (2010-2011), and Need4Khilafah (2012-2014) see James Brokenshire, "Alternative Names for Proscribed Organisation Al Muhajiroun" (HMG, 2014).
42. From 1998-2015 in Hannah Stuart, "Islamist Terrorism: Analysis of Offences and Attacks in the UK" (The Henry Jackson Society, 2017), 981.
43. For membership estimates see Nick Lowles and Joe Mulhall, "Gateway to Terror: Anjem Choudary and the al-Muhajiroun Network" (Hope not Hate, November 2013), 14; Michael Kenney, *The Islamic State in Britain: Radicalization and Resilience in an Activist Network* (New York: Cambridge University Press, 2018), 5; for rejection of terrorism conveyor-belt see Kenney, 202.
44. EDL, "About Us," English Defence League, January 2016, http://www.englishdefence league.org.uk/mission-statement/.
45. George Kassimeris and Leonie Jackson, "The Ideology and Discourse of the English Defence League: 'Not Racist, Not Violent, Just No Longer Silent,'" *The British Journal of Politics and International Relations* 17, no. 1 (February 1, 2015): 171–88; for Britain's traditional far-right see Nigel Copsey and Matthew Worley, eds., *Tomorrow Belongs to Us*, 1 edition (Abingdon, Oxon: Routledge, 2017).
46. Kevin Braouezec, "Identifying Common Patterns of Discourse and Strategy among the New Extremist Movements in Europe:," *Journal of Intercultural Studies* 37, no. 6 (November 1, 2016): 637–48.
47. Dominic Casciani, "Four Jailed in Terror Bomb Plot Case," *BBC News*, April 18, 2013, sec. UK; Dominic Casciani, "Six Men Admit Plot to Bomb EDL Rally," *BBC News*, April 30, 2013, sec. UK.
48. Hilary Pilkington, *Loud and Proud: Passion and Politics in the English Defence League* (Manchester University Press, 2016); for further membership and demographics see Jamie Bartlett and Mark Littler, "Inside the EDL: Populist Politics in a Digital Age" (Demos, November 2011).
49. Tom McTague, "The Man to 'Make the British Establishment's Head Blow off,'" *Politico Europe*, December 21, 2018.
50. Matthew Taylor, "Anders Behring Breivik Had Links to Far-Right EDL, Says Anti-Racism Group," *The Guardian*, July 26, 2011; Vikram Dodd, "How London Mosque Attacker Became a Terrorist in Three Weeks," *The Guardian*, February 1, 2018.
51. Kenney, *The Islamic State in Britain*, 66.
52. Al-Muhajiroun member interview cited in Lowles and Mulhall, "Gateway to Terror," 53–55.
53. Phil Mackie, "Defence League 'Feeds Extremism,'" *BBC News*, November 19, 2010, sec. UK.
54. Central Criminal Court, "Sentencing Remarks of His Honour Judge Hilliard Q.C." (Judiciary of England and Wales, June 10, 2013); for al-Muhajiroun's connection to the plot see

Morten Storm, Tim Lister, and Paul Cruickshank, *Agent Storm: My Life Inside al Qaeda and the CIA*, Reprint edition (Grove Press, 2015), 225–27.
55. Testimony cited in BBC News, "Bomb Plot 'a Reaction to Insults,'" *BBC News*, June 7, 2013, sec. UK.
56. Gurwinder Bhogal, "The Hate Factory," *Medium*, June 2017; BBC News, "Four 'in TA Base Toy-Car Bomb Plot,'" *BBC News*, April 15, 2013, sec. UK; Dominic Casciani, "Could Khalid Masood Have Been Stopped?," *BBC News*, October 3, 2018, sec. UK.
57. Pilkington, *Loud and Proud*, 74.
58. Joel Busher, *The Making of Anti-Muslim Protest*, 1 edition (Abingdon, Oxon: Routledge, 2016), 56–58; see also Annette Linden and Bert Klandermans, "Revolutionaries, Wanderers, Converts, and Compliants: Life Histories of Extreme Right Activists," *Journal of Contemporary Ethnography* 36, no. 2 (2007): 184–201.
59. Busher, *The Making of Anti-Muslim Protest*, 52.
60. For statistics see Bartlett and Birdwell, "Cumulative Radicalization: A Review of Evidence," 5–7.
61. Ivan Humble's full interviews in BBC Three, *Former EDL Member Transformed By An Unlikely Friendship*, 2018, https://www.youtube.com/watch?v=geYk038rhnI; Ivan Humble, "Stories: Ivan Humble," The Forgiveness Project, n.d., https://www.theforgivenessproject.com/ivan-humble; Lizzie Dearden, "How Anjem Choudary Gave Birth to Tommy Robinson and the Far-Right," *The Independent*, October 17, 2018.
62. Darren Caroll's full interviews in Hsiao-Hung Pai, *Angry White People: Coming Face-to-Face with the British Far Right* (London: Zed Books, 2016), 94–96; Open Your Eyes to Hate, *Far Right Voices | Darren Carroll*, 2017, https://www.youtube.com/watch?v=ph9xDGH0Sd8.
63. Chris Skellorn's full interview in Nathan Hyde, "A Leeds Man's Journey from Marching with the EDL," *Leeds Live*, April 21, 2019; Israel Advocacy Movement, *From EDL to Islam - a Muslim Tells a Zionist His Story*, 2018, https://youtu.be/mQChVY9vneM?t=137.
64. Pilkington, *Loud and Proud*, 45.
65. Pilkington, 46.
66. EDL, *Tommy Robinsons Christmas Message*, 2010, https://www.youtube.com/watch?v=mQChVY9vneM.
67. EDL, *Robinson Speech Birmingham*.
68. Kenney, *The Islamic State in Britain*, 84–87.
69. Naseeha Sessions, *Anjem Choudary Dawah in UK*, 2015, [Video link redacted].
70. Sageman, *Turning to Political Violence*, 6.

Thucydides's Trap by the Numbers

Austin Parenteau

Graham Allison's recent book, Destined for War: Can the United States and China Escape Thucydides's Trap? *proffered sixteen examples of Thucydides's Trap scenarios in which a rising power confronted an established power. This analysis seeks to expand upon that research by conducting a quantitative analysis of the cases Allison examines to understand which are truly Thucydides's Trap situations. This analysis uses two datasets, the Correlates of War data developed by David Singer et al. for cases after 1816 and the Maddison Project economic history estimates for cases before 1816. Ultimately, although not all cases examined show compelling evidence of a Thucydides's Trap scenario when measured by hard power alone, this analysis concludes that the same proportion of cases of Thucydides's Trap (6/8) resulted in war as did Allison's analysis (12/16), implying that although the Trap may prove dangerous, it is far from inevitable.*

Introduction

Thucydides's explanation of the origins of the Peloponnesian War and the rivalry between Athens and Sparta, has fascinated policymakers, theorists, and international relations enthusiasts alike. It also forms the basis of the eponymously labelled Thucydides's Trap, which is a concept of power transition wars emphasizing a rising power confronts an established power, leading to conflict. This phenomenon has become particularly relevant in recent years, as the applicability of the trap to the current dynamics between the United States and China, undeniably the top two powers in our present global system, seems to neatly mirror the dynamics described by Thucydides in his own era, millennia ago. As the United States' power declines relative to a rapidly rising China, many scholars have asked if a similar fate awaits these two modern day behemoths.

Amongst these scholars has been Graham Allison, who published *Destined for War: Can the United States and China Escape Thucydides's Trap* in 2017 to examine this phenomenon historically. In his book and several associated articles, Allison lays out sixteen cases of proposed Thucydides's Trap scenarios throughout the last 500 years to examine how established powers in a given system handled the rise of potential peer challengers.[1] *Destined for War* provides excellent qualitative analysis of these various case studies, concluding that the rise of China does not mean inevitable war for the United States but rather suggests ongoing frictions, a "chronic condition that must be managed over a generation".[2]

However, less time has been devoted to examining the quantitative measures of these various scenarios as relates directly to Thucydides's Trap, which might allow greater predictive insight into whether the United States and China are in fact already walking a well-trod path, and if so, how far along that path they find themselves. Power transition theorists, such as Organski, Kugler, and others have previously demonstrated correlations between rivals approaching power parity and war.[3] Fewer have gone as far back as to look at cases in the 15th century, though Kim has looked as far back as 1648.[4] However, by examining Allison's chosen cases in this way, additional light can be shed on how to combine qualitative and quantitative aspects of this research.

There are two main questions to answer in this regard, which this analysis will seek to examine. The first, is whether the cases selected by Allison as Thucydides's Trap scenarios all fit the definition of a Thucydides's Trap scenario, namely a rapid

change in relative power between the two states in question. The second is whether, among those cases which do demonstrate a rapid change in relative power between two states, that rapid change in relative power necessarily coincides with war.

Methodology

Defining the Trap

Although there have been a number of interpretations that show great similarities to Thucydides's Trap in the realm of power transition theory, this analysis will focus on the definition outlined by Thucydides. The original Thucydides's Trap, as articulated by the historian himself, resulted from "the rise of Athens, and the fear that inspired in Sparta, that made war inevitable".[5] Therefore, if the Trap is correct in its assessment, we should expect to see relative power relationships which undergo rapid shifts towards parity (even if not necessarily reaching parity in terms of power) to result in war. Likewise, we would expect dyadic relationships in which there is no such dramatic shift to result in peace over that period.

The empirical evidence presented here demonstrates a story consistent with Allison's thesis in *Destined for War*, that in situations in which rapid change in the relative power of two states over a short period of time occurs, conflict often accompanies this change.[6] However, it does not demonstrate that such conflict is inevitable. Additionally, among the cases chosen by Allison, the data show not all instances actually meet the criteria of a Thucydides's Trap scenario, as they do not demonstrate rapid change in hard power metrics in the time specified. This, of course, does not address the 'fear' aspect of the Trap, but it nevertheless implies that these cases are likely best approached with some other paradigm. Of the eight cases which do demonstrate rapid change, six resulted in war during the period of transition and 2 did not. Therefore, although the data here do not support every case study as an example of the Trap, the exact same ratio of cases which did work as examples of the Trap resulted in war (6/8) as did in Allison's analysis (in which 12/16 resulted in war).[7]

Measures of Power

Having discussed the theory to be examined, there is one further critical aspect of the analysis to be discussed: how to measure relative power between states going back as far as the 15th century. For this purpose, two datasets will be employed. The first, from the Correlates of War Project, contains data for all great powers on six key metrics of national power (total population, urban population, energy consumption, iron and steel production, military expenditure, and military personnel) from 1816-2012.[8] These metrics are then aggregated for each country, year by year, into a single 'Composite Indicator of National Capability (CINC),' and represents that country's power as a fraction of the world as a whole. When comparing two country's CINC scores in a given year, it is possible to compare exactly how they stack up in aggregate across these metrics, which aim to measure military and economic power. These metrics are not perfect, of course, but they offer a plausible method for comparing how two states might compare in terms of relative power in a given year. The dataset has also been used in previous research, such as Houweling and Siccama's critique of Organski and Kugler.[9]

Prior to 1816, data unsurprisingly become far scarcer. Fortunately, an organization known as the Maddison Project has undertaken the task of providing estimates of GDP/c and population for countries and regions as far back as 1 CE.[10] As pre-1816 extends to eras before mass professional armies, a country's population might be considered a reasonable proxy for its military capability and its real GDP/c might serve as a useful proxy for its economic power. For this analysis, to attempt to match as closely as possible the Correlates of War model for CINC, these two metrics will be weighted equally. Additionally, to match the

Correlates of War model, these will then be added together to generate a 'world' total (of just those two countries), and each country's relative power score will be expressed as a percentage of this total. This is somewhat arbitrary but aims simply to ensure that there is a uniform method of examining the relative power difference both between any two countries being examined and also across cases. Failure to do this would result in nigh impossible comparisons across time.

Both of these datasets have severe limitations and drawbacks. A few potentially critical factors which are entirely missing include efficacy in use of resources, technology, and diplomacy. Although, for instance, one country might have at its disposal a great deal more resources than its rival, if it cannot marshal them in conflict as effectively, it is unlikely to be seen as a peer rival. Similarly, if one power's technology is substantially greater than another, especially if this includes a revolutionary technology, such as gunpowder or nuclear weapons, this might affect how countries might view one another in terms of relative power. Additionally, neither of these metrics makes any space for diplomacy, alliance networks, or international standing, which could, in certain instances prove compelling as an asset for a particular state over another.

One final decision which must be noted regards the exclusion of the cases in which the Habsburgs are included. Although analysis of the Habsburgs as relates to Thucydides's Trap is interesting and potentially compelling, when working with the datasets available, their empire becomes unwieldy to discuss with rigor, as their myriad intermarriages and acquisitions make it difficult to neatly map their power onto particular regions, and as the Maddison project uses regions rather than states as its unit of measurement, this makes it notably more difficult than with the Correlates of War data to maintain rigor. Although there may be future avenues of research on these cases, for the purposes of this analysis, the three cases Allison selected which included the Habsburgs will be excluded.

Methodology

For each selected case after 1816, each state's CINC power for each year is subtracted from the other in the dyadic relationship specified. This difference is then plotted year by year for the decades surrounding either the war which historically occurred between the states (or coalition of states, as some cases have) or around a point of tension in which war could have theoretically broken out, as identified by Allison.[11] For cases before 1816, the above outlined method of generating a relative power metric which mirrors CINC is plotted in the same fashion, though often, as the data estimates may occur at fifty or hundred year intervals, these older graphs are extended to show more data points and thus a better sense of any potential trends.

For the purposes of this analysis, a shift in power will be considered 'rapid change' if it meets two criteria. The first is that the relative power differential, whether measured by CINC or the approximation for older data, must double in magnitude in the quarter century before either the war or point of tension specified.

Results

Below are graphical representations of each case study used to test this hypothesis. These match those cases highlighted by Allison as potential Thucydides's Traps. In examining the 'rapid change' interpretation of Thucydides's Trap, we should expect to see large shifts in power difference preceding war. 'Large' is defined as at least doubling/halving in magnitude.

For each graph in the below, the power of the second country (after the 'V') is subtracted from the power of the first country (or coalition of countries) and this difference is graphed year by year. Periods of war are highlighted and labelled. When viewing the following graphs, it is important to bear in mind that during war, relative power may shift drastically as a result of how a conflict is progressing. These, intra-bellum shifts, should not be considered as indicative of future conflict,

Figure 1: Cases in which Thucydides's Trap war is not predicted by the data.[12,13]

and focus should be before the war sections, if any.

The five cases are all examples in which the data do not present compelling evidence of rapid change in power differential between the powers specified. In reverse historical order: In the first case, the United Kingdom and France relative to Germany show very little shift in CINC surrounding the period of German unification in 1990–91. In the second case, although Japan does rise relative to China and Russia in the 19th century, by the time it has begun its first war against either of these two powers, its differential has only changed from a high of 0.27 in 1877 to 0.23 in 1893. In the third case, the U.K. and France maintain a relatively stable power differential with Russia before and throughout the period of the Crimean War. In the fourth case, France declines relative to the United Kingdom from the medieval to the renaissance periods. However, this relationship then settles around 0.1 CINC differential (favoring France) for the entirety of this period. Although the overall change is large, it occurs over a period of several centuries. Finally, in the fifth case, not only is there little change between Spain and Portugal, but Spain is (perhaps unsurprisingly) shown to be the dominant power, rather than Portugal.

In these cases, by Thucydides's paradigm, we would expect no war in any of them. However, despite the lack of rapid, substantial change in relative power in any of the five above cases, we see wars occur in three of them. Again, this analysis does not take into account the 'fear' aspect of Thucydides's Trap, but by hard power alone, it

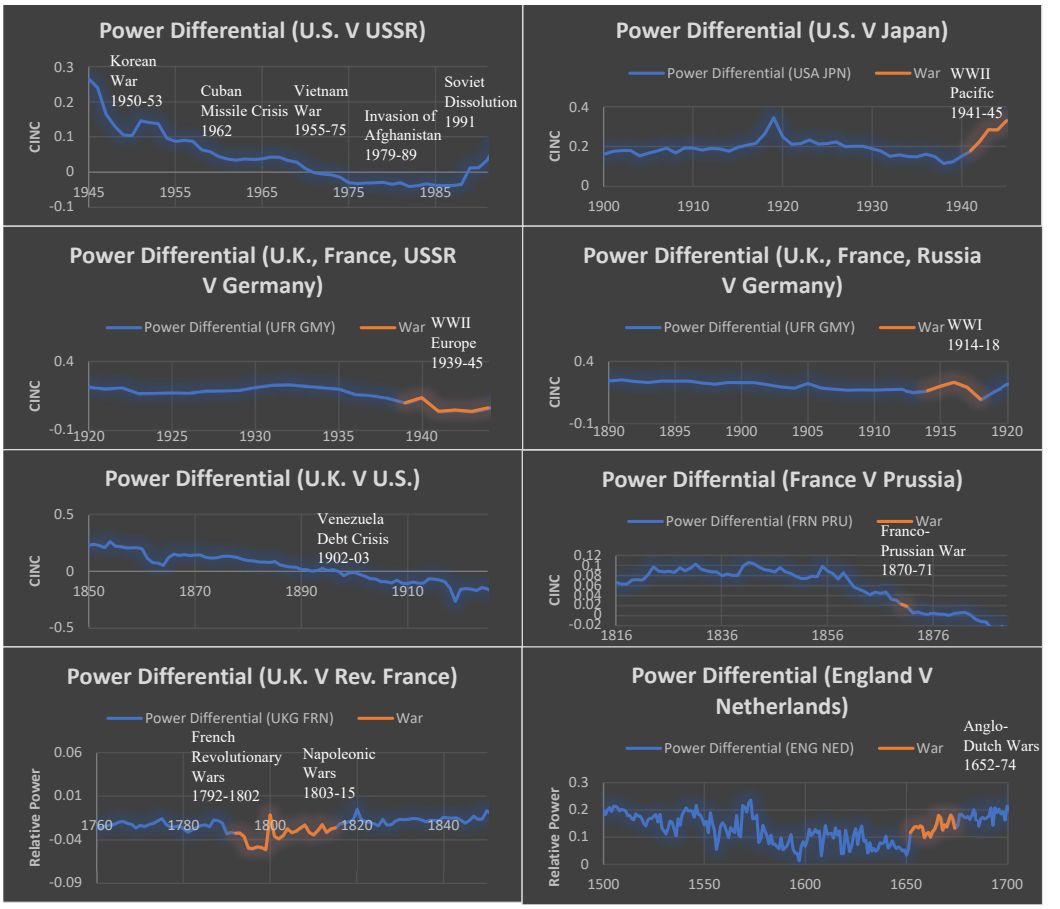


Figure 2: Cases in which the data predict a Thucydides's Trap war.[14,15]

seems that these five cases do not qualify to be genuine Thucydides's Trap scenarios.

In contrast to the five cases mentioned above which do not demonstrate rapid change as defined by this analysis in the period leading up to conflict, the eight cases here show just that. In the first case, the United States and Soviet Union not only precipitously shift in terms of relative power but also exchange the top position twice within the context of the Cold War, falling from a high immediately after WWII of 0.26 CINC difference (favoring the United States) to a low of -0.04 CINC (favoring the Soviet Union). In the second case, there is a precipitous change in relative power between Japan and the United States in the lead up to the attack on Pearl Harbor and World War II, from a difference of a high of 0.35 CINC in 1919 to 0.11 CINC in 1938. In the third case, the relative power advantage of the coalition of Britain, France and Russia drops precipitously in the lead up to WWII, falling from 0.23 in 1932 to 0.09 on the eve of WWII. A similarly precipitous drop can be seen amongst the same coalition against Germany in the prelude to WWI in the following case, with the differential falling from 0.25 in 1891 to 0.15 in 1913. In the fifth case, the United States overtakes the United Kingdom, at points slowly and at others rapidly, changing the difference in power from 0.23 CINC favoring the U.K. in 1851 to -0.27 CINC favoring the U.S. in 1919. In the sixth case, France is overtaken by Prussia in the 19th century, falling from a high of 0.09 CINC (favoring France) in

1855 to a low of -0.03 (favoring Germany) in 1893 (and continuing to decline thereafter). In the 19th and 18th centuries, for the seventh case, France rose relative to Britain leading up to the Napoleonic Wars, moving from -.016 in 1775 to -.0325 in 1793. This is just enough to count as sufficient change by our definition. In the final case, the power difference between the Netherlands and England undergoes a shift from 0.13 in 1625 to 0.03 in 1650 by the time their wars begin.

In each of the above cases, the Thucydides's Trap would predict war. In six cases, U.S./Japan, U.K., France, Russia/Germany (WWI and WWII), France/Prussia, U.K./France, and England/Netherlands, war occurs following this period of rapid relative power shift. However, the two cases which have the most drastic change are also the two in which war did not result, those of the U.K./U.S. and U.S./USSR.

The results of the graphical data analysis show eight cases of those analyzed which are consistent with the Thucydides's Trap, in that they show a rapid change in power differential between the states in question during the periods specified. Two of these nevertheless persisted in peace, despite period of intense tension, such as the Venezuela Debt Crisis and Cold War. However, six of them resulted in war immediately following the rapid change in relative power. The remaining five cases did not show rapid power change, making them arguably poor candidates to analyze via the paradigm of Thucydides's Trap. This results in six out of eight cases of Thucydides's Trap analyzed ending in war.

It seems that the data analyzed here demonstrate that although not all of Allison's chosen cases present compelling evidence of Thucydides's Trap scenarios, his results are corroborated by those that do. The Trap seems to be, at most, a dangerous period, which may result in war, but other intervening factors can override this tendency, making the Trap quite far from 'inevitable'.

This is further evidenced by the fact that the two cases which present the most drastic power transitions, that of the shift between the U.S. and U.K. in the 19th century and the U.S. and USSR in the 20th, are the two exceptions which do not result in war. If the Thucydides's Trap was truly inevitable, these would be the cases most expected to result in war. In the U.S./USSR example, this shift is so dramatic that over the course of the Cold War it happens in drastic form, twice, with the USSR overtaking the U.S. just after WWII and the U.S. returning to overtake Russia after the collapse of the Soviet Union.

Summary of Results:

	War Occurred	No War Occurred
Rapid Change	United States/Japan, U.K., France, USSR/Germany (WWII), U.K., France, Russia/Germany (WWI), France/Prussia, France/U.K. (Rev.), Netherlands/England	US/USSR, U.K./U.S.
No Rapid Change	China, Russia/Japan, U.K., France/Russia, U.K./France	U.K., France/Germany, Portugal/Spain

Implications for the US-China Relationship

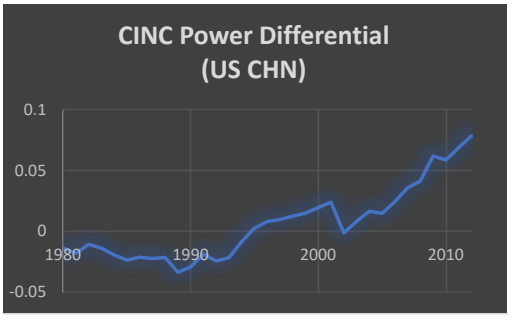


Figure 3: CINC Power Differential.[16]

In light of the historical findings here, it is worth discussing how any of this relates to the pressing question of the day: whether the United States and China are destined for a military confrontation. As shown above in the differential chart for the U.S. and China up until 2012, China already overtook the United States as measured by CINC metrics in 2002. Before performing the above analysis, this would, by a strict Thucydidean understanding, look like a foregone conclusion that the US and China would be barreling towards military confrontation. However, in the cases which most resemble this graph historically, in that it demonstrates a complete overtake by one power of another, those of the U.K. and U.S. and U.S. and USSR, peace prevailed over war.

There are some reasons for concern, however, which are not represented fully in these data. As potential explanation for these two cases of peace, scholars including Allison have posited the close cultural ties of the U.K. and U.S. in the 19th century and presence of mutually assured destruction during the Cold War.[17] Neither of these forces can be said to be fully present in the relationship between the U.S. and China in the 21st century. No amount of cultural exchange is likely to match the shared history the U.S. and U.K. experienced during the 19th century, and although China maintains a nuclear deterrent, it is orders of magnitude smaller than the one the Soviet Union employed. None of this requires that the U.S. and China will find themselves inevitably at war. Such arguments are hypotheses and somewhat unfalsifiable. Nevertheless, it is worth noting that although quantitatively, the data presented herein would contend that the U.S.- China relationship matches the most optimistic ones in history, there are also additional factors to consider which might temper that assessment.

Analyzing the Thucydides's Trap quantitatively has failed to find a compelling and unequivocal demonstration of an inevitable Trap, even when limited to cases in which rapid power change occurs. Although Allison's cases offer the beginnings of pushing power transition theory back further into the historical record, more research can be done to increase the number of available cases to examine, extending beyond the selected examples here or those included in other research. States have historically found ways out of the Trap without resorting to war, and although war does seem to be a highly likely possibility, it does not seem to be inevitable.

About the Author:

Austin Parenteau is a second-year student in Georgetown's Security Studies Program. He graduated magna cum laude from Georgetown's School of Foreign Service in 2019, where he majored in International Politics with a concentration in International Security. *He would like to thank both the Security Studies Program and the Bilden Scholarship for making this research possible.*

Endnotes

1. Graham Allison, *Destined for War: Can America and China Escape Thucydides's Trap?* Boston, MA: Houghton Mifflin Harcourt, 2017).
2. Ibid.
3. Jacek Kugler, "The Asian Ascent: Opportunity for Peace or Precondition for War?" *International Studies Perspectives* 7, no. 1 (2006), 36.
4. Woosang Kim, "Power Transitions and Great Power War from Westphalia to Waterloo," *World Politics* 45, no. 1 (1992), 161.
5. Graham Allison, "The Thucydides Trap: Are the U.S. and China Headed for War?" *The Atlantic*, September 24, 2015, https://www.theatlantic.com/international/archive/2015/09/united-states-china-war-thucydides-trap/406756/.
6. *Destined for War: Can America and China Escape Thucydides's Trap?,* 38-40.
7. Graham Allison, "Thucydides Trap Case File," *Belfer Center for Science and International Affairs*, accessed August 25, 2019, https://www.belfercenter.org/thucydides-trap/case-file.
8. David J. Singer, Stuart Bremer, and John Stuckey, "Capability Distribution, Uncertainty, and Major Power War, 1820-1965, Correlates of War- National Material Capabilities (v5.0)." *Bruce Russett (Ed) Peace, War, and Numbers* (Beverly Hills: Sage, 1972), 19–48.
9. Henk Houweling and Jan G. Siccama, "Power Transitions as a Cause of War," *The Journal of Conflict Resolution* 32, no. 1 (1988), 87.
10. Maddison Project Database, version 2018; Jutta Bolt, Robert Inklaar, Herman de Jong and Jan Luiten van Zanden (2018), "Rebasing 'Maddison': new income comparisons and the shape of long-run economic development," Maddison Project Working paper 10, https://www.rug.nl/ggdc/historicaldevelopment/maddison/research
11. "Thucydides Trap Case File."
12. Maddison Project Database, version 2018.
13. "Capability Distribution, Uncertainty, and Major Power War, 1820–1965. Correlates of War- National Material Capabilities (v5.0)."
14. Maddison Project Database, version 2018 and "Rebasing 'Maddison.'
15. "Capability Distribution, Uncertainty, and Major Power War, 1820–1965. Correlates of War- National Material Capabilities (v5.0)."
16. "Capability Distribution, Uncertainty, and Major Power War, 1820–1965. Correlates of War- National Material Capabilities (v5.0)."
17. "Thucydides Trap Case File."

American Signal Failures in Venezuela: The Challenge of Credible Bargaining in Crisis

Felipe Herrera

Since the Venezuelan National Assembly's invocation of Article 233 setting off a constitutional crisis pitting Nicolás Maduro and his supporters against Juan Guaidó and his opposition coalition, very little progress has been made toward a resolution. Despite the broad international support in the early months of Guaidó's de jure presidency, the United States has not been able to mobilize a unified response to achieve its objectives in Venezuela, and most countries have instead imposed their own myriad of sanctions policies without serious multilateral cooperation. As the crisis stretches on with no end in sight, Guaidó risks a gradual erosion of his international legitimacy as his European allies grow weary of the protracted diplomatic stalemate. Guaidó's opposition movement has lost the momentum it had gained at the start of 2019, and the failure to favorably resolve the crisis thus far can be attributed to the inability of the United States to clearly define its strategy and signal its intents. The general confusion and questions surrounding America's intent to either use force or simply continue imposing sanctions impeded diplomatic progress, and conversely allowed Maduro to shore up support within his military and prevent defections through the rhetoric of anti-imperialism. Additionally, three of Maduro's most involved international allies—Cuba, Russia, and China—were not seriously taken into account as necessary partners in any sort of negotiated settlement. Rather, the United States maintained aggressive policies against these three countries that further obstructed a successful resolution to the Venezuelan crisis. This essay deploys game theory to demonstrate how the United States was on track to achieve strategic success with its course of action to continue implementing targeted sanctions, but the invasion-signaling rhetoric within the Trump Administration constituted a major failure in signaling due to its discouragement of the Venezuelan military from defecting to Guaidó. This, coupled with the exclusion of necessary partners, pushed attainment of U.S. policy objectives out of reach.

Introduction and Background

On 10 January, 2019, the Venezuelan National Assembly invoked Article 233 of the Constitution, declaring that President Maduro had effectively abandoned his position and arguing that "de facto dictatorship" meant there was no democratic leader.[1] Soon thereafter, the United States recognized Juan Guaidó as the de jure president of Venezuela,[2] and the list of states recognizing Guaidó has grown to include over 50 others.[3] Threats of invasion abounded, generally muddying the waters of diplomacy as most nations rejected the prospect of a military operation to resolve the crisis. The United States failed to clearly define its strategy and was addled by an incoherent and ineffective approach, and a game theoretic analysis of the crisis illuminates the pitfalls of threatening the military option. However, this approach is limited in its scope, and the role of third party actors cannot be understated in examining how the Venezuelan constitutional crisis has played out. Maduro's most involved partners—China, Russia, and Cuba—were crucial to resolving this crisis, yet U.S. policies precluded these countries from the negotiating table, limiting the multilateral approach needed for a successful resolution.

Despite threatening notepads implying that the United States was sending 5,000 troops to Colombia to prepare for a military operation[4] and heavy-handed rhetoric claiming, "Maduro's days are numbered,"[5] Secretary of State Mike

Pompeo continued to reiterate his "[confidence] that the Venezuelan people" will resolve the crisis themselves. In February 2019, Peru's Assistant Foreign Minister ruled out the use of force as "unacceptable . . . [and] not a solution for what's happening in Venezuela," before a meeting of the Lima Group in Colombia.[6] More recently at the United Nations General Assembly, the United States and 16 Latin American countries met to sign the Rio Treaty, a Cold War-era mutual defense agreement last invoked following the September 11th attacks.[7] This action demonstrates a general acknowledgement among the states party to the treaty that the Venezuelan crisis constitutes a regional security concern requiring broad defense cooperation. Because the United States specifically refused to include language precluding intervention, European governments remain concerned that the invocation of the Rio Treaty could unnecessarily entice Venezuela's regional neighbors to consider military action with U.S. approval.[8]

The signing of the Rio Treaty comes at a time when support for the Venezuelan opposition coalition under Guaidó appears to be faltering. On September 16, Maduro signed a deal with smaller opposition parties unaligned with Guaidó in the Venezuelan National Assembly to retake 55 congressional seats, reform the electoral council, and release some political prisoners.[9] The National Assembly has been the source of Guaidó's international legitimacy since the invocation of Article 233, however, this new deal fractures the opposition and gives the majority back to Maduro's ruling party. Additionally, as Venezuela-based and opposition-controlled Citgo Petroleum Corporation threatens to default on a $900 million dollar bond, lawmakers fear the company will be seized by Russian state-run oil company Rosneft and other financial backers of Maduro. All of this follows on the heels of Maduro's quiet loosening of market restrictions in Venezuela, which have moderately tempered the country's economic crisis over the past several months. By scaling back the frenzied printing of money, temporarily halting the policy of frequent salary hikes, and dropping enforcement of price controls, inflation has decreased from a peak of 2.6 million percent in January to 135,000% in August.[10] The refugee crisis has also provided an economic boost for Maduro, as remittances annually totaling $4 billion are sent to Venezuela in hard dollars.[11]

It is no wonder, then, that the Venezuelan opposition aligned with Guaidó has been left highly dissatisfied by U.S. and regional efforts at reconciliation since January 2019. Despite continued waves of sanctions by the U.S. Treasury Department—most recently in August 2019[12]—in addition to increased regional cooperation on law enforcement operations to track down and freeze sources of income for Maduro insiders,[13] Guaidó's European allies have become frustrated with the protracted diplomatic stalemate.[14] A fresh wave of elections, as part of Maduro's deal with the smaller opposition parties, may be more palatable to them than continued limbo and we should expect to see a major erosion of Guaidó's legitimacy among European nations should Maduro proceed with the deal and announce elections.[15] The potential loss of control over Citgo and the corporation's transference to Russian financiers of Maduro would represent another nail in the coffin for a resolution to the Venezuelan crisis on America's terms.

Beyond the coalition supporting Guaidó, Cuba, China, and Russia remain highly involved players, especially since the Trump Administration has repeatedly accused them of propping up President Maduro.[16] With an estimated 20,000 Cuban troops contributing security and intelligence assistance in Venezuela, Cuba is the most invested external actor, seeking to preserve its access to cheap oil to prevent serious shocks to its own economy[17] in addition to maintaining its ideological commitment to its longtime socialist partner. The fuel shortage in Cuba threatens to destabilize its already fragile economy, which has suffered

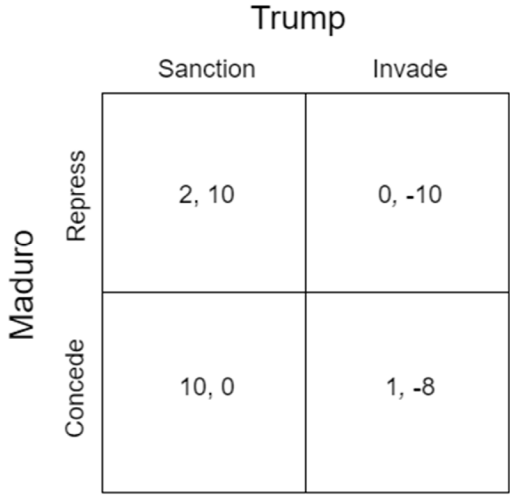
from American sanctions levied over the country's support for Maduro.[18]

China and Russia are highly motivated by their share of investments in Venezuela, with China having invested over $50 billion since 2007[19] and Russia holding over half of Citgo as collateral for various loans.[20] Russia's interests, however, extend beyond economic concerns alone, and Putin cites the Libyan and Syrian intervention cases to justify fears that "if it does nothing, America will use military power to topple a Moscow-friendly regime."[21] There is also a sense of geopolitical "retribution" from Putin's perspective, who considers "inserting himself in Washington's backyard [as] payback for U.S. meddling near Russia's borders."[22] Understanding the motivations of Maduro's biggest partners was a crucial, yet explicitly disregarded, facet in reaching a successful multilateral resolution to the crisis.

Modeling the Crisis

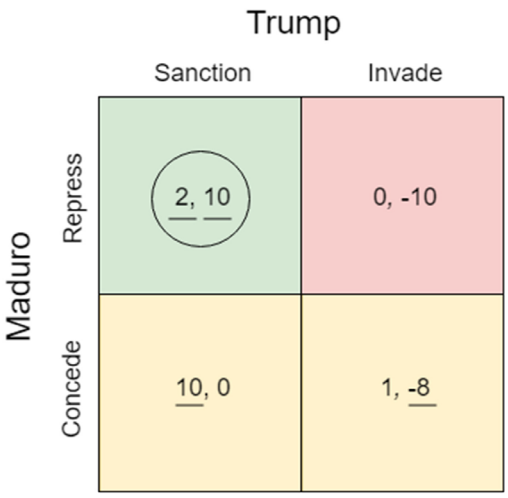
In the early stages of the constitutional crisis, a broad consensus was reached by most countries who threw their support behind Guaidó to specifically denounce the option of military intervention. These countries signaled their intent to provide humanitarian aid to nations receiving Venezuelan migrants and collaborate on sanctions policies against Maduro.[23] But in February 2019, U.S. Vice President Pence continued to reassure Guaidó's coalition that force remained an option for the United States,[24] and the U.S. has since continued to occasionally broach the option, however seriously it is actually being considered. These actions on the part of the United States have constituted a major signal failure, serving as serious barriers to credible bargaining according to game theory.

The study of game theory in international relations, pioneered by Thomas Schelling and his theories on bargaining and strategic behavior, maintains that violent conflict is a result of bargaining failure due to asymmetric or incomplete information and unsuccessful signaling that fails to establish credible commitments.[25] According to Schelling, the objective is not to defeat your opponent in every interaction but to seize all possible opportunities to cooperate, or risk violence.[26] This cooperation is made possible by effective bargaining, done through costly signaling that clearly expresses intent, capabilities, and outcome preferences. The continuous-action space is the total range of outcomes in an interaction, and the bargaining space is the overlap between the preferences of both actors involved. Only in "pure conflict . . . [such as] wars of complete extermination" is there no overlap where a satisfactory bargain can be made.[27]



The 2x2 model assumes that suffering an invasion is the worst possible outcome for Maduro, earning a payoff of -10, presupposing that an invasion would play out like the NATO intervention in Libya. Maduro can continue coping with sanctions with the aid of Cuba, Russia, and China, and maintaining power would earn a payoff of 10. The model additionally assumes that an invasion under any circumstances would be successful in deposing Maduro while destabilizing the region, thus earning only a minimal payoff for President Trump of 0, should Maduro continue repressing, or 1, should Maduro concede. Sanctions that fail still earn at least a slight payoff of 2, as taking any action at all

is deemed politically sufficient for Trump in Florida polls,[28] but successful sanctions earn the full payoff (10) of resolving the crisis. Payoffs in the model above are presented as Trump, Maduro—i.e. the Sanction-Repress quadrant yields a 2 for Trump and a 10 for Maduro. Solving for the Nash equilibrium (highlighted in green), we find that the game is strongly disposed towards the status quo, Trump-Sanction/Maduro-Repress, and this is precisely how the crisis has played itself out since Guaidó's announcement in January.



This 2x2 model, however, assumes complete and perfect information. A split decision tree shown on the following page takes into account the odds that Maduro's military leaders defect and oust him, as Guaidó hoped would happen:

The initial 2x2 model is reflected on the left side of this decision tree and represents the situation given that Venezuela's military remains loyal to Maduro (with a probability of p, i.e. the unknown percent chance of loyalty). The dotted lines separating the two halves of the model illustrate decision-making under uncertainty, as neither Trump nor Maduro can be absolutely certain whether Venezuelan military leaders will defect at the start of the game. Assuming the Venezuelan military defects (with a probability of $1-p$, i.e. the unknown percent chance of defection), the payoffs for Maduro are highly negative regardless of his decisions in the game, although an early concession in this situation would avoid retribution for continuing to repress. Solving for the subgame-perfect Nash equilibria through backwards induction from each outcome, we again find that the situation is status quo oriented for the United States, favoring sanctions over an invasion, while Maduro's decision-making is entirely determined by the loyalty of his military.

Although these models are limited in their explanatory and prescriptive utility by their nature as one-off games, we can apply the same concepts across time and draw a key takeaway. Using sanctions in a vacuum (as in the model) the United States can have no way of deducing their true impact without prior knowledge of the Venezuelan military's loyalty to Maduro. Put another away, at the start of this one-off game, the subgame-perfect Nash equilibria of the model indicate that the U.S. will always use sanctions, regardless of any other conditions in the game. But within the context of the actual situation across time, where this game is infinitely repeated, U.S. sanctions can be effective if their intended purpose is to shift the probability (p) that the Venezuelan military defects, conceptualized by applying a discount factor ($0 < \delta < 1$) to the probability of loyalty vs. defection. As such, the best strategy for the Trump Administration, as deduced by the inferences made from the model, is to continue implementing highly targeted sanctions with a clear focus on shifting loyalties within the military away from Maduro. In this sense, success cannot be determined solely by outcomes immediately following the implementation of sanctions, but rather by expanding the time horizon to account for the loyalty-altering effects of targeted sanctions.

For Maduro, however, the main point of emphasis in this model is that implementing sanctions is the equilibrium strategy profile for the United States. With this information, signals expressing an intent to invade lose their ability to effectively

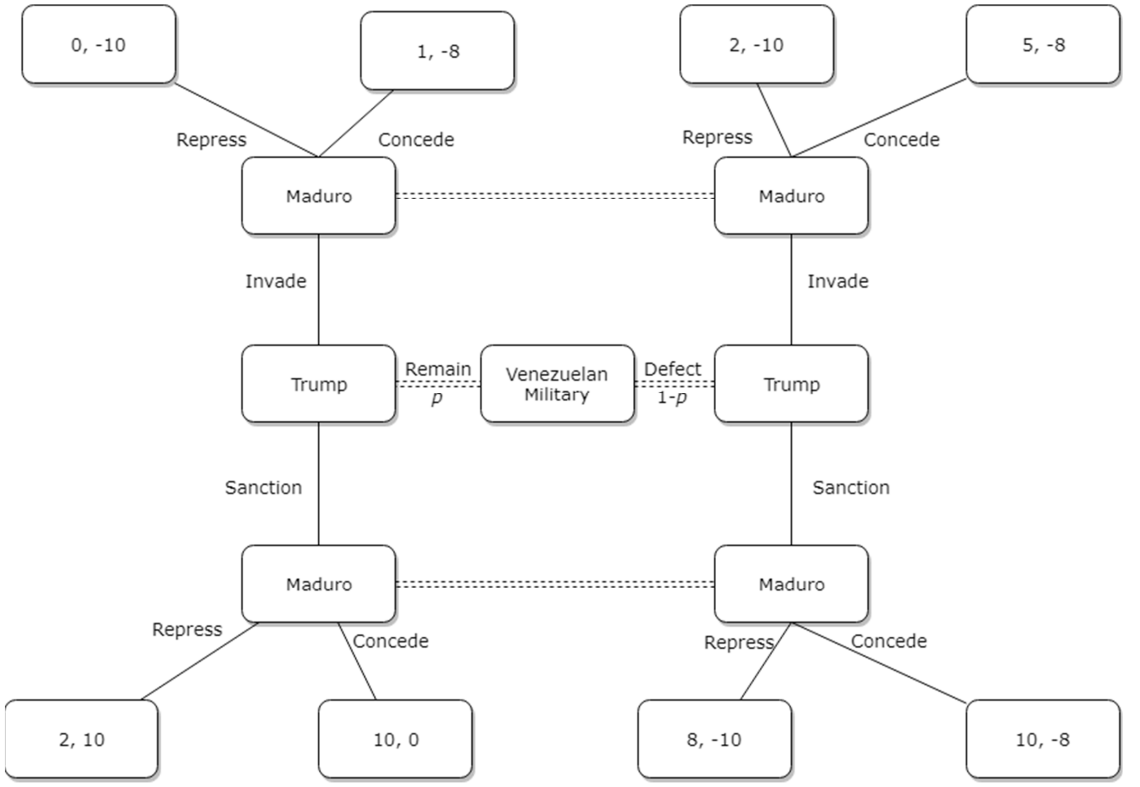


Figure 1

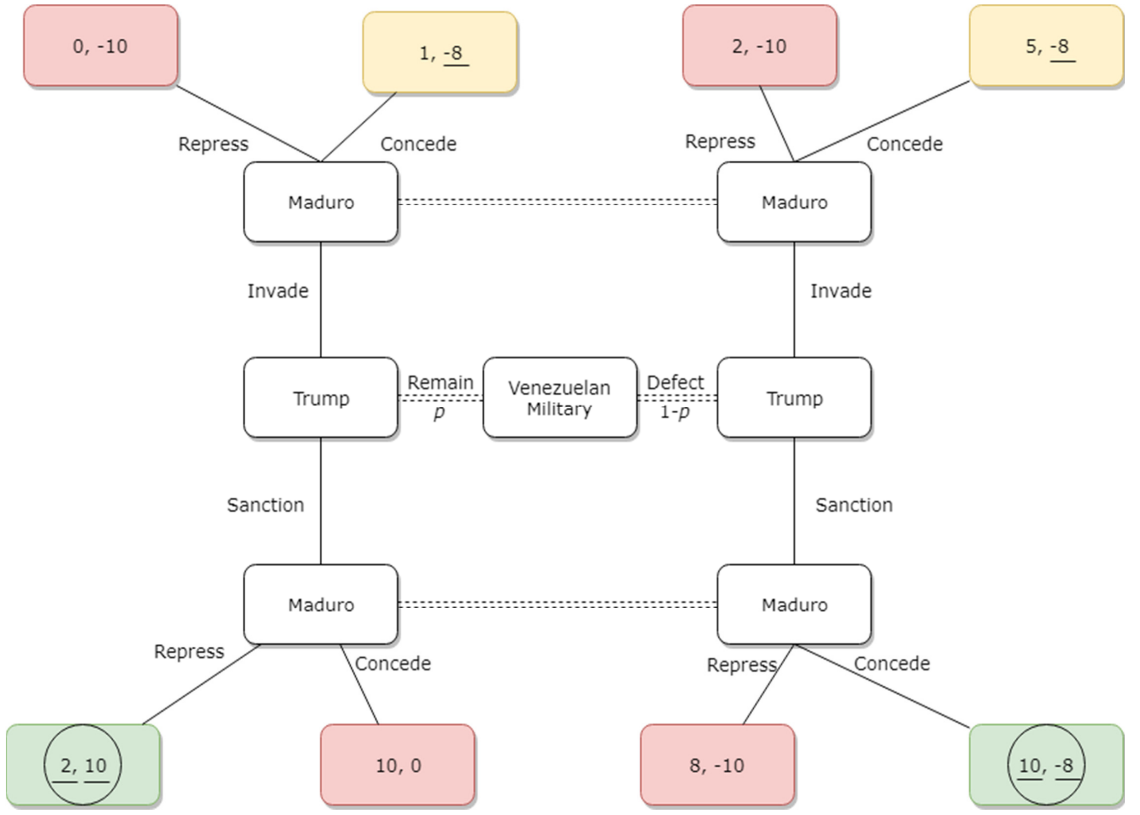


Figure 2

apply pressure to concede and actually have an inverse effect. In fact, Maduro can weaponize this rhetoric to generate a rally-around-the-flag effect within the Venezuelan military to shore up support. Thus, again applying this one-off game across a broader time horizon, threats of military intervention negate the loyalty-diminishing effects of targeted sanctions and allow Maduro to increase the probability (p) that his military leaders remain loyal with a positive discount factor ($\delta > 1$). Continuing to assume, as the model recommends he should, that the United States will only implement sanctions, Maduro can choose to repress to retain power as his dominant strategy profile for the foreseeable future.

The Hawk-Dove Game

Returning to the 2x2 model, the Venezuelan crisis to date has exemplified the hawk-dove game, also known as 'chicken,' a classic 2x2 game. Both actors aim to force the other to yield to them while trying to avoid the worst outcome, like two cars driving from opposite directions on a single lane, refusing to back down, but hoping to avoid a collision. A military intervention would be the worst outcome for both the United States and Venezuela; in terms of loss of life for Venezuela and public perception and influence costs for the U.S., assuming the intervention goes the route of the Iraqi, Libyan, or Syrian cases. Avoiding this outcome requires one actor to yield to the other, while both sides signal their resolve to keep going and risk a collision.

In this regard, Maduro has more credibility in posturing as risk-prone given that the nature of the crisis is both personal and existential when one considers the domestic hypersensitivity of authoritarians to both material and perceived losses. Seemingly counterintuitively, dictators can be acutely sensitive and accountable to constituencies, though not popular audiences. Unlike in democracies, the cost of deposition is not a career change but very often exile or execution.[29] In the case of Venezuela, the constituency that President Maduro is held accountable to is the military and decisions resulting in his deposition are considered existential, whereas the interaction is not nearly as critical for President Trump.

Returning to the metaphor of two drivers on a single lane, the relatively low personal stakes for Trump compared to Maduro means that failure to yield is not necessarily perceived as a head-on collision in a game of 'chicken' given that escalation to the use of force would merely draw condemnation from the international community, but would not constitute an existential disaster for President Trump. This gives President Trump a level of flexibility in his decision-making to explore different policy options without a serious level of commitment. This flexibility carries its own negative consequences, which are further worsened by the fact that the costs of signaling can collapse in an era when a single tweet can decide the course of policy. The study of game theory has established that bargaining requires costly signals because they establish commitments, demonstrate capabilities, and express intents. The inability or unwillingness to credibly commit and the mixed signals sent by the United States created the perception that there was no cogent strategy undergirding the policy options Trump explored, preventing successful bargaining.

Iterations of the Game

The first iteration of the hawk-dove game involved Maduro's decision to order American diplomats to leave the country after the United States recognized Guaidó, after which the U.S. refused to evacuate nonessential diplomatic staff in the embassy in Caracas. As the deadline set by Maduro passed, the United States effectively called his bluff while misunderstanding his strategy. At this point, all Maduro needed to do to maintain power was sit and wait for the crisis to pass; acting brazenly would needlessly provoke his military loyalists to reconsider their position.

Learning from this, the Venezuelan opposition and its international allies hoped forcing humanitarian aid into the country on February 23 would trigger the collapse of his regime,[30] inducing a second iteration of the hawk-dove game. Although Maduro's violent response to this aid drew about 160 rank-and-file military desertions,[31] his military leaders remained loyal because the United States' rhetoric has given Maduro the best get-out-of-jail-free card he could have hoped for: a narrative of regime change under the guise of humanitarian aid.

The third iteration of this game happened on April 30, when Guaidó announced an uprising to seize power, and military deserters attempted to take over La Carlota Air Base but were frustrated by pro-Maduro forces.[32] While it appeared Maduro was preparing to flee the country once the coup was underway, Secretary of State Mike Pompeo alleges that Russian forces ultimately convinced Maduro to stay.[33] Although this situation again encapsulates the basic elements of a hawk-dove game, requiring a decision to yield or not yield, the coup attempt demonstrates that these models are insufficient to capture the dynamics influencing the entire situation. The external actors involved play an outsized role in the Venezuelan crisis through their ideological, economic, and geopolitical motivations. The factors that incentivize them to act should have been accounted for by the Trump Administration as soon as it became clear how involved the countries would be, and an analysis of their motivations is necessary to understand why the Venezuelan crisis has not yet been resolved.

External Considerations

As Maduro's most hands-on partner, Cuba's ideological motivations cannot be disregarded. Cuba cannot concede that a fellow socialist regime is failing, and this image must be protected or Cuba will become alienated as a potential facilitator in negotiations.[34] However, given the country's fears of a return to the dire economic conditions of the "Special Period" following the collapse of the Soviet Union, these considerations may soon fall by the wayside as gas shortages worsen considerably under American sanctions.[35] But, the crumbling of the ideological façade has been well underway for some time now; Cuba ratified a new constitution in February 2019, officially authorizing foreign investment, free enterprise, and private property.[36] Maduro's quiet market reforms to resuscitate the Venezuelan economy further convey that the partnership between these countries may extend beyond historical ideological commitments, as Cuba and Venezuela are collaborating on implementing marginal reforms gradually to salvage their economies.

These concurrent shifts in economic policy demonstrate that Trump's sanctions have potentially had the inverse of their intended effect. Rather than dislocating the Bolivarian alliance, the two countries are approaching their economic crises bilaterally, despite prior ideological bonds. Following the failed coup attempt in April 2019, Cuba expressed a willingness to help negotiate a peaceful end to Venezuela's political crisis,[37] but continued U.S. sanctions against Cuba and Venezuela have driven both countries to seek relief elsewhere, most recently with the case of Indian refining corporation Reliance Industries Ltd resuming shipments of crude oil.[38] The willingness to negotiate a settlement was dismissed by the U.S. and the Bolivarian alliance has consequently moved on.

Russia has no historically ideological ties to the Maduro government like Cuba does. Its motivations are likely more geopolitical in nature, as Putin tries to keep a Moscow-friendly and anti-U.S. regime afloat in the Western Hemisphere. Russia has been "utterly preoccupied" with America's use of force to drive "favorable regime changes around the world," and fears that Russia would eventually be on the target list.[39] Putin's opposition to regime change in Venezuela can thus be understood in the

context of his fears of the "unacceptable precedent such change might set for Russia itself and for other states closer to home in Eurasia."[40]

Conversely, Russia has stronger economic ties to Colombia and Brazil than it does to Venezuela, two countries that have recognized Juan Guaidó's presidency, and the low likelihood that Russia would put those relationships at risk over Maduro has driven an increasing divide between Russia's economic and political elite.[41] Still, Secretary of State Pompeo's discussions with Russian Foreign Minister Sergey Lavrov have thus far failed to effectively stress these economic factors and highlight how Russia's economic position in the region would actually benefit from greater stability in Venezuela. Rather, Citgo's $900 million default will present Russian creditors with leverage to provide debt relief to Venezuela, and cooperation between Russia and Maduro will continue unabated.

In the same vein, China's primary concern is inherently economic when it comes to Venezuela as it has invested over $50 billion in around 800 projects,[42] but the country has thus far not expressed a serious inclination to step in to secure Maduro's regime. Unlike Russia and Cuba, China has tread carefully in dealing with the Venezuelan crisis while "signaling that it would work with any government in developing a long-term cooperation strategy."[43] After a negotiated transition, China could play a large role in supporting a "multilateral-led macroeconomic stabilization program" that would include a significant debt restructuring.[44] Guaidó's representative to the Inter-American Bank, Ricardo Hausmann, has long suggested that China will be an essential partner in the "reconstruction" of Venezuela after a transition, highlighting the "enormous opportunities" of China-Venezuela engagement once the country is stabilized.[45] A post-Maduro government that remains friendly to China would be an important draw in getting China to the table to aid in negotiations. Unfortunately, the U.S.-China trade war hindered any sort of cooperation on Venezuela.

Conclusions

The head of the U.S. section at Cuba's Foreign Ministry Carlos Fernandez de Cossio has stated that there can be no negotiations without the participation of Nicolás Maduro.[46] Such participation would require a strong and coherent U.S. foreign policy, with a clear focus on intended outcomes. Continued threats of military invasion from both public statements and the Twitter accounts of President Trump, Former National Security Advisor John Bolton, and Senator Marco Rubio have had the unintended effect of generating a rally-around-the-flag effect within the Venezuelan military, as we have seen with Maduro's weaponization of anti-imperialist rhetoric.

Understanding the crisis and the actions of the Trump Administration through the lens of game theory, this strategy is not without merit, as it is necessary to convince the other player in a hawk-dove game that you fully intend to carry out your threat. The issue in this case, however, is the seeming incoherence of the U.S. strategy, where some policymakers deny the intent to intervene while others promote it zealously. This incoherence impeded progress because it was impossible for other actors to comprehend America's signaling, a necessary component of successful bargaining in game theory.

Although time and again the United States' allies in Latin America and beyond have denounced the military option, continued hostile rhetoric within the U.S. has undermined meaningful diplomacy. Following the regional consensus and delimiting America's strategy to seek a negotiated settlement that included the external actors most involved in the Venezuelan crisis would have clearly signaled American intents and demands, while removing a key factor weaponized by Maduro to maintain support with his military leaders. For credible bargaining, the

rhetorical focus within the United States should have been on highly targeted sanctions that would have increased the probability that the Venezuelan military defects, as noted in the split decision tree model, while also broadening the time horizon to accept that the purpose of the sanctions is not an immediate end to the crisis, but a gradual erosion of loyalty to Maduro. While a US-led military intervention would almost certainly succeed in deposing President Maduro, the United States should learn from its tumultuous history of regime change and seek to effectively seize all opportunities for cooperation with this as a clear strategic intention.

About the Author:
Felipe Herrera is an M.A. candidate in the Walsh School of Foreign Service's Security Studies program at Georgetown University. He received his B.A. in International Studies from American University's School of International Service in 2018, and he currently works at Human Rights Watch as an administrative assistant. He can be reached at (786) 333-3415 or at fh276@georgetown.edu.

Endnotes

1. "Venezuela: President of the National Assembly Cites Constitutional Basis for Assuming Office the Presidency on an Interim Basis," *Foreign News*, Library of Congress, January 31, 2019. http://www.loc.gov/law/foreign-news/article/venezuela-president-of-the-national-assembly-cites-constitutional-basis-for-assuming-office-the-presidency-on-an-interim-basis/
2. "Recognition of Juan Guaido as Venezuela's Interim President," Press Statement, *United States Department of State*, January 23, 2019. https://www.state.gov/secretary/remarks/2019/01/288542.htm
3. "The Latest: Pompeo urges Venezuelan troops to let aid in," *Miami Herald*, February 23, 2019. https://www.miamiherald.com/latest-news/article226677224.html
4. Eli Rosenberg and Dan Lamothe, "'5,000 troops': Photo of John Bolton's notes raises questions about U.S. military role in Venezuela crisis," Politics, *The Washington Post*, January 28, 2019. https://www.washingtonpost.com/politics/2019/01/29/troops-photo-john-boltons-notes-raise-questions-about-military-role-venezuela-crisis/?utm_term=.b0e34cb733a3
5. "Venezuela crisis: President Maduro's 'days numbered'—Mike Pompeo," *BBC*, February 24, 2019. https://www.bbc.com/news/world-latin-america-47348293
6. Jim Wyss, "Lima Group member rules out military force against Venezuela," *Miami Herald*, February 25, 2019. https://www.miamiherald.com/news/nation-world/world/americas/venezuela/article226745184.html?fbclid=IwAR1JXYwTGHrl4eobDVI4CAQPYQhOCNbHgkUiyFYAVHxrH-blyrK7tetVsI8
7. Claudia Torrens, "US Allies Invoke Treaty to Pressure Venezuela's Maduro," *Associated Press*, September 24, 2019. https://www.apnews.com/5c331bbf8b954b0392aa997b1d973b0d.
8. Courtney McBride, "'Rio Treaty' Nations to Cooperate on Sanctions on Venezuela's Maduro," *Wall Street Journal*, September 24, 2019, sec. World. https://www.wsj.com/articles/rio-treaty-nations-to-cooperate-on-sanctions-on-venezuelas-maduro-11569286176.
9. Anatoly Kurmanaev and Ana Vanessa Herrero, "Venezuela's Maduro Trains Sights on Opposition's Last Bastion: Congress," *The New York Times*, September 16, 2019, sec. World. https://www.nytimes.com/2019/09/16/world/americas/venezuela-maduro-congress.html.
10. Kejal Vyas, "Venezuela Quietly Loosens Grip on Market, Tempering Economic Crisis," *Wall Street Journal*, September 17, 2019, sec. World. https://www.wsj.com/articles/venezuela-quietly-loosens-grip-on-market-tempering-economic-crisis-11568718002.
11. Ibid.
12. "Venezuela-Related Sanctions." Accessed October 16, 2019. https://www.treasury.gov/resource-center/sanctions/programs/pages/venezuela.aspx.
13. Courtney McBride, "'Rio Treaty' Nations to Cooperate on Sanctions on Venezuela's Maduro," *Wall Street Journal*, September 24, 2019, sec. World.
14. Anatoly Kurmanaev and Ana Vanessa Herrero, "Venezuela's Maduro Trains Sights on Opposition's Last Bastion: Congress," *The New York Times*, September 16, 2019, sec. World.
15. Ibid.
16. Anne Gearan and Karen DeYoung, "Trump Threatens 'Complete Embargo' and 'Highest-Level Sanctions' against Cuba over Venezuela," *The Washington Post*, 30 Apr. 2019, www.washingtonpost.com/politics/bolton-reiterates-all-options-open-to-trump-in-venezuela-warns-russia-against-meddling/2019/04/30/6851a09e-6b79-11e9-be3a-33217240a539_story.html?noredirect=on&utm_term=.4fc869c93946.
17. Adam Taylor, "How Many Cuban Troops Are There in Venezuela? The U.S. Says over 20,000. Cuba Says Zero." *The Washington Post*, 2 May 2019, www.washingtonpost.com/world/2019/05/02/how-many-cuban-troops-are-there-venezuela-us-says-over-cuba-says-zero/?noredirect=on&utm_term=.802db0a56dcd.
18. "Cuba's Acute Fuel Shortage Begins to Bite," *Reuters*, September 13, 2019. https://www.reuters.com/article/us-cuba-economy-idUSKCN1VY2F7.
19. Angus Berwick, "Special Report—How a Chinese Venture in Venezuela Made Millions While Locals Grew Hungry," *Reuters*, 7 May 2019, uk.reuters.com/article/uk-venezuela-china-food-specialreport/special-report-how-a-chinese-venture-in-venezuela-made-millions-while-locals-grew-hungry-idUKKCN1SD1CW.

20. Emily Tamkin, "Why Is Russia Clashing with the United States over Venezuela?" *The Washington Post*, 1 May 2019, www.washingtonpost.com/world/2019/05/01/why-is-russia-clashing-with-united-states-over-venezuela/?utm_term=.458ec9e8b45c.
21. Ibid.
22. Ibid.
23. Rafael Bernal, "Trump amps up pressure on Venezuela with fresh aid, sanctions," *The Hill*, February 25, 2019. https://thehill.com/latino/431442-trump-amps-up-pressure-on-venezuela-with-fresh-aid-sanctions
24. Karen DeYoung, Anne Gearan, and Anthony Faiola, "On ousting Maduro, only Venezuela's opposition appears to favor a bolder approach," *The Washington Post*, February 25, 2019. https://www.washingtonpost.com/world/national-security/on-ousting-maduro-only-venezuelas-opposition-appears-to-favor-a-bolder-approach/2019/02/25/a7f975a2-393b-11e9-a2cd-307b06d0257b_story.html?utm_term=.fd32ece8e741
25. Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, Massachusetts: Harvard University Press, 1960).
26. Ibid.
27. Ibid.
28. Marc Caputo, "Trump Venezuela Policy Scores in Florida," *POLITICO*, https://www.politico.com/story/2019/01/30/trump-venezuela-florida-policy-1138307.
29. Jessica L. Weeks, "Strongmen and Straw Men: Authoritarian Regimes and the Initiation of International Conflict," *The American Political Science Review*, 106, no. 2 (May 2012), 326–347.
30. Amy B. Wang, "How the Venezuela crisis is unfolding, in images," *The Washington Post*, February 23, 2019, https://www.washingtonpost.com/world/2019/02/23/how-crisis-venezuela-is-unfolding-images/?utm_term=.5add2358d93a
31. Karen DeYoung, Anne Gearan, and Anthony Faiola, "On ousting Maduro, only Venezuela's opposition appears to favor a bolder approach," *The Washington Post*, February 25, 2019.
32. Euan McKirdy, "Venezuela's Maduro Claims to Have Defeated 'Coup,' as Rival Guaido Urges More Protests," *CNN*, 1 May 2019, www.cnn.com/2019/05/01/americas/venezuela-guaido-maduro-intl/index.html.
33. Adam Taylor, "How Many Cuban Troops Are There in Venezuela? The U.S. Says over 20,000. Cuba Says Zero," *The Washington Post*, 2 May 2019.
34. Francisco Monaldi, "China Can Help Save Venezuela. Here's How," *Americas Quarterly*, 23 Apr. 2019, www.americasquarterly.org/content/how-china-can-play-constructive-role-venezuela.
35. Carrie Kahn, "Cubans Increasingly Anxious About Gas Shortages Under Trump Sanctions Against Venezuela," *NPR*, 5 May 2019, www.npr.org/2019/05/05/720376155/cubans-increasingly-anxious-about-gas-shortages-under-trump-sanctions-against-ve.
36. "Cubans Overwhelmingly Ratify New Socialist Constitution," *Reuters*, February 25, 2019. https://www.reuters.com/article/us-cuba-constitution-referendum-idUSKCN1QE22Y.
37. Stephen Wicary and Jose Enrique Arrioja, "Cuba Says Maduro Must Be at Negotiating Table to Fix Venezuela," *Bloomberg*, 6 May 2019, www.bloomberg.com/news/articles/2019-05-06/cuba-says-maduro-must-be-at-negotiating-table-to-fix-venezuela.
38. "India's Reliance to Resume Venezuela Oil Loadings after Four-Month Pause." *Reuters*, October 9, 2019. https://www.reuters.com/article/us-oil-pdvsa-reliance-exclusive-idUSKBN1WO24L.
39. Emily Tamkin, "Why Is Russia Clashing with the United States over Venezuela?" *The Washington Post*, 1 May 2019, www.washingtonpost.com/world/2019/05/01/why-is-russia-clashing-with-united-states-over-venezuela/?utm_term=.458ec9e8b45c.
40. Ibid.
41. Kenneth Rapoza, "What Russia Stands To Lose In Venezuela," *Forbes Magazine*, 6 May 2019, www.forbes.com/sites/kenrapoza/2019/05/06/what-russia-stands-to-lose-in-venezuela/#77e571676579.
42. Angus Berwick, "Special Report—How a Chinese Venture in Venezuela Made Millions While Locals Grew Hungry," *Reuters*, 7 May 2019.

43. Francisco Monaldi, "China Can Help Save Venezuela. Here's How," *Americas Quarterly*, 23 Apr. 2019, www.americasquarterly.org/content/how-china-can-play-constructive-role-venezuela.
44. Ibid.
45. Josephine Ma, "China 'Could Play Big Role in Venezuela's Reconstruction'." *South China Morning Post*, South China Morning Post, 1 Apr. 2019, www.scmp.com/news/china/diplomacy/article/3003399/china-could-play-big-role-venezuelas-reconstruction-iadb.
46. Stephen Wicary and Jose Enrique Arrioja, "Cuba Says Maduro Must Be at Negotiating Table to Fix Venezuela," *Bloomberg*, 6 May 2019.

Applying Institutional Wisdom from Economic Traditions to Defense Institution Building

Casey Wetherbee

In recent years, policymakers have emphasized the importance of structural reforms in achieving development and security goals, especially in countries with relatively weak institutions. For example, the United States government has openly acknowledged the need for governance reform and institutional change on both local and national levels in its approach to fragile states, recently demonstrated by the Global Fragility and Violence Reduction Act of 2018 (H.R. 5723) and the Stabilization Assistance Review (SAR). This new focus seems to exist within the more scholarly branch of the defense and security communities, and there has not been enough time for it to meaningfully translate into policy implementation. Meanwhile, since the late 1980s the role of governance institutions in promoting growth has been central to the fields of development economics, most notably in the policies of the World Bank, and the new institutional economics (NIE) school of economic thought. Throughout this paper, I seek to connect political economy theory to the defense and security sectors by providing an analytical framework based primarily in World Bank doctrine and academic literature from the NIE school and applying it to the defense and security sectors. I argue that policymakers should increasingly emphasize the importance of building institutions that lower transaction costs, signal credible commitments, and heighten transparency and accountability in order to reform the incentive structures that allow for corruption, bureaucratic inefficiency, and cycles of violence in fragile states.

Introduction

In 1989, a turning point in the development community came when the World Bank released a Long Term Perspective Study, entitled "From Crisis to Sustainable Growth," which detailed a "crisis of governance" that plagued sub-Saharan Africa.[1] While international aid was pouring into building infrastructure and facilitating public sector management reform in the region, conditions only seemed to be getting worse. The World Bank's diagnosis of the root cause of this dilemma—that throwing money at a problem would not solve it without insistence on accountability and assurance that those funds would be properly used—led it to issue a memorandum to provide a legal framework by which it could address political stability.[2] The inextricable link between governance and economic security, however, could not be ignored, which has impacted the course of development research and policy to the present day. As scholars of defense and security studies begin to evaluate the importance of institutional transformation in achieving policy objectives, they can draw upon decades of institutional economic theory as a useful framework for analysis.[3]

At the same time, the field of new institutional economics (NIE) began to gain traction within the academic community. Economists in this tradition noticed that the free market often did not produce rational outcomes due to systematic flaws and defined institutions broadly as the solutions to those problems. As the "rules of the game," institutions were theorized to consist of laws, customs, norms, and other constraints both formal and informal that limited interactions in a society.[4] NIE traditionally deals with markets and firm structures, and how institutions can facilitate efficient exchanges by reducing

transaction and information costs. Despite its purely economic origins, the role of institutions in combating structural inefficiencies has important implications for the defense and security sectors.

Definition of Institution

The concept of an "institution" is one that varies across fields and professions and can be interpreted broadly, but for the purposes of this paper it will refer to the definition presented previously; this definition of institutions as laws, norms, and other types of constraints allows one to move beyond the economic realm by removing the explicit mention of market function that is present in much of the institutional economic literature.[5] Indeed, many political economists and economic historians in the NIE school of thought have addressed the diversity of types of institutions as they extend to the political and legal spheres, upon many of which this paper will expand in the subsequent discussion of institutions.[6] Furthermore, some practitioners of other social sciences—including anthropologists, sociologists, and even evolutionary biologists—have incorporated elements of institutional theory into their varying perspectives.[7]

Since the definition and interpretation of what an institution is and does is so broad, it is a helpful exercise to determine what an institution is *not*. Many individuals unfamiliar with institutional theory may mistake "institutions" for "organizations," which is akin to mistaking the "rules" for the "players."[8] Continuing with this analogy, organizations have priorities and seek to "win" by operating within institutional constraints. Thus, organizations are manifestations of the institutional environment in which they operate, and they consist of groups of individuals bound by some common goal; for example, political parties, firms, athletic associations, universities, etc. are all organizations. Clearly, the institutions that govern political parties are not the same as those that govern baseball teams, and they range in level of formality and malleability. This is not intended to be a blanket criticism of authors who include the word "institution" in their works when they are actually referring to multilateral organizations or organs of state.[9] For the purposes of this paper, though, it is most helpful to analyze the institutional framework that underlies state function and interstate cooperation rather than examining the organizations that arise from that framework.

It is also important to acknowledge the nonlinear causal relationship between security and growth; that institutional development can lead to improvements in both factors through varying mechanisms. In a 2005 speech to the UN Commission on Human Rights (now the UN Human Rights Council), former UN Secretary-General Kofi Annan declared that "we will not enjoy development without security, or security without development."[10] There are numerous perspectives on the relationship between security and growth, and it remains unclear whether or not one factor directly causes the other and the exact mechanisms by which they affect each other.[11] Additionally, a central question in the field of political economy is the relationship between different types of political institutions—or regime type—and growth, to which there is neither a clear answer nor a causal mechanism.[12] The various intersections among these political and economic factors help explain how and why institutional theory has been adapted to so many different academic traditions. Though this paper does not seek to test a hypothesis about the relationship between security and development, it will inevitably explore that relationship in its discussion of the role of institutions in fostering both of those goals.

Insights from the Development Community

This paper primarily draws from World Bank doctrine as a proxy for the

progression of the development community's understanding of the role of institutions. The World Bank specifically highlighted the importance of governance, defined as "the manner in which power is exercised in the management of a country's economic and social resources for development."[13] This emphasis emerged from the failure of purely market-based reforms—namely, the structural adjustment programs that were popular during the 1980s—to improve growth figures, especially in sub-Saharan Africa, leading officials at the Bank to consider addressing political reforms as well.[14] In the subsequent years, the World Bank would include explicit mentions of institutions for good governance in its yearly World Development Reports (WDRs), which address a variety of topics but ultimately seek to provide in-depth analysis of a specific issue pertaining to development. Over the last 30 years, these WDRs demonstrate an evolution of the World Bank's understanding of the importance of institutions of governance and rule of law that continues to echo throughout the development community's priorities and policy prescriptions, and can certainly be adapted to the defense and security sectors as well.

The World Bank's Initial Conception of Governance

The proliferation of the World Bank's coverage of governance in 1991 produced a broad framework for the components of good governance. The formal, legal framework contained the following elements: a set of rules that are known in advance, that are actually in force; mechanisms to ensure the application of the rules and to allow for departure from them; resolution of conflicts in the application of rules through binding decisions of an independent judicial body; and transparent procedures for amending the rules when they no longer serve their purpose.[15] In addition, the paper called for increased accountability and transparency that would hold public officials responsible for their actions and help mitigate aspects of poor governance. These characteristics of poor governance were easy to recognize and included an unpredictable framework of law and government behavior, institutions that permitted rent-seeking, misallocation of resources, and non-transparent decision-making.[16] Though none of these areas of governance were entirely new to the Bank's work, as confronting elements of the political realm was inevitable in public sector management, the effort and time devoted to fleshing out a theory of good governance marked a turning point in the development community's focus on the political elements of institutional growth, and paved the way for more refined analyses of political and economic situations.

Though it took several years to develop, a clear World Bank doctrine using more specific and nuanced applications of the role of institutions in governance, largely inspired by NIE, began to take form in the early 2000s. WDR 1997 on The State in a Changing World, for example, was the first WDR that primarily focused on political phenomena instead of loosely addressing them as a part of a larger work about markets, finances, or other economic aspects of development. Its primary recommendation was that the state should focus its activities to match its capabilities, and should reinvigorate public institutions in order to ensure adequate incentives for government officials as well as credible checks of corruption and arbitrary rent-seeking.[17] Although these general ideas were not completely novel, and this did not indicate a complete U-turn on the part of the Bank, the focus on political institutions did serve as a corrective for the pro-market emphasis of the 1980s that failed to ameliorate—and may even have contributed to—the crisis of that time.[18] WDR 1997 also included elements of NIE, such as the importance of transaction costs, which were also featured in WDR 2002 on Building Institutions for Markets. According to that WDR's authors, institutions performed three key functions: they

channeled information, defined property rights and contracts, and helped to regulate competition in markets.[19] It also included a lengthy discussion on how to actually build institutions, suggesting that future policymakers complement existing institutions in order to adapt to local conditions, an argument held by numerous political economy scholars, especially prevalent in regions where informal market institutions dominate.[20]

Additionally, WDR 2002 continued the previous discussion about reforming the incentives that public officials face, as well as the importance of an independent, impartial judiciary, in order to credibly improve markets to promote growth and development.[21] The authors of the report saw institution-building as a step-by-step process, taking into account individual country context while also acknowledging that every country had interest groups that benefited from existing arrangements while those who might benefit from change were not sufficiently organized. Interestingly, the report warned against an excessive faith in decentralization, especially when incentives for public officials were not in place, and encouraged experimentation to identify effective political institutions.[22] Also, by emphasizing the importance of accountability of all public officials, including members of the judiciary, the World Bank demonstrated its focus on both political and legal institutions in order to strengthen its policy goals, which, though still oriented toward poverty reduction and economic development, clearly included institutional reforms independent of purely economic concerns.

Further Analysis of Governance Institutions for Development

The World Bank also deepened its analysis of institutions beyond simple governance, including WDR 2011 on Conflict, Security, and Development. In its analysis of fragile states from a developmental lens, its central message was that a particular manifestation of violence at any one time was less important than the underlying institutional deficits that permitted repeated cycles of violence.[23] The report focused on three primary goals of institution-building that would break these cycles of violence: citizen security, justice, and jobs. In order to achieve this, the report urged governments to focus on forming "inclusive-enough coalitions" that incorporated the broad segments of the population whose confidence would be necessary to transform institutions.[24] These coalitions would ensure that actions signal a credible break with the past and would not be reversed, keeping in mind that governments have to balance short-term risks with long-term gain, as actions taken toward democratization and privatization may have immediate ramifications. Programs to achieve these goals include multisectoral approaches to link community structures with the state, as well as security and justice reform to improve transparency, public job creation programs, involvement of women in security and peacemaking, and focused anti-corruption initiatives.[25] The report also implored international actors to play their part in aiding fragile states by harnessing regional and international organizations in order to provide specialized, integrated assistance to reduce pressure on weak institutions within fragile states, especially considering that many modern risks include transnational crime and illicit financial flows that have regional and global implications.

When just less than 30 years earlier the Bank was completely unwilling to address political reforms in its policy proposals, the 2017 World Development Report was entirely dedicated to Governance and the Law. This mainly arose from the concerns about vulnerability to global economic fluctuations and rising inequality in certain countries, even as the diffusion of technology and knowledge have lifted millions out of poverty and improved growth rates.[26] Despite the continual improvement in policy solutions, the actual implementation of those

solutions is severely lacking; thus, the report simply defines governance as the ways in which various actors work together to implement policy within an institutional framework.[27] The analysis in the report starts from the assumption that every society cares about shielding its members from any threats of violence, about promoting prosperity, and about how such prosperity is distributed—security, growth, and equity, respectively.[28] Appraising governance in terms of the ability to deliver on these promises highlights its importance across sectors, correctly implying that a strong institutional framework is necessary to ensure attainment of, for example, the UN's Sustainable Development Goals for social and economic advancement.

According to the report, institutions must provide three core functions: credible commitments in order to promote long-term investment and policy goals, coordination to overcome collective action problems, and cooperation between the state and citizens to prevent free-riding and ensure compliance.[29] In terms of bolstering security, the report dedicates a chapter to "Governance for security," and emphasizes the importance of elite bargains in preventing violence while balancing rent-seeking with long-term development.[30] All of these themes point to a convergence in the World Bank's theoretical conception of the role of institutions in the present day, especially as it pertains to their role in politics. The focus on partnerships between national and local political groups an example of two of the aforementioned functions of institutions—credible commitments and cooperation—reflects a complex understanding of the importance of institutions in providing good governance for security. By aligning the incentive structure faced by politicians with the priorities of local leaders, governments can more adequately utilize their monopoly on the use of force to ensure citizen security.[31] In addition, institutions that allow for increased accountability of police forces demonstrate credibility and contribute to the development of the "inclusive-enough coalitions" mentioned in WDR 2011.

New Institutional Economics

Though the World Bank doctrine does incorporate aspects of NIE into its policy proposals and concept of governance, it is useful to analyze the institutional theory present in the literature and separate of the Bank's focus on development policy. One important function of institutions, as briefly mentioned earlier, is that they reduce transaction costs: "When it is costly to transact, institutions matter."[32] Transaction costs can be defined as the "costs of running the economic system," and are divided into *ex ante* and *ex post* types: Overcoming information costs and negotiating an agreement fall under the former category, while the latter category involves effecting a transaction, or contract, that has already been negotiated.[33] As Ronald Coase observed, in an economic system devoid of transactional frictions, the actors involved in a transaction will be able to bargain to reach an optimal outcome—the presence of inefficiencies, economic or otherwise, indicates that there are omnipresent transaction costs that require institutions to be overcome.[34] The aforementioned information costs also have *ex ante* and *ex post* categories: adverse selection exists in systems in which consumers have less information about a product than the producer or seller, and moral hazard occurs when a party to a transaction has an incentive to take undue risks or act inappropriately if the other party has limited information about their intentions.[35] In this way, information costs can be considered a subset of transaction costs, both of which are relevant outside of a purely economic context.[36]

In theory, institutions help to overcome transaction costs by reducing the friction in a transactional exchange. Institutional theorists operate from a foundation of bounded rationality and opportunism, in which people act rationally but only to a certain extent, as people can only operate under the information that they have

available to them in order to maximize their self-interest—under opportunism, people will exploit these bounds by willful deceit.[37] In a market system, for example, this means that vendors may sell their products at prices that are higher than their worth, exploiting the lack of complete information on the part of potential buyers.[38] Similarly, institutions help to overcome the principal-agent problem, in which one person or group (the "agent") makes decisions on behalf of another person or people (the "principal"), which naturally results in information asymmetry between the principal and the agent.[39] Examples of this relationship include elected officials and their constituents, corporate management and stakeholders, and investors and entrepreneurs, among others, all of which present issues of moral hazard and adverse selection in their contractual arrangements. In the former phenomenon, agents may choose not to expend the amount of effort that the principal may expect after a contract is already signed, or may be affected by perverse incentives, while the latter issue can be illustrated by the insurance market, in which people with higher risk will demand insurance at a higher rate, though the insurers will not be aware of that risk—in this situation, the insurer is the principal while the agent is the person being insured.[40] Theoretically, in all of the above circumstances, the market should not function, or if it does function, it will not function efficiently due to the high and unequal information costs associated with transacting. This is where institutions come into play, by providing incentives to agents to be transparent, monitoring mechanisms to ensure best practices, and credible enforcement of punishments to those who engage in willful and unlawful deceit.[41]

Many theorists, especially those who examine historical institutionalism, focus on path dependence and cultural influences in their analyses of the role of institutions and their development. Numerous economic historians have, for example, connected the institutional legacies from colonialism to modern rates of growth and development, showing that regions in which the colonial authorities set up extractive institutions that protected rent-seeking landlords fare considerably worse in the modern day compared to regions where individual property rights were better defined.[42] In these cases, those areas and countries found it much more difficult to develop strong institutions, which would not only involve building those institutions themselves, but would also require that they reform the incentive structure that is already in place, which was built to benefit certain powerful elites and continues to do so. Though path dependence primarily describes unintended consequences of history, many economic historians also emphasize the importance of a cultural approach to institutions, in which people operate based on culturally defined heuristics that often have institutional manifestations—this is important because it informs how policy should incorporate elements of cultural, perhaps more informal institutions.[43]

In the last decade, in the development community as well as increasingly in the defense and security sectors, there has been an important emphasis on function over form, prioritizing efficient outcomes instead of nominal policy adoption. Scholars have identified "isomorphic mimicry" as the tendency of states to emulate the successes of other states merely by adopting policies or systems of best practices without making the institutional reforms necessary to ensure actual success.[44] Many countries with poor institutions, whose governments engage in excessive rent-seeking behavior or simply lack institutional capacity, have incentives to set targets or adopt policies that may gain them international favorability—and even rewards in the form of IMF loans or foreign aid—without actually following through on achieving functional success.[45] In this way, many external sponsors are complicit in setting targets or conditions for financing that incentivize shallow institutional targets that signal short-term solutions, but may even worsen

the situation in that country by not fully addressing endemic problems.[46] It is crucial to emphasize that the conception of institutions according to NIE does not only involve the establishment of policies or plans, but requires the establishment of a formal or normative constraint that actively limits the behavior of actors within a system. Therefore, the superficial reforms that characterize isomorphic mimicry often do not constitute institutional transformations, which are themselves necessary to foster meaningful change and achieve long-term objectives.

Applications to the Defense and Security Sectors

In the context of defense and security, institutions are important for several reasons, one of which being that they provide signals to the general population. As mentioned in the previous paragraph, these signals are only helpful if they are actually functional and fully implemented in the host country. Especially in fragile states, though, it is crucial to provide immediate signals—redeployment of security forces, credible political appointments, or removal of discriminatory policies, for example—in order to boost citizen confidence in the government and signal a clear break with the past.[47] It is important to ensure that these types of signals are not seen simply as short-run signals of credibility, which can merely reflect a personalistic regime or isomorphic mimicry and do not formulate the norms and cultural foundation for real long-run change.[48] One way in which this can be combated is by simultaneously proposing reforms that signal future change, such as realistic timelines for political reform and decentralization, along with immediate signals.[49] This can be made more effective by utilizing support from NGOs and the international community, which can provide commitment mechanisms and third-party monitoring.[50] For example, if the signals sent by a government do not match up with the verifiable indicators recorded by a third-party monitor, there may be an instance of signals that do not constitute institutional change. These reforms must also be communicable to the populace, as governments will not be able to signal change if people are not aware of it—this can be facilitated by transparent publication of results as well as statewide, regional, and international dialogues.

Long-lasting institutional reforms that can change the executive, judicial, etc., culture of a country need external support because they can require many years to take form and may not be beneficial to agents in the political system in the short term. For this reason, application of World Bank doctrine suggests that regional and bilateral cooperation is key to supporting institution-building while contributing to the achievement of national policy objectives. For example, the United States engages in financial and technical assistance to allies across the world through the Defense Security Cooperation Agency, which includes foreign military sales as well as international military education and training.[51] These partnerships are crucial not only to strengthening military alliances, but also to fostering a constructive dialogue around the importance of institution-building, especially in partner countries with relatively weaker governance institutions. This achieves the dual goal of improving citizen security and human development in those countries while also ensuring that the money spent on foreign military sales, as well as development projects and other investments, is allocated efficiently by the host government that would otherwise lack the institutional capacity necessary to effectively utilize those resources.

One reason for this is that institutions are often necessary in order to change the incentive structure of public service in a country. On a base level, institutions provide the framework for decision-making: for example, in theory, people are incentivized to innovate in a market-based system, whereas they do not face the same incentives in a command economy. Classic problems of economics, such as collective

action and free-riding, directly result from institutional structures, or the lack thereof, wherein people do not feel obligated to contribute to an economic system.[52] Therefore, it is essential to demonstrate that the status quo is actually costlier than a future with better incentives resulting from a strengthened institutional framework. Under the assumption of opportunism, public officials are incentivized to take advantage of institutional deficits that permit information asymmetry, power imbalances, and other opportunities to increase personal utility at the expense of society—hence why corruption and clientelism are major obstacles to development across the world. The lessons from NIE and its treatment of information costs would dictate that institutions should increase transparency and provide credible enforcement/punishment mechanisms against those who are willfully deceitful. Beyond this, though, people in power have to be incentivized to not engage in such behavior in the first place, which involves deeper institutional reforms. Key drivers for reform in this vein include buy-in at the highest levels of political society and a prominent champion for change, which helps to kickstart the process of fundamentally transforming the incentive structure that public officials within a country face.[53]

Just as in markets, political systems are rife with transaction costs that constrain how individual actors interact, which permeate into the security and defense sectors as well. One specific subfield that deals with public bureaucracy is the new economics of organization, which analyzes organizational relationships focusing on hierarchical control and contractual arrangements.[54] One central question of NIE asks why some transactions are organized into firms while others are managed by the market, and the general answer—and a subsequent focus of the new economics of organization—is that firms are organizations that arise out of an institutional framework intended to lower transaction costs.[55] In other words, when there are excessive costs to transact using the price mechanism, actors will create firms that internalize transactions within a hierarchy and minimize the need for excessive contracting. While this is logical in the purely economic sense, the new economics of organization applies this framework to legislative bodies such as Congress, thus originating the concept of the political firm.[56] The difficulty of public bureaucracy, however, is that the institutional arrangements that benefit politicians do not necessarily align with the public interest, as politicians can be "bought out" by specific interest groups.[57] In this way, a politician may be incentivized to sabotage an agency that acts against, for example, the interests of a particular business sector by making it less structurally efficient.[58] Therefore, from an institutional perspective, it is necessary to integrate public servants' incentives with the outcomes of their policies—essentially giving politicians a stake in their own results.[59]

A strong institutional framework that punishes corruption and encourages investment in policies that foster long-run development can accomplish policy goals. From a defense and security standpoint, it is important to highlight that, though corruption and inefficiencies may result in a short-run benefit to the politician and their inner circle, governance institutions are necessary for them to actually achieve their policy goals, both in the short run and the long run. There are myriad reasons for this. A strong institutional framework allows governments to effectively allocate resources to signal to their populations that they can credibly commit to protecting property rights and enforcing contracts, which can prevent countries from entering into continuous cycles of violence and can ensure citizen security and jobs, which in turn translates to productive work and long-run development.[60] This also applies directly to defense and security, as institutions of oversight and monitoring can keep track of spending patterns to detect inefficiencies and diagnose problems. By clearly identifying a focal point at which

the institutional deficit lies, a defense ministry, for example, may identify excessive expenditures or budgetary inconsistencies and target those areas in its future improvements.[61]

Institutions also help to overcome transaction costs in formulation and implementation of policy by overcoming the aforementioned incentives for inefficient bureaucracy. A state with weak governance institutions will inherently contain high information costs associated with political and security "transactions," including the procurement of relevant data to inform a policy or operation, or clearly organized results of the application of that policy or operation. On the other hand, in a state with strong institutions, the defense ministry can meaningfully communicate its policy goals within the governance structure while also constantly assessing their capabilities and planning military/defense operations accordingly, which cannot happen with excessive corruption and/or rent-seeking behavior.[62] A juxtaposition of these two policy environments, especially in the defense and security sectors, has significant implications. In the former state, a high-level public official may face incentives to take bribes and allocate resources inefficiently and in a manner misaligned with the public good. In the latter state, however, the same public official would have interests that are aligned with the public good and would be able to feasibly achieve those shared goals within a stronger institutional framework while also taking advantage of stronger institutions of transparency and accountability to credibly report that progress to their constituents. The prospect of benefiting from a bribe would be eliminated in an institutional structure that contains credible punishment for corruption and incentives to serve the public good above personal gain.

The U.S. government's interagency security assistance architecture has incorporated some of the aforementioned insights, though the programs are relatively new. The case study of defense institution building in Guatemala demonstrates the multisectoral approach necessary to implement institutional reform in a fragile state with weak institutions. Guatemala experienced a a bloody civil war from 1960 to 1996 in which various insurgent groups sought to overthrow the government apparatus, taking approximately 200,000 lives and causing millions of dollars worth of infrastructural devastation through scorched-earth tactics.[63] In the war's aftermath, criminal organizations such as MS-13 engaged in drug trafficking, further weakening state institutions that were already plagued by corruption and clientelism at both national and local levels.[64] The dominance of these institutional deficits implied that traditional U.S. security assistance strategies, such as foreign military financing and sales, would not be effective alone. In 2012, the Guatemalan President Otto Pérez-Molina requested assistance from the U.S. government with devising a national security strategy, effectively putting defense institution building to the test.[65] Instead of merely providing traditional best practices, U.S. officials worked directly with officials from the Guatemalan Ministry of Defense to devise feasible goals, such as the reduction of corruption and streamlining of resource management and oversight. These led to the publication of a National Defense Strategy in 2013 that included within its provisions the creation of an integrated defense governance system that would drive policy priorities with a capabilities-based approach.[66] This included a strict regime of transparency and accountability in order to centralize resource management, moving away from previously opaque financial management processes and simultaneously reducing the space in which corrupt practices could occur. In this way, the ministry could ensure that it was utilizing U.S. security assistance to the best of its potential, whereas in the past it lacked both the capacity and the incentive structure to use such money and resources efficiently.[67] Though the long-term results of this

defense institution building program are yet to be seen, its focus on strengthening institutional capacity through bureaucratic reform, in addition to formal institutions of transparency and accountability, exemplify a sustainable solution that serves the interests of both Guatemala and the United States.

Conclusion

Cooperation on the local, regional, national, and international levels is necessary in order to strengthen institutions in the long term. It is important to note that part of the reason that these institutions are necessary is that they ensure continuity, allowing states to transcend personalistic regimes and prevent arbitrary action on the part of public officials.[68] The close partnership that is necessary to form these institutions, though, is not intended to be everlasting, and therefore countries that are providing such assistance should do so with the intention of allowing for local ownership when the targeted institutional goals are realized. Regional and international bodies can provide third-party monitoring and transparency, through cooperation and dialogue on ideas for improving outcomes, or by aiding with infrastructure for transparent publication of the results of reforms.[69] Especially as transnational security threats arise, this collaboration is essential to prevent cycles of violence and instability. Interagency defense and security cooperation can help build and strengthen institutions in vulnerable states by specifically addressing the disconnect between capability and program design, the time horizon of reform, and bureaucratic management of spending.[70] In this area, the United States can take leadership as it already has with previously mentioned institutions of cooperation, which would bolster its presence in vulnerable regions such as Latin America and sub-Saharan Africa that also are susceptible to the influence of a rising Chinese presence.[71]

Additionally, the development and institutional economic communities both emphasize the importance of tailoring institutions to individual country conditions and to embrace informal institutions in underdeveloped countries in which they predominate society.[72] Many countries with relatively weak governance institutions may have strong informal, normative institutions that nonetheless constrain members of society, and therefore impact the outcomes of a policy or process that would otherwise be considered a best practice. This country-specific context implies that a model of best fit is more appropriate for targeting institutional reforms than a general conception of what those reforms should look like across the board, especially pertaining to program design in developing countries.[73] Despite this, there are still many limits to informal institutions that imply that they may not be sustainable in the long term. For example, they are often not inclusive of different cultural or linguistic groups, preventing the creation of broad coalitions that exist under strong formal institutions.[74] Nonetheless, it is essential to consider informal institutions when formulating policy, especially at the local level, as they can increase the understanding of what types of reforms are and are not possible, while also potentially providing targets for how to *change* the "rules of the game" to improve governance. The example of Guatemala illustrates this complex interaction with incentive structures facing bureaucrats at the ministerial and national levels of governance.

By 1990, the development community as well as the academic community of NIE had realized the importance of institutions of governance in ensuring economic growth. The mechanisms by which institutions effect change are best explained by the school of NIE. Put simply, "institutions are formed to reduce uncertainty in human exchange," meaning that they provide durable rules and norms that constrain actors but provide predictable and continuous patterns of behavior.[75] Strong institutions reduce transaction costs by facilitating the flow of information to

mitigate adverse selection and moral hazard, and reduce agency costs by providing transparency and contract enforcement between principal and agent. Further analysis of institutional phenomena such as path dependence and isomorphic mimicry demonstrates the nuance of institutional reform, emphasizing the importance of cultural and historical context, as well as function over form, in how institutions are built and evaluated. The World Bank has adopted many of these concepts and transformed them into policy prescriptions to ensure that their programs can be effectively funded and implemented. In its World Development Reports, the Bank urges governments to adopt reforms that heighten transparency and accountability of public servants, combat corruption and rent-seeking, and increase external monitoring, all with the goal of shifting the perverse incentives that breed inefficiencies. From an economic perspective, these reforms create a credible commitment on the government's part to actually protect property rights and enforce contracts, which allows people to feel comfortable investing in the future and fostering long-run economic growth.[76] The same logic applies to the defense and security sectors of government. It is necessary to navigate the institutional framework from which governments arise to identify the incentives that dictate which policies will be adapted within the political structure. The United States can demonstrate leadership in defense institution building by engaging further in security cooperation with strategic regional partners and focusing its attention on reforms that make the systems in those countries more transparent and effective in the long term.

About the Author:
Casey Wetherbee is a junior in the BSFS program at Georgetown studying International Political Economy

Endnotes

1. Sarwar K. Lateef, *Evolution of the World Bank's Thinking on Governance* (Washington, D.C.: World Bank Group, 2016), 2.
2. Ibid., 7.
3. While a careful consideration of institutions and governance has taken place in the fields of development and institutional economics, the discussion of defense institution building within the American defense and security sectors only began in earnest a few years ago, with the RAND Corporation's publication of "Defense Institution Building: An Assessment" in 2016, followed by the National Defense University's release of numerous publications about different aspects of DIB. See Alexandra Kerr and Michael Miklaucic, eds. *Effective, Legitimate, Secure: Insights for Defense Institution Building* (Center for Complex Operations, Institute for National Strategic Studies, National Defense University, 2017).
4. Douglass C. North, *Institutions, Institutional Change, and Economic Performance* (Cambridge: Cambridge University Press, 1990), 3.
5. Walton H. Hamilton, "The Institutional Approach to Economic Theory," *The American Economic Review* 9, no. 1 (1919): 309–318, www.jstor.org/stable/1814009; Douglass C. North, 72–75.
6. Kathleen Thelen, "Historical Institutionalism in Comparative Politics," *Annual Review of Political Science* 2 (1999): 369–404; Stanley L. Engerman and Kenneth Sokoloff, "History Lessons: Institutions, Factor Endowments, and Paths of Development in the New World," *Journal of Economic Perspectives* 14, no. 3 (2000): 217–232; Yoram Barzel, *A Theory of the State: Economic Rights, Legal Rights, and the Scope of the State* (Cambridge: Cambridge University Press, 2002): 13–58; Daron Acemoglu, "Why Not a Political Coase Theorem? Social Conflict, Commitment and Politics," *Journal of Comparative Economics* 31, no. 4 (2003): 620–652.
7. Clifford Geertz, "Bazaar Economy: Information and Search in Peasant Marketing," *American Economic Review* 68, no. 2 (1978): 28–32; Mark Granovetter, "Economic Action and Social Structure: The Problem of Embeddedness," *American Journal of Sociology* 91, no. 3 (1985): 481–510; Peter A. Hall and Rosemary C.R. Taylor, "Political Science and the Three New Institutionalisms," *Political Studies* 44, no. 4 (1996): 936–57; Lustick, Ian S. "Taking Evolution Seriously: Historical Institutionalism and Evolutionary Theory," *Polity* 43, no. 2 (2011): 179.
8. Douglass C. North, 3.
9. Robin Hay, *Military and Security Institutions: Challenges in Development and Democratization* (Centre for International Relations, Queen's University, 1994); John R. Galvin, *European Security Institutions: Ready for the Twenty-First Century?* (Brassey's, 2000).
10. https://www.un.org/sg/en/content/sg/statement/2005-04-07/secretary-generals-address-commission-human-rights
11. Robert Bates, Avner Greif, and Smita Singh, "Organizing Violence," *Journal of Conflict Resolution* 46, no. 5 (2002): 599–628; World Bank, 2011. *World Development Report 2011: Conflict, Security, and Development* (Washington, D.C.: World Bank Group); "Security and Development," *SIPRI Yearbook 2015*, SIPRI.
12. Adam Przeworski and Fernando Limongi, "Political Regimes and Economic Growth," *The Journal of Economic Perspectives* 7, no. 3 (1993): 51–69; Nathan M. Jensen, "Democratic Governance and Multinational Corporations: Political Regimes and Inflows of Foreign Direct Investment," *International Organization* 57, no. 3 (2003): 587–616.
13. World Bank, *Governance and Development* (Washington, D.C.: World Bank Group, 1992).
14. *Evolution of the World Bank's Thinking on Governance*, 4–5.
15. *Managing Development: The Governance Dimension* (Washington, D.C.: World Bank, 1991).
16. Ibid., 5–6.
17. In its section on "Restraining Arbitrary State Action and Corruption," WDR 1997 describes how many public officials face incentives to engage in corrupt activities, including the unproductive extraction of rents through bribery, at the expense of the general populace. World Bank, 1997. *World Development Report 1997: The State in a Changing World*. Washington, D.C.: World Bank Group: 99-109.
18. *Evolution of the World Bank's Thinking on Governance*.

19. *World Development Report 2002: Building Institutions for Markets* (Washington, D.C.: World Bank Group, 2002).
20. Celestine Nyamu Musembi, "De Soto and Land Relations in Rural Africa: Breathing Life into Dead Theories about Property Rights," *Third World Quarterly* 28, no. 8 (2007): 1457–1478.
21. *World Development Report 2002: Building Institutions for Markets*.
22. Ibid., 46.
23. *World Development Report 2011: Conflict, Security, and Development* (Washington, D.C.: World Bank Group, 2011), 145–180.
24. Ibid., 120–127.
25. Ibid., 256.
26. *World Development Report 2017: Governance and the Law* (Washington, D.C.: World Bank Group, 2017).
27. Ibid., 3.
28. Ibid., 4.
29. Ibid., 261.
30. Though the chapter discusses security, it mainly focuses on citizen security against widespread violence, and how governance institutions can foster security in this sense. These institutions range from sanction and deterrence institutions to power-sharing to redistributive institutions in order to ensure commitment and cooperation. This paper, by contrast, will later focus on how wisdom from development economics and theory can be applied to defense and security institution-building, which more directly involves reforms to the defense and security sectors of government.
31. *World Development Report 2017: Governance and the Law*, 115.
32. Douglass C. North, 12.
33. Kenneth Arrow, "The Economics of Agency," in John W. Pratt and Richard Zeckhauser, eds., *Principal and Agency: The Structure of Business* (Boston: Harvard Business School Press, 1985): 37–51; Oliver Williamson, *The Economic Institutions of Capitalism* (New York: Free Press, 1985): 19–20.
34. Ronald Coase, "The Nature of the Firm," *Economica* 4, no. 16 (1937): 386–405; Ronald Coase, "The Problem of Social Cost," *Journal of Law and Economics* 3 (1960): 1–44.
35. George Akerlof, "The Market for Lemons: Qualitative Uncertainty and the Market Mechanism," *Quarterly Journal of Economics* 84, no. 3 (1970), 488-500.
36. Transaction costs can be divided into three broad categories: search and information, contracting and bargaining, and monitoring and enforcement. The author's exposure to these categories comes from the course "Political Economy of Institutions and Development," taught by Professor Raj Desai of Georgetown University.
37. Oliver Williamson, *The Economic Institutions of Capitalism* (New York: Free Press, 1985), 47; Moritz Weiss, *Transaction Costs and Security Institutions: Unravelling the ESDP* (Palgrave Macmillan, 2011): 31–35.
38. According to Akerlof (1970), this adverse selection problem will create a situation in which no market transactions will occur, because consumers will assume that they will only be buying overvalued products as sellers of higher-quality goods will exit the market rather than sell their goods at at undervalued equilibrium price. Therefore, institutions are necessary in order for the market to function at all in the face of information asymmetry.
39. Kenneth Arrow, "The Economics of Agency," in John W. Pratt and Richard Zeckhauser, eds., *Principal and Agency: The Structure of Business* (Boston: Harvard Business School Press, 1985): 37–39.
40. Ibid., 40.
41. Douglass C. North, 72–75.
42. Stanley L. Engerman and Kenneth Sokoloff, "History Lessons: Institutions, Factor Endowments, and Paths of Development in the New World," *Journal of Economic Perspectives* 14, no. 3 (2000): 217–232; Daron Acemoglu, Simon Johnson, and James A. Robinson, "Reversal of Fortune: Geography and Institutions in the Making of the Modern World Income Distribution," *Quarterly Journal of Economics* 117, no. 4 (2002): 1231–1294; Abhijit Banerjee and

Lakshmi Iyer, "History, Institutions, and Economic Performance: The Legacy of Colonial Land Tenure Systems in India," *American Economic Review* 95, no. 4 (2005): 1190–1213.
43. Peter A. Hall and Rosemary C.R. Taylor, "Political Science and the Three New Institutionalisms," *Political Studies* 44, no. 4 (1996): 936–57.
44. Matt Andrews, Lant Pritchett, and Michael Woolcock, "Looking like a state: The seduction of isomorphic mimicry," *Building State Capability: Evidence, Analysis, Action* (Oxford University Press, 2017): 30–52; Mark T. Buntaine, Bradley C. Parks, Benjamin P. Buch, *International Studies Quarterly*, 61, no. 2 (2017), 471–488.
45. In "The Politics of Health Aid: Why Corrupt Governments Have Incentives to Implement Aid Effectively," Simone Dietrich of the University of Geneva offers a nuanced argument suggesting that corrupt governments may not efficiently allocate aid to improve conditions across the board, but may focus on a specific area in which compliance is relatively inexpensive. This explains why many autocratic regimes have robust public health infrastructures, which provides a good signal to the international community while also fostering domestic support for the regime, though it does not improve the democratization effort.
46. A current example of this phenomenon is Chile, as the common justification for the October 2019 protests in Santiago is that the Chilean people have endured three decades of government apathy toward persistent inequality and inadequate public goods. Though Chile has relatively strong institutions, reflected by its membership in the Organization for Economic Cooperation and Development, it also has a very high level of inequality largely owing to a lack of public spending, accompanied by a widespread perception of corruption and a focus on economic development at the expense of the poorer sectors of the population. The presence of universal public education, despite its poor quality, is an example of a surface-level institution that may appear strong in a report of education rates, but can nonetheless exacerbate inequality and conflict.
47. *World Development Report 2011: Conflict, Security, and Development*, 145–180.
48. Matt Andrews, *The Limits of Institutional Reform in Development: Changing Rules for Realistic Solution* (Cambridge, England: Cambridge University Press, 2013).
49. *World Development Report 2011: Conflict, Security, and Development,* 145–180.
50. One example of the international community providing commitment mechanisms to support institutional reform is the International Committee against Impunity in Guatemala (CICIG). Earlier in 2019, President Jimmy Morales terminated CICIG's activity in Guatemala, which triggered an institutional crisis, as Morales was being investigated for campaign financing issues. This situation illustrates the need for an internal agent for change within a country, who is willing to invite external supporters to help improve institutional conditions.
51. Much of the work that eventually resulted in this paper originated from my work at the William J. Perry Center for Hemispheric Defense Studies, a regional center of the Defense Security Cooperation Agency in Washington, D.C., which provides context for my insights into the relative interest in institutions on the parts of the defense and security communities compared to the development community.
52. Mancur Olson, *The Logic of Collective Action* (Cambridge, Mass.: Harvard University Press, 1965), 5–52.
53. Alejandro J. Alemán, "Transforming Defense in Guatemala," in Kerr, Alexandra, and Michael Miklaucic, eds. *Effective, Legitimate, Secure: Insights for Defense Institution Building* (Center for Complex Operations, Institute for National Strategic Studies, National Defense University, 2017): 307.
54. Terry M. Moe, "The New Economics of Organization," *American Journal of Political Science* 28, no. 4 (1984): 739–777.
55. Ronald Coase, "The Nature of the Firm," *Economica* 4, no. 16 (1937): 386–405.
56. Barry R. Weingast and William J. Marshall, "The Industrial Organization of Congress; Or, Why Legislatures, Like Firms, Are Not Organized as Markets," *Journal of Political Economy* 96, no. 1 (1988): 132–163.
57. This problem is especially prevalent in mixed and command economies in which politicians have a significant role in shaping and controlling economic policy, because while they

have control rights over the rules governing economic production, they do not have a direct stake in the cash flow resulting from such policies. This lack of sole ownership led politicians in the USSR to only advocate for optimal outcomes after taking bribes from those with cash flow rights—worse, a Coase theorem equilibrium could not be established because the bureaucracy became such that these bribes had to be paid to multiple disparate actors before anything would be done, as shown by Boycko et al (1995).

58. Terry M. Moe, "The Politics of Structural Choice: Towards a Theory of Public Bureaucracy," in Oliver Williamson, ed., *Organization Theory* (New York: Oxford University Press, 1990): 116–153.

59. Interestingly, democratic political institutions are not necessary to ensure that public officials may have a stake in policies that promote growth. For example, in revolutionary Mexico, even under political instability, the government was able to achieve growth by vertically integrating, directly involving members of the private sector in decision-making processes that affected them (Haber et al 2002). Additionally, the reputation of the South Korean political elites served as a credible commitment mechanism due to their long time horizon, contributing to the country's booming growth during the period of export-oriented industrialization (Acemoglu 2003). Additionally, South Korea's tendency to channel rent-seeking behaviors back into the economy by serving as a dividend-collector contributed to growth; on the other hand, looting and rent-scraping by Mobutu and Marcos in Zaire and the Philippines (respectively) diverted profits to their private coffers and did not provide any long-run, or short-run, benefit to the economy (Wedeman 1997).

60. *World Development Report 2011: Conflict, Security, and Development*.

61. "Transforming Defense in Guatemala," 301-302.

62. *World Development Report 2011: Conflict, Security, and Development*, 85.

63. Hal Brands, "Crime, Irregular Warfare, and Institutional Failure in Latin America: Guatemala as a Case Study," *Studies in Conflict & Terrorism* 34, no. 3 (2011), 232.

64. Ibid., 237.

65. "Transforming Defense in Guatemala," 290.

66. Ibid., 293-4.

67. Ibid., 302.

68. *World Development Report 2017: Governance and the Law*, 196.

69. Douglass C. North, 72–75; *World Development Report 2011: Conflict, Security, and Development*.

70. Jean Giraldo, "Assessment and Program Design," in Kerr, Alexandra, and Michael Miklaucic, eds. *Effective, Legitimate, Secure: Insights for Defense Institution Building* (Center for Complex Operations, Institute for National Strategic Studies, National Defense University, 2017).

71. The U.S. National Security Strategy's emphasis on great power competition as well as China's disregard for institutional development and democratic norms demonstrate why this should be considered an American priority from a security standpoint.

72. *World Development Report 2002: Building Institutions for Markets* and Celestine Nyamu Musembi, "De Soto and Land Relations in Rural Africa: Breathing Life into Dead Theories about Property Rights," *Third World Quarterly* 28, no. 8 (2007): 1457–1478.

73. "Assessment and Program Design," 78.

74. *World Development Report 2002: Building Institutions for Markets*.

75. Douglass C. North, 72–75.

76. Yoram Barzel, *A Theory of the State: Economic Rights, Legal Rights, and the Scope of the State* (Cambridge: Cambridge University Press, 2002): 13–58.

The F-35: The Program, Plane, Problems, And Possibilities

Iza Szawiola

The F-35 and its variants were born from the Joint Strike Fighter program, which sought to replace multiple different aircraft with one standard plane and three variants across the different services. While a technological marvel, both the plane and the program have been scrutinized and criticized for what the F-35 can and cannot do. This paper briefly walks through the history of the program, basic specifications of the F-35, the three variants and their intended uses, the problems encountered with the variants and with the program overall, the other nations involved, and lessons that can be learned from this program.

Introduction

The Joint Strike Fighter (JSF) program began in 1996 with the task of finding a way to replace the F-16 Falcon, A-10 Warthog, F/A-18 Hornet, and AV-8B Harrier—and their respective missions—with one plane, the F-35. The mission of the program was to "facilitate development of fully validated operational requirements, proven operational concepts, and transition mature technologies to support successful development and production of affordable next-generation strike weapon systems for the Navy, Marine Corps, Air Force, and our allies." The program sought to bring about the future strike fighter,[1] a multi-role combat aircraft designed primarily as an attack aircraft with a focus on affordability. Additionally, F-35 was meant to "bring cutting-edge technologies" to future battlespaces.[2] The program is now managed jointly by the U.S. Air Force and U.S. Navy, while the Service Acquisition Executive (SAE), or executive oversight responsibility, alternates between the two.[3] The F-35 strives to help the services avoid the high cost of developing, procuring, and operating different aircrafts for each service, and the three variants allow the services to meet their specific operational needs. This piece provides an overall background on the JSF program, including some of the difficulties it has suffered. It offers a brief overview of the three F-35 variants, their missions, their individual qualities and concerns, and discusses the future of the program along with recommendations.

History

In 1993, former Secretary of Defense Les Aspin did a Bottom-Up Review (BUR) in which he observed the need for a Joint Advanced Strike Technology (JAST) program.[4] The BUR intended for the JAST program to find a replacement for the Navy's A-12 program and Air Force's multi-role fighter (MRF), both of which were slated to be terminated. In 1995, the Defense Advanced Research Projects Agency (DARPA) incorporated the development of an advanced short takeoff and vertical landing (STOVL) aircraft into the JAST program. This was because both the USMC and the UK were interested in purchasing new STOVL aircraft to replace the attack aircraft Harrier STOVL. The program was then renamed to the Joint Strike Fighter (JSF) program "to focus on joint development and production of a next-generation fighter/attack plane."[5]

Originally, Boeing Aerospace, Lockheed Martin, and McDonnell Douglas (who partnered with Northrop Grumman and British Aerospace) proposed three different airframe designs. The Defense Department announced on November 16, 1996 that two consortia, led by Boeing and Lockheed, had been chosen to compete in the Concept Demonstration Phase (CDP) of the JSF program. They two firms agreed

to each build a demonstrator aircraft for the three variants. Additionally, Pratt and Whitney would provide engineering support and propulsion hardware. In October 2001, Lockheed's team, including Northrop Grumman, BAE Systems, Pratt and Whitney, and Rolls-Royce, won the contract to build JSFs after the Secretary of Defense certified that the JSF program "had successfully completed the CDP exit criteria and demonstrated sufficient technical maturity to enter" the system development and demonstration (SSD) phase.[6] A Preliminary Design Review (PDR) was conducted in April 2003, and Critical Design Reviews (CDRs) were conducted in February 2006 for the F-35A and F-35B and June 2007 for the F-35C.[7]

Technical Overview

The F-35 was created to be a moderately affordable fifth-generation strike fighter that could be produced with three variants for the U.S. Air Force, the Marine Corps, and the U.S. Navy. The three variants share 80 percent of their parts. The F-35A for the USAF is a conventional takeoff and landing (CTOL) plane, the F-35B has STOVL capabilities for the USMC and the F-35C is carrier landing enabled for the USN.[8] A fifth-generation fighter distinguishes itself from previous generations by combining "new developments such as thrust vectoring, composite materials, supercruise (the ability to cruise at supersonic speeds without using engine afterburners), stealth technology, advanced radar and sensors, and integrated avionics to greatly improve pilot situational awareness."[9] Currently, the only other U.S. military aircraft that can be classified as "fifth-generation" is the USAF's F-22.

It is no exaggeration to call the F-35 a technological marvel. Among its avionics and cockpit features, L-3 Display Systems "is developing the panoramic cockpit display system, which will include two 10in×8in active matrix liquid crystal displays and display management computer." Vision Systems International supplies an advanced helmet-mounted display system (HMDS), and BAE develops side stick and throttle controls as well as an alternative HMDS design. The HMDS projects airspeed, heading, altitude, targeting information and warnings directly onto the aviator's helmet visor, granting him or her incredible situational awareness. Ball Aerospace provides a communications, navigation and integration (CNI) body antenna suite and Harris Corporation provides "advanced avionics systems, infrastructure, image processing, digital map software, fibre optics, high-speed communications links and part of the." One of the most important characteristics of the F-35 is its ability to "combine information with Aegis [weapon] systems and other command and control systems operated by allies worldwide," which will enhance American forces' ability to work with allies and improve combat capabilities.[10] The technology provides the F-35 with information faster than ever before. All of these capabilities enhance an aviator's ability to have a clear picture of his or her surroundings and accurately and quickly assess the situation.

In terms of armament, the F-35 will carry weapons "in two parallel bays located in front of the landing gear. Each weapons bay is fitted with two hardpoints" which can carry various bombs and missiles.[11] The F-35 can carry armament both internally and externally, but if weapons are loaded externally, the F-35's stealth decreases dramatically.[12] Internally, the F-35 is cleared to carry joint direct attack munitions (JDAM), wind-corrected munitions dispensers (CBU-105 WCMD), joint stand-off weapons (JSOW), small diameter bombs (SDB), Paveway IV guided bombs, AIM-120C AMRAAM air-to-air missiles, and Brimstone anti-armor missiles. Externally, the F-35 can carry joint-air-to-surface stand-off missiles (JASSM), AIM-9X Sidewinder, AIM-132 ASAAM, and Storm Shadow cruise missiles.[13]

Multiple companies are responsible for other F-35 features. Regarding the engine, all three variants will use either the "Pratt and Whitney afterburning turbofan F-135, a derivative of the F119 fitted on the F-22," or the developing F-136 by General Electric and Rolls-Royce. The engine will also have two BAE Systems full authority digital electronic control (FADEC) systems and Hamilton Sundstrand's gearbox. Lockheed Martin Missile & Fire Control and Northrop Grumman Electronic Sensors and Systems together provide the JSF electro-optical system, including long-range detection and precision targeting by Lockheed's electro-optical targeting system (EOTS) and Northrup Grumman's distributed aperture system (DAS) thermal imaging system.[14] DAS "allows the operator or the fleet managers to see hundreds of miles away on a 360-degree basis,"[15] and "streams real-time imagery from six infrared cameras mounted around the aircraft to the helmet, allowing pilots to 'look through' the airframe."[16] The advanced electronically scanned array (AESA) is being developed by Northrop Grumman Electronic Systems. The AN/APG-81AESA multi-function radar will include agile beam steering capabilities and "combine an integrated radio frequency subsystem with a multifunction array."[17] Meanwhile, BAE Systems will supply the JSF electronic warfare suite with its information & electronic warfare systems (IEWS), along with some subsystems from Northrop Grumman. Other systems and suppliers from the ones discussed above include Smiths Aerospace, Parker Aerospace, ATK Composites, Vought Aircraft Industries, Moog Inc., Edo Corporation, Stork Aerospace, and Goodrich.[18] Additionally, the "F-35 core combat systems are interactive with one another, creating a synergistic outcome and capability rather than providing an additive-segmented tool,"[19] meaning that the pilot will be able to nearly seamlessly use these functions together without needing to control each one individually.

F-35A

The Air Force's F-35A variant is a CTOL aircraft. According to the Air Force's website on the aircraft, the mission of the F-35A is to replace the F-16s and A-10s with a plane that has enhanced survival capabilities in advanced threat environments. It also features aerodynamic performance and advantec integrated avionics, as well as next-generation stealth and situational awareness capabilities.[20]

In 2015, damning reports showed the F-35A repeatedly losing to the F-16—the very aircraft it was slated to replace—in mock dogfights due to its poor turning abilities. As an aircraft touted for its superior multi-role capabilities and a direct replacement for the F-16, the reports were certainly not positive. However, new 2019 leaked videos show that the F-35A's maneuverability has improved so dramatically that it would be difficult for older jets to compete with it,[21] removing the biggest concern with replacing the aging F-16.

While it seems obvious how the F-35A will replace another fighter plane, there has been some debate on how the F-35A will complete the A-10's primary mission of close air support (CAS). CAS is air-action that is coordinated with the movement and fire of ground forces against enemy targets that are close to friendly forces. The A-10's "thirty-millimeter cannon can fire at a greater range and with more accuracy than any other fighter, and it can loiter over a target area longer than any other fourth-generation platform."[22] The A-10's ability to loiter along with its "pilots who are intimately familiar with the faculties, movement, mindsets and limitations of the Army, puts the A-10 weapons system heads above all others in the CAS environment."[23] However, because of the limited numbers of A-10s, other aircraft such as the F-16 and F-15E must supplement them in the CAS mission. In Afghanistan, A-10s only flew 24 percent of all CAS sorties. These other aircraft did well in this role, showing that CAS is not limited to just the realm of

the A-10 and giving hope to the F-35A. Moreover, the F-35 provides critical capabilities such as stealth and sensor fusion technologies to operate in a modern, high threat CAS environment that the A-10 was not designed for.[24]

This being said, there are valid arguments for not completely retiring the A-10, one of which is the culture and community surrounding the plane. As previously mentioned, part of the reason the A-10 excels at CAS is because the A-10 pilots are trained specifically to operate with the Army, which requires not only technical and tactical know-how but also an understanding of how the service works. The F-35A was designed to be able to serve a variety of functions and missions, and while the plane can do CAS admirably well, it may prove unreasonable to expect all F-35A pilots to intimately understand what it means to work with the Army. This is especially true when the A-10 is not only equally effective but also much less costly. Particularly in low-threat environments, it may not be necessary to have a fifth-generation fighter when the A-10 would do perfectly well.[25] In interviews with 23 pilots experienced in CAS who flew the A-10, F/A-18, AV-8B, and F-35, all "23 pilots picked the F-35 over their previous fighter for CAS missions in a high-threat environment. However, more than half picked their fourth-generation jets over the F-35 for CAS in low-threat situations."[26] In the early 2000s the Army voiced this concern, and originally the USAF planned to also purchase the STOVL F-35Bs specifically to replace the A-10s and keep CAS as a USAF priority. However, this decision was later reversed, and the USAF still plans on retiring the A-10.[27]

CAS is not the only USAF mission the F-35A will perform. The F-35 has been tasked with missions such as "interdiction, suppression of enemy air defenses, air superiority and special weapons,"[28] which it will do along with the F-15X and the F-22 Raptor. The USAF has been adamant about keeping the F-15E Eagle along with the F-35A, but if forced to choose, former USAF Secretary Heather Wilson stated that they will choose the fifth-generation F-35A over a fourth-generation aircraft.[29] Currently, the primary missions of the F-22 are air-to-air dominance and counter air defense missions such as protecting friendly forces and important interests from enemy air attack.[30] In an interview, Marine Corps Lieutenant Colonel Dave Berke, who has experience flying for the Air Force as well, explained that the F-22 and F-35 are different from fourth-generation aircraft because of the way data—such as flight and sensor data—are processed onboard. "The difference is how you think," Berke said. "In the Raptor, the data is already fused into information thereby providing the situational awareness. . . . There's virtually no data in the F-22 that you have to process; it's almost all information."[31]

Because both the F-22 and F-35 have this onboard data processing capability, pilots will now have access to information that was previously only available in the Control Systems (AWACS) and the Combined Air Operation Center (CAOC). In essence, instead of just making tactical decisions, these pilots will now have increased visibility into operational and strategic developments, and this information will be distributed in the battlespace.[32]

Comparing the two fifth-generation aircraft, the F-35A is not as stealthy or capable in air-to-air combat as the F-22, but it is still meant to be quite adept in these areas as well as in air-to-ground combat. Most importantly, the F-35A is scheduled to be a more affordable plane than the F-22.[33] There are certainly similarities between the F-22 and F-35, but, while the F-35 was designed to fulfill a variety of functions such as air-to-ground missions, the F-22 was designed to be a formidable air superiority fighter.[34] In another interview, Berke noted that he believes the most important measure of an aircraft is situational awareness, and in this measure, according to Berke, the F-35 beats all other

platforms, including the F-22.[35] In this sense, the two aircraft complement each other and fill in the others' gaps.[36] However, the F-22 is no longer in production, and a 2017 Pentagon report to Congress argued against restarting production.[37] The question remains: can the F-35A do all the missions it is slated to do?

F-35B

The F-35B is scheduled to replace Boeing's AV-8B Harrier jump jet, a custom aircraft designed for the Marine Corps. The aircraft is designed to have vertical takeoff and landing. For decades, the AV-8B was the only fixed-wing plane that could be used with the Navy's amphibious assault ships,[38] making it critical to the Marine Corps aviation mission to "attain and maintain combat readiness to support expeditionary maneuver warfare."[39] The F-35B has this capability as well, requiring the aircraft to work very differently from its other variants. Specifically for the F-35B, "the engine is coupled with a shaft-driven lift fan system for STOVL propulsion. The counter-rotating lift fan, developed by Rolls-Royce Defence, can generate more than 20,000lb of thrust. Doors installed above and below the vertical fan open as the fin spins up to provide vertical lift."[40]

At the beginning of 2019, there were 124 AV-8Bs in USMC service, and the aircraft is expected to be completely phased out by 2028.[41] Thankfully, pilots have found the F-35B, a remarkable replacement. Andy Egdell, a Squadron Leader in the Royal Air Force (RAF), noted that while the AV-8B requires pilots to constantly assess the plane's flying and respond to the pilot, with the F-35, "you just sit there and go hands free and it will stay exactly where you've put it. Flying an F-35 to an aircraft carrier is an absolute pleasure, as opposed to a Harrier, which frankly can be borderline terrifying."[42]

Egdell was able to execute the first ever aft-facing landing on a carrier with the F-35B.[43] Similarly, retired Marine Corps Colonel Arthur "Turbo" Tomassetti said that he had to practice hovering in a AV-8B, but with the F-35, "hovering is so easy that there have been pictures of pilots with their hands above the canopy rails showing, 'Look, no hands' because once you put it where you want, it's going to stay there until you tell it to move or it runs out of gas."[44] The most notable recently reported issue came in 2019 when a pilot had difficulty landing due to the presence of hot gas ingestion on a day where temperatures were over 90 degrees Fahrenheit. This fix is the USMC's main priority for the F-35 program, since the problem could affect F-35B operations in the Middle East. F-35 program head Vice Admiral Mat Winter was confident that this one-off incident would be addressed in fixes scheduled to be in place by April 2020.[45]

F-35C

The USN's mission is to "maintain, train and equip combat-ready Naval forces capable of winning wars, deterring aggression and maintaining freedom of the seas."[46] In order to do this, the USN needs to control the sea and project power.[47] Naval aviation, along with carrier strike groups and expeditionary strike groups, provide the U.S. with strategic options and flexibility.[48] In order to maintain a high level of performance against adversaries, the USN needs to continuously explore new technological advances in its aircraft. This is where the F-35C comes in. The USN's carrier variant (CV) is the newest of the three variants and is also the only fifth-generation fighter specifically built for carrier operations. Compared to the other variants, the F-35C has more robust landing gear for catapult launches and fly-in arrestments, and the larger wings' wingtips fold in to maximize space on the carrier's deck. It also has more internal fuel capacity than the other variants, carrying almost 20,000 pounds of internal fuel, which affords it a longer range and more persistence than other fighters in a combat configuration.[49] In addition to the F-35B, the USMC plans to have four F-35C squadrons.[50]

The F-35C will replace the much-loved F/A-18C Hornet, and as the Navy buys more F-35Cs, it intends to buy fewer F/A-18E/F Super Hornets. The F-35C was originally supposed to reach initial operations capable (IOC) in late 2015, but that was pushed back to early 2019.[51] In order to be at IOC, at least one F-35C squadron has to be "properly manned, trained and equipped to conduct assigned missions in support of fleet operations. This includes having 10 Block 3F, F-35C aircraft, requisite spare parts, support equipment, tools, technical publications, training programs and a functional Autonomic Logistic Information System (ALIS)."[52] For the Navy in particular this delay was not ideal—the F/A-18 fleet's reliability rate has worsened[53] since the Navy has had to fly longer using older fighters, whose parts are difficult to source and require more maintenance.[54]

The bigger problem, of course, is that the Navy has been "lukewarm" about the F-35C,[55] which is the most expensive variant, the least numerous,[56] and double the cost of the F/A-18E.[57] Unlike the F-35C's issues with cost and delays, Boeing's F/A-18 has a reputation of being on time and in cost and "stands poised to deliver a significant portion of advanced capabilities with an F/A-18 update."[58] While the aging F/A-18C needed to be retired and replaced, some argue for limiting the number of F-35Cs and instead reinvesting into "more advanced Super Hornets and its electronic attack variant in the form of the EA-18G Growler while investing in a stealthy new unmanned strike aircraft and a future F/A-XX."[59] The reason behind this argument is that the USN may have to keep its carrier almost 1,000 nautical miles offshore in order to stay out of reach of new Chinese anti-ship ballistic missiles. This requires a longer-range air wing than that provided by the F/A-18 and F-35C.[60] Flightglobal reported in May 2019 from the Navy League Sea-Air-Space conference that the USN plans on designing the F/A-XX without cooperating with other services because the Navy has different priorities than the Air Force. USN Deputy Director of Air Warfare Angie Knappenberger told reporters that "the Navy does not plan on using the fighter to penetrate enemy airspace, a key requirement for the U.S. Air Force's Next Generation Air Dominance (NGAD) jet."[61] Long term, this would lead to each air wing in the Navy having two F/A-XX and two F-35C squadrons.[62]

Although an upgraded and advanced F/A-18 would certainly have its uses, the F-35C still has one thing even an upgraded F/A-18 will never have: stealth. For now, it seems that in the near future the USN will combine the relatively small numbers of stealth F-35Cs with the numerous and potentially more powerful Advanced Super Hornets.[63]

JSF/F-35 Problems And Praise

The JSF program, while a revolutionary idea, has been under near-constant bombardment by critics. One of the issues with the program is with how the aircraft is being developed: it is being produced and evaluated simultaneously. While this can speed up the process of getting planes out into the field, it also produces frequent design changes. Furthermore, the JSF program was restructured three times before 2013. Each restructuring caused significant delays and rising costs, making the program seem "too big to fail," which "places industrial interests over taxpayer money and operational requirements."[64] Another issue is the program's leadership. In the first 18 years, the "JSF/F-35 program office had nine different directors—one every two years—and no matter how bright an individual may be, it takes at least a year to become familiar with the interwoven complexities of such a program."[65] Finally, Congress put Air Force Lieutenant General Chris Bogdan in charge of the program, and while his tenure from 2012 to 2017 was not untainted by controversies, the improvements to the program highlight the need for stable leadership.[66]

However, the stability has not lasted—in 2017 when Bogdan retired Navy Rear. Adm. Mat Winter was named the new head of the program,[67] but by July 2019 this position had switched again due to the Navy and Air Force switching program leadership roles.[68]

For the planes itself, data from Navair's Sources Sought solicitation on the Federal Business Opportunities (FBO) website suggested in 2016 that "F-35 fighters are expected to require between 41.75 and 50.1 maintenance man-hours (MMH) per flight hours, or about three times as many as most fighter aircraft currently operated by Western air forces."[69] In terms of costs, in May 2019, Robert Daigle, the outgoing head of the Department of Defense's Cost Assessment and Program Evaluation (CAPE) office, acknowledged during a House Armed Services subcommittee hearing that the Defense Department's goal of getting cost per flight hours (CPFH) for the F-35A down to $25,000 by fiscal year 2025 is most likely impossible. For FY24, CAPE estimates $36,000 per hour and the F-35 Joint Program Office (JPO) estimates $34,000. Both would be an improvement on the FY18 rate of around $44,000. Although Lockheed believes there is a way to reach this goal, the latest Defense Department acquisition figures estimate $1.196 trillion in F-35 operation and maintenance costs. This seems to obscure some positive developments, such as the falling unit costs of the F-35, which by FY20 will fall to $80 million for the F-35A[70] and is projected to cost less than $100 million for the other two variants in FY20/FY21.[71] Additionally, CPFH has been reduced by about 15 percent since 2015.[72] However, the costs were expected to be much lower; originally, the flyaway cost on average was supposed to be $28-38 million in FY94 dollars.[73] That said, the F-35A will still be decidedly less expensive than "the dated, four-plus generation Eurofighter Typhoon, the French Rafale M, or the latest version of the F-15K Strike Eagle. It will outperform those jets and every other four-plus-generation fighter in high- or low-threat air-to-surface scenarios, and none of them would fare well against the F-35 in an air-to-air engagement."[74]

There are also cost issues outside of flying and buying the aircraft. While Air Combat Command head Gen. Mike Holmes accepted that the unit price of the F-35 is falling, he noted that it might be difficult to buy and sustain the other systems associated with the F-35, such as the logistics platform and simulators. "Right now the air vehicle is out ahead of those other elements," Holmes said. "Producing more elements would be one part of it, but keeping up in all of those other areas — to me — would be the challenge."[75] Moreover, according to Winter, the supply chain is having difficulties getting parts to Lockheed's production line on time. This causes the aircraft to move slower through the production process and, therefore, increases labor costs. Winter says Lockheed is 600 parts behind on average, and this shortage of spare parts is also a strain on the services' operational jets, which have to compete with the new production aircraft for these same supply of parts. The parts themselves are not as reliable as expected, and it is taking them longer than planned to move them through depot.[76] The F-35 "is meeting four out of eight reliability and maintenance (R&M) targets, including the most important such as mean flight hours between failure and maintenance man-hour per flight hour."[77]

Cost, while certainly an important issue, is far from the only one. According to the Pentagon's annual operational testing report,[78] the Navy's F-35C has unacceptably low "fully mission capable" rates. This means that the aircraft is "almost never fully ready for combat"[79] even though the USN is pushing ahead with the plane. In past years, the Director of Operational Test and Evaluation (DOT&E) reports have found cyber vulnerabilities in the F-35

and performance issues in availability and reliability, and in life expectancy testing. The 2018 report shows lack of progress in "nearly every essential area," and the report "is markedly less transparent than previous reports. It provides no updates on the crippling deficiencies highlighted in previous years, reports far fewer findings critical of the program than earlier reports, and contains almost no quantitative results on the F-35's most urgent problems."[80]

Additionally, the report presents "little hard data on maintainability; availability and flying hours; weapons-testing results; ALIS-caused maintenance problems; pilot difficulties with sensors and display; and shortfalls in testing resources and realism."[81] The report also shows that "testing on the Air Force weapons systems used in air-to-ground attack indicates 'unacceptable' accuracy," and the F-35B service life could be as low as 2,100 hours, which is significantly lower than the expected service life of 8,000 hours.[82] Reliability of the F-35 has already been an issue- after the crash of an F-35B in South Carolina in September 2018 the Pentagon ordered all the F-35 fighters grounded for a time.[83] These are just a few of the problems mentioned in the report and highlighted by the POGO investigation. The potential of the HMDS is incredible, but unfortunately it has not been able to reach it yet. Pilots have complained about night system interface issues that heavily interfere with mundane tasks such air-to-air refueling or tanking. With pilots saying that tanking seems like almost a near-emergency procedure, fixing the HMDS is certainly and urgent operational need.[84]

While these are certainly glaring problems with the JSF program, the F-35 seems to excel in the realm of pilot opinions. A Heritage Foundation report asked thirty-one experienced pilots who currently fly the F-35A to rate their previous fourth-generation aircraft (F-15C, F-15E, F-16C, and A-10) and the F-35A for energy and maneuvering characteristics and then asked the pilots which fighter he would prefer "in combat if he were to face a clone flying the other jet in six different air-to-air situations."[85] The pilots "selected the F-35A 100 percent of the time in beyond-visual-range situations and over 80 percent of dogfighting situations where energy and maneuverability are critical to success."[86] The U.S. can also take solace in the fact that this is not the first time a multi-mission aircraft has not measured up to lofty ambitions. Previous foreign examples include the WWII German Junkers Ju-88 and 1970s Panavia Tornado, and in the U.S. military even the current mainstay F/A-18 had issues when it first debuted. At the beginning, the F/A-18 "lacked the range and payload of the A-7 Corsair and acceleration and climb performance of the F-4 Phantom it was meant to replace."[87]

The pilots' enthusiasm for the F-35 can give the U.S. hope that, once certain issues are resolved, the plane can become the marvel it has been described as, albeit a more expensive one than anticipated.

Other Nations

With the focus mostly on how the U.S. military is going to use the new F-35s, it is easy to forget that this is a joint venture in more ways than one. Many other nations signed up to help fund and receive the F-35 variants. In 2001, "the UK MoD signed a memorandum of understanding [MoU] to cooperate in the SDD . . . phase of JSF and, in September 2002, selected the STOVL variant to fulfill the future joint combat aircraft (FJCA) requirement."[88] Each partner nation is classified as a certain level. The level-one partner, the UK, contributes 10 percent of development costs. Level-two partners, Italy and the Netherlands, contribute $1 billion and $800 million, respectively, Level-three partners, Australia, Canada, Denmark, Norway, and Turkey contribute between $125 million and $175 million. Singapore and Israel are Security Co-operation Participants (SCP), essentially a fourth tier of partner, and Japan is an export partner.[89] Each "level also determines the schedule of deliveries, as well

as technology transfers and subcontracting opportunities."[90] All the partners plus Singapore signed up to the SDD phase. By 2007, Australia, Canada, the Netherlands, the UK, Norway, Turkey, Denmark, and Italy had signed a MoU for the F-35 Production, Sustainment, and Follow-on Development (PSFD) phase, and Israel requested the sale of F-35 aircraft in May 2018. Additionally, as of 2019 South Korea has received six F-35As.[91] Greece is also considering the F-35 to replace its aging F-16 fleet.[92] However, in July 2019 Turkey was officially excised from the JSF program due to its decision to accept a Russian S-400 anti-air missile system.[93]

Though the F-35 program is multinational, "everyone understands that its fate depends solely on the politics within the famed Beltway where forces bent on tidying up America's fiscal house are challenging the bloated [defense] budget."[94] For example, there has been considerable friction regarding the share of work and technology transfer, with some partners like the UK arguing that the U.S. has been exceedingly cautious about the transfer of JSF technologies.[95] Since the F-35 source code for the onboard computer controls more than 90 percent of system functions, Lockheed is expected to perform most if not all the source code changes in the U.S. For foreign partners, an appropriate analogy is that "the buyer is expected to agree to operate the machine, but without touching the fuse box."[96]

If there is this friction, why would partner nations agree to participate in the program? USAF Major Valerie "Twitch" Wetzbarger summed up the benefits of allied nations having F-35s by noting that "the F-35 enables the U.S. Air Force to be a more integrated force. For example, in my squadron, Americans, Italians, and Norwegians work together and teach each other. Flying the same jet builds a stronger joint and coalition team and makes us more capable as a NATO unit."[97] Wetzbarger is referring to the "interoperability" of the partner nations with the U.S., which is made easier by using the same weapons system used by the U.S. military. The F-35 represents a contribution to the security of certain U.S.-centered international institutions, mainly NATO and ANZUS. The Japanese, an Aegis partner, will benefit from being able to pair the powerful system with new F-35s. Regarding South Korea, the F-35A's "will generate a whole new approach to linking C4ISR into a more effective deployable force" by allowing the U.S. to use a honeycomb approach to the Pacific, "where force structure is shaped appropriately to the local problem but can reach back to provide capabilities beyond a particular area of interest."[98] From a U.S. perspective, Assistant Professor Srdjan Vucetic argues that in spite of the friction due to the JSF program, "partner countries continue to offer a fairly unambiguous recognition of US authority and status as the 'leader'. In other words, there is no imminent erosion in the American security system (and so, depending on your perspective, American leadership, hegemony, imperium)—at least as far as the so-called traditional allies are concerned."[99] With national defense being shared by multiple nations, sharing platforms only makes security easier.

Lessons And Takeaways

As with any new military innovation, the F-35 program has been filled with both technological advancement and political and economic frustration. There are lessons we can glean from the program thus far that will hopefully help the U.S. in future programs, as well as important questions that should be asked to determine the future of each of the services in regards to air power.

The JSF program itself was structured in a way that invited delays and increasing costs. By developing and building the F-35s at the same time the U.S. and partner nations were hoping to get planes in the air faster and more efficiently. Instead, the program had to be restructured multiple times, all three variants were heavily delayed, and price per plane and

for research and development shot up. In the future, it may be prudent to avoid this process and assess other ways to improve efficiency and timeliness of the end product. In addition to the process, the JSF program also suffered from a lack of continuous leadership. It proved near impossible for any head of the program to be able to stabilize and fix the JSF program with the short amount they were in charge of it. It was only when Bogdan stayed in charge for a few years that positive progress was made on some of the most pressing issues, such as cost. If Lt. Gen. Eric T. Fick remains head of the F-35 program for a few more years, I believe the JSF program and the military will be much better served. Moving forward, stable leadership should be kept in mind as a priority for any new military program.

The three services involved are also not immune to scrutiny. The Air Force's intention is to replace the F-16, a fighter plane, and the A-10, an air-to-ground CAS plane, with the F-35A. There are certainly pros to having a multi-use plane: having many of one type of aircraft that can complete multiple missions instead of various, mission-specific planes means that there is a higher likelihood of a USAF aircraft being in the area that can complete an urgent mission at a moment's notice. However, the question is just how well the F-35A will be able to complete all the missions it is tasked with. Once the F-35A has several years of service under its belt, it will be worthwhile to study whether the USAF was right to procure a multi-mission plane or whether it was better served with having multiple aircraft, each with its own specific mission set. This will be especially important to assess for CAS. Another important question for the Air Force is if the F-35A will not serve as a substitute for the F-22, does the Air Force need to design a new air superiority fighter, or is that not necessary to complete the Air Force's missions?

The Navy seems to already have learned from the JSF program and has announced that its next plane, the F/A-XX, will not be a joint program. While having one plane with three variants yields benefits such as more efficient part procurement and better joint capabilities amongst the three services, it also forces researchers and developers to think of a large range of goals, missions, and preferences, which can lead to compromises and certain key features missing. The USN will certainly be well served with a stealth aircraft, but would a Navy-specific stealth plane designed only for the USN have been a better, and perhaps cheaper, fit for the USN? Perhaps part of the reason the JSF program has been plagued with difficulties is because of the very concept it was founded on: one plane with three variants for three different services. When the services start looking to future aircraft, I would recommend they do so separately. This lesson also holds true for the USMC. While the service is pleased to replace the aging and difficult AV-8B Harrier, the F-35B was delayed and more costly than anticipated. For the next jump jet, the USMC may also want to look into a USMC-specific design.

It was outside the scope of this paper to really delve into the F-35 foreign partnerships, but it is worth looking into the difficulties and benefits of working with other nations. For the U.S., this helps spread the cost of research and development while still maintaining control of the program. It also makes it easier for the U.S. military to cooperate and work with allied nations, since they are working with the same weapons systems and platforms. However, it does lead to some strained relationships and compromises as well. For the foreign partners many of the same holds true, except they have less sway on the program and are beholden mostly to U.S. politics and decision-making, especially regarding the F-35 source code. On the whole, despite frustrations and compromises I believe both the U.S. and its allies mainly benefit from joint programs such as the F-35.

Regardless of the pros and cons of the JSF program, it is clear that it is here

to stay. The U.S. can only hope that F-35's issues will be resolved and that the variants will prove successful in their stated missions.

About the Author

After growing up in Connecticut, Iza obtained an undergraduate degree from Duke University with a double major in Political Science and Russia Language and Culture. She now works in Northern Virginia and is working towards a masters degree from Georgetown SSP with a concentration in Military Operations.

Endnotes

1. Derek W. Avance, Robert E. Clay, David S. Grantham, David Kelly, John Rupp, Christopher S. Ceplecha, Terry M. Featherston, Patrick A. Kelleher, Garry L. Pendleton, and Christopher E. Yelder, "The Joint Strike Fighter," *The Directorate of Research, Air Command and Staff College*, April 1996, accessed August 12, 2019.
2. "35 Lightning II Program," *The F-35 Lightning II,* accessed August 13, 2019, http://www.jsf.mil/.
3. Jeremiah Gertler, *F-35 Joint Strike Fighter (JSF) Program: Background and Issues for Congress,* Library of Congress Working Paper, December 22, 2009, 9, https://apps.dtic.mil/dtic/tr/fulltext/u2/a512761.pdf.
4. Avance, et al, "The Joint Strike Fighter"
5. Gertler, "F-35 Joint Strike Fighter (JSF) Program: Background and Issues for Congress," 7.
6. Ibid, 7.
7. Ibid, 7.
8. Eric Tegler, "WTF-35: How the Joint Strike Fighter Got to Be Such a Mess," *Popular Mechanics*, July 27, 2018, https://www.popularmechanics.com/military/a21957/wtf-35/.
9. Gertler, "F-35 Joint Strike Fighter (JSF) Program: Background and Issues for Congress," 2.
10. Robbin F. Laird and Edward T. Timperlake, "The F-35 and the Future of Power Projection," *NDU Press*, no. 66 (Fall 2012): 85-93, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-66/jfq-66_85-93_Laird-Timperlake.pdf?ver=2017-12-06-115714-667.
11. "F-35 Lightning II Joint Strike Fighter (JSF)"
12. Kyle Mizokami, "We're Stuck With the F-35 and That Might Not Be a Bad Thing Anymore," *Jalopnik*, October 03, 2018, https://foxtrotalpha.jalopnik.com/were-stuck-with-the-f-35-and-that-might-not-be-a-bad-th-1828869804.
13. "F-35 Lightning II Joint Strike Fighter (JSF)"
14. Ibid.
15. Laird and Timperlake, 87.
16. "Unprecedented Situational Awareness," F-35 Helmet Mounted Display (Lockheed Martin), accessed December 7, 2019, https://www.f35.com/about/capabilities/helmet)
17. "F-35 Lightning II Joint Strike Fighter (JSF)"
18. Ibid.
19. Laird and Timperlake, 88.
20. "F-35A Lightning II."
21. Alex Lockie, "The F-35 Was Once Trounced by F-16s in Dogfights, but It Just Proved It Can Out-turn Older Jets," *Business Insider*, January 16, 2019, https://www.businessinsider.com/f-35-once-beaten-by-f-16s-shows-stunt-turns-older-jets-cant-touch-2019-1.
22. John Venable, "A-10 Versus F-35: What a Head-to-Head Showdown Won't Answer," *The Heritage Foundation*, June 6, 2016, https://www.heritage.org/defense/commentary/10-versus-f-35-what-head-head-showdown-wont-answer.
23. Ibid.
24. Ibid.
25. Ibid.
26. John Venable, "F-35 vs. A-10 Flyoff Poses More Questions," *The Heritage Foundation*. March 1, 2017, https://www.heritage.org/defense/commentary/f-35-vs-10-flyoff-poses-more-questions.
27. Venable, "A-10 Versus F-35: What a Head-to-Head Showdown Won't Answer"
28. Ibid.
29. Oriana Pawlyk, "Air Force Wants Both F-35 and F-15EX. But If Forced to Choose, It's No Contest: SecAF," *Military.com*. May 20, 2019, https://www.military.com/daily-news/2019/05/20/air-force-wants-both-f-35-and-f-15ex-if-forced-choose-its-no-contest-secaf.html.
30. Laird and Timperlake, "The F-35 and the Future of Power Projection," 86.
31. Ibid, 87.
32. Ibid, 87.
33. Gertler, "F-35 Joint Strike Fighter (JSF) Program: Background and Issues for Congress", 3.

34. Linda Shiner, "F-35: What The Pilots Say." Air & Space Magazine. March 22, 2019, https://www.airspacemag.com/military-aviation/f-35-faces-most-critical-test-180971734/.
35. Ibid.
36. "F-22 vs. F-35: Which Stealth Fighter Wins in a Shootout?" *The National Interest*. January 15, 2019, https://nationalinterest.org/blog/buzz/f-22-vs-f-35-which-stealth-fighter-wins-shootout-41652.
37. "The Air Force Just Closed The Door on New F-22 Raptors," *The National Interest*. July 05, 2019, https://nationalinterest.org/blog/buzz/air-force-just-closed-door-new-f-22-raptors-65511.
38. "F-35 Lightning II Joint Strike Fighter (JSF)"
39. *2019 Marine Corps Aviation Plan,* Report, https://www.aviation.marines.mil/Portals/11/2019AvPlan.pdf.
40. "F-35 Lightning II Joint Strike Fighter (JSF)."
41. David Axe, "The F-35B Is the Future of the U.S. Marine Corps (But Can Old Harrier Jets Keep Flying?)," *The National Interest*, April 07, 2019, https://nationalinterest.org/blog/buzz/f-35b-future-us-marine-corps-can-old-harrier-jets-keep-flying-51202.
42. Shiner, "F-35: What The Pilots Say."
43. Ibid.
44. Ibid.
45. Aaron Mehta, "The Marine Corps' 'No. 1 Priority' for the F-35 Involves a Rough Landing in Hot Environments," *Defense News*, June 14, 2019, https://www.defensenews.com/air/2019/06/12/the-marine-corps-no-1-priority-for-the-f-35-involves-a-rough-landing-in-hot-environments/.
46. "Our Navy's Mission: How the Surface Forces Fit In," *U.S. Navy*, Fall 2017, https://www.public.navy.mil/surfor/swmag/Pages/Our-Navys-Mission-How-the-surface-forces-fit-in.aspx.
47. Ibid.
48. "Naval Aviation Vision 2016-2025," *U.S. Navy*, 2016, https://www.navy.mil/strategic/Naval_Aviation_Vision.pdf.
49. "F-35C Lightning II," *F-35 Lightning II*, Accessed August 13, 2019, https://www.f35.com/about/variants/f35c.
50. Mark D. Faram, "This Is What's Going on with the Navy's F-35C Program," *Navy Times,* February 28, 2019, https://www.navytimes.com/news/your-navy/2019/03/01/this-is-whats-going-on-with-the-navys-f-35c-program/.
51. Mizokami, "We're Stuck With the F-35 and That Might Not Be a Bad Thing Anymore."
52. "F-35C Achieves Initial Operational Capability," *U.S Navy*, February 28, 2019, https://www.navy.mil/submit/display.asp?story_id=108746.
53. Kyle Mizokami, "The F-35C Is Finally Ready for Combat, Though Of Course It Was Years Late," *Jalopnik*, March 08, 2019, https://foxtrotalpha.jalopnik.com/the-f-35c-is-finally-ready-for-combat-though-of-course-1833108052.
54. Mizokami, "We're Stuck With the F-35 and That Might Not Be a Bad Thing Anymore."
55. Dave Majumdar, "America's Lethal F-35 vs. F/A-18 Super Hornet: Who Wins?" *The National Interest*, April 02, 2016, https://nationalinterest.org/blog/the-buzz/americas-lethal-f-35-vs-f-18-super-hornet-who-wins-15670.
56. Lockie, "The F-35 Was Once Trounced by F-16s in Dogfights, but It Just Proved It Can Out-turn Older Jets."
57. "Aircraft Museum - F/A-18E/F Super Hornet," *Aerospaceweb.org*, accessed August 13, 2019, http://www.aerospaceweb.org/aircraft/fighter/f18ef/.
58. Lockie, "The F-35 Was Once Trounced by F-16s in Dogfights, but It Just Proved It Can Out-turn Older Jets."
59. Majumdar, "America's Lethal F-35 vs. F/A-18 Super Hornet: Who Wins?"
60. Ibid.
61. Mizokami, "After the F-35, the Navy Will Make Its Next Fighter Without the Air Force."
62. Ibid.
63. Lockie, "The F-35 Was Once Trounced by F-16s in Dogfights, but It Just Proved It Can Out-turn Older Jets."

64. Srdjan Vucetic, "The F-35 Joint Strike Fighter: A Global Snapshot," *Strategic Analysis* 37, no. 5 (2013): 649–56. doi:10.1080/09700161.2013.821277.
65. Venable, "Operational Assessment of the F-35A Argues for Full Program Procurement and Concurrent Development Process."
66. Ibid.
67. Aaron Mehta and Valerie Insinna, "F-35 Program Chief Bogdan to Retire; Deputy Director to Be His Successor," *Defense News*, August 08, 2017, https://www.defensenews.com/breaking-news/2017/03/28/f-35-program-chief-bogdan-to-retire-deputy-director-to-be-his-successor/.
68. Ben Werner, "F-35 Program Leadership Changes as Turkey's Future in Program Uncertain," *USNI News*, July 15, 2019, https://news.usni.org/2019/07/15/f-35-program-leadership-changes-as-turkeys-future-in-program-uncertain.
69. Giovanni De Briganti, "Navair Sees F-35 Requiring Up to 50 Maintenance Hours per Flight Hour," *Defense Aerospace*, December 5, 2016, http://www.defense-aerospace.com/articles-view/feature/5/179243/navair-projects-f_35-to-need-50-maintenance-hours-per-flight-hour.html.
70. Valerie Insinna, "One of the F-35's Cost Goals May Be Unattainable," *Defense News*, May 03, 2019, https://www.defensenews.com/air/2019/05/02/one-of-the-f-35s-cost-goals-may-be-unattainable/.
71. Mizokami, "We're Stuck With the F-35 and That Might Not Be a Bad Thing Anymore."
72. Insinna, "One of the F-35's Cost Goals May Be Unattainable."
73. Christopher Bolkcom, *Joint Strike Fighter (JSF) Program: Background, Status, and Issues,* Report no. RL30563 - The Library of Congress, January 11, 2002, https://www.everycrsreport.com/files/20020111_RL30563_f4cf70861cb78ab27e9029846fa9c51ccfbf6995.pdf.
74. John Venable, "Why Trump Blasted the 'Out of Control' F-35 Program," *The Heritage Foundation*, December 21, 2016, https://www.heritage.org/defense/commentary/why-trump-blasted-the-out-control-f-35-program.
75. Insinna, "One of the F-35's Cost Goals May Be Unattainable."
76. Ibid.
77. Chris Pocock, "Question Marks Remain Over F-35 Availability, Support," *AIN Online*, June 16, 2019, https://www.ainonline.com/aviation-news/defense/2019-06-16/question-marks-remain-over-f-35-availability-support.
78. *FY18 DoD Programs: F-35 Joint Strike Fighter (JSF),* Report, Accessed August 12, 2019. https://assets.documentcloud.org/documents/5736009/FY2018-DOT-E-F35-Report.pdf.
79. Dan Grazier, "F-35 Far from Ready to Face Current or Future Threats, Testing Data Shows," *Pogo*, March 19, 2019, https://www.pogo.org/investigation/2019/03/f-35-far-from-ready-to-face-current-or-future-threats/.
80. Ibid.
81. Ibid.
82. "Stealth F-35 Joint Strike Fighter Has Some Serious Problems: Report," *The National Interest*, January 31, 2019, https://nationalinterest.org/blog/buzz/stealth-f-35-joint-strike-fighter-has-some-serious-problems-report-42892.
83. James Clark, "Pentagon Orders Entire F-35 Fleet Grounded," *Task & Purpose*, April 15, 2019, https://taskandpurpose.com/pentagon-f35-grounded.
84. Ibid.
85. John Venable, "Operational Assessment of the F-35A Argues for Full Program Procurement and Concurrent Development Process," *The Heritage Foundation*, August 4, 2016, https://www.heritage.org/defense/report/operational-assessment-the-f-35a-argues-full-program-procurement-and-concurrent.
86. Ibid.
87. Tegler, "WTF-35: How the Joint Strike Fighter Got to Be Such a Mess."
88. "F-35 Lightning II Joint Strike Fighter (JSF)."
89. Srdjan Vucetic and Kim Richard Nossal, "The International Politics of the F-35 Joint Strike Fighter," *International Journal* 68, no. 1 (Winter 2012-2013), 5.

90. Vucetic and Nossal, "The International Politics of the F-35 Joint Strike Fighter," 5.
91. Franz-Stefan Gady, "2 More Republic of Korea Air Force F-35A Stealth Fighters Arrive in South Korea," *The Diplomat*, July 17, 2019, https://thediplomat.com/2019/07/2-more-republic-of-korea-air-force-f-35a-stealth-fighters-arrive-in-south-korea/.
92. Igor Bozinovski, "Greece Eyes F-35s as F-16 Replacement," *Flightglobal.com*, April 15, 2019, https://www.flightglobal.com/news/articles/greece-eyes-f-35s-as-f-16-replacement-457481/.
93. Aaron Mehta, "Turkey Officially Kicked out of F-35 Program, Costing US Half a Billion Dollars," *Defense News*, July 17, 2019, https://www.defensenews.com/air/2019/07/17/turkey-officially-kicked-out-of-f-35-program/.
94. Vucetic, "The F-35 Joint Strike Fighter: A Global Snapshot."
95. Gertler, "F-35 Joint Strike Fighter (JSF) Program: Background and Issues for Congress," 13.
96. Vucetic, "The F-35 Joint Strike Fighter: A Global Snapshot."
97. Shiner, "F-35: What The Pilots Say."
98. Laird and Timperlake, "The F-35 and the Future of Power Projection."
99. Srdjan, "The F-35 Joint Strike Fighter: A Global Snapshot."

Counterintelligence 101 revisited

A review of William R. Johnson's *Thwarting Enemies at Home and Abroad: How To Be a Counterintelligence Officer* (Washington, D.C.: Georgetown University Press, 2009)

Edgar Iván Espinosa

This article provides some lines of critique to William R. Johnson's Thwarting Enemies at Home and Abroad: How To Be a Counterintelligence Officer. *While this re-edition of the classic succeeds in depicting the timeless principles of the discipline, it fails in linking them with covert action. This is particularly relevant at present when Russia is deploying aggressive "active measures" around the globe. Also, the training-oriented handbook lacks a proper discussion on the ethical implications of invasive tools such as surveillance and interrogation.*

Almost since the beginning of intelligence studies, the field of Counterintelligence (CI) has had little scholarship devoted to it, despite its importance for both protecting intelligence activities, personnel, products, and for disrupting the opposition's capabilities. The scarce literature on this subject has been mainly limited either to attempting to provide a definition (like John Ehrman's classic article "Toward a Theory of CI: What are We Talking About When We Talk about Counterintelligence?") or to digging into espionage cases (like Ronald Kessler's books).[1] Thus, *Thwarting Enemies at Home and Abroad* presents itself as a must-read for entry-level intelligence officers, students and scholars interested in the core tactics and procedures for detecting spies and handling agents. Certainly, this is not another dissertation from a strategic perspective, but an easy-to-read didactic handbook.

William Johnson, an American CI officer with over three decades of experience, originally published the book in 1987, at the end of a tragic decade for US intelligence. According to a study of the Defense Personnel and Security Research Center (PERSEREC), in that period 62 Americans were arrested for espionage, almost half of them caught three years before the book's release.[2] In this context, the CIA's green light for the publication of this book could be read as an attempt to assuage concern by conveying that the agency indeed possessed highly trained professionals working to prevent catastrophes like those caused by Edward Lee Howard, Karl and Hana Koecher, and Jonathan Pollard.[3]

Despite the intrinsic value of this re-edition of the classic, some issues are worth further analysis. One of them is the content's structure. Initially, the topics seem to be ordered in a deductive way. The first three chapters distinguish CI activities: defensive (physical and personnel security), and active-offensive counterespionage. Johnson also contrasts the tensions between law enforcement (prosecuting a spy) and counterespionage (turning the spy to manipulate the enemy). The following chapters use sanitized cases to concisely explain how safe houses, dead drops and the whole support apparatus work. The use of active tactics, such as double agents, moles and defectors are also clarified. However, the final two chapters abruptly alter the logic of contents by returning to the basics: how to manage a file and what strategic deception is. Since the book was conceived as a training manual, it would have been more sensible to introduce these topics before discussing mole hunts or double agent playing. Johnson would agree: "Without

organized information, the CI officer can't get where she has to go" (p. 175).

Johnson's understanding of CI should also be scrutinized. He visualizes the discipline as a set of techniques: "aimed at frustrating the active efforts of alien conspiratorial organizations to acquire secret or sensitive information belonging to the government" (p. 2). Whereas this concept reflects the essence of CI, the author does not link it with covert action, an activity barely discussed at the end of the book (p. 198).[4] This is surprising because as practitioners may immediately recognise, CI is a key element for guaranteeing a spectrum of plausible deniability by protecting the planning and execution of covert actions. For instance, in order for a country to obfuscate its involvement in the manipulation of foreign elections, its CI should, in principle, ensure that orders are transmitted through secure channels; actions are carried out within safe facilities; neither personnel nor infrastructure can be identified or linked to authorities; moles are rooted out; and that previously recruited foreign agents are able to securely report back on the reactions. The broader, Russian-style CI approach of "active measures" would also consider protecting intelligence activities by launching disinformation campaigns or some other distractors through employing both covert and overt tools.[5] In this regard, and considering the time of the original publication, it would have been interesting to see a comparison of American and Russian approaches to CI.

Another weakness of the book is the author's overly rigid view of the attributes necessary in a CI officer. Specifically, he argues that curiosity, pattern recognition, scepticism, patience, and nerve are all essential traits for CI officers. Though he is right, these are not exclusive of CI. Rather, they are vital for all intelligence professionals, whether an analyst, an operative, or a manager. This narrow-mindedness may be an example of why James Olson, former chief of CIA counterintelligence, considers one of the ten commandments of CI to be to not make an uninterrupted career in this craft.[6]

Johnson's sometimes superficial and ambivalent approach towards ethical considerations are also disappointing. For example, while he rejects physical torture because it does not produce reliable information (p. 35), he does not censure strong psychological pressure: "We said that physical pain is not relevant in interrogation. Anxiety, humiliation, loneliness, and pride are another story" (p. 36). Other examples are the reductionist way in which he suggests that CI efforts work to acquire information: "(. . .) either directly by filching or copying documents, or by installing surveillance devices" (p. 32). Also, when referring to elaborating dossiers of persons of interest and the possibility that these may constitute a violation of privacy, he blatantly suggests: "Build your dossiers but keep them out of the wrong hands. You have violated privacy at the beginning; respect it thereafter" (p. 184). These issues merit a more thorough elaboration, and the author would have done well to emphasize that these actions must be performed for a greater good (national security) and assessed case-by-case. While the author's main concern was to explore tradecraft, it would have been useful to provide prospective officers with some criteria for evaluating the pros and cons of executing those actions or even worse examples: blackmail, honeytraps, feeding drug habits, evidence fabrication, spying on fellow citizens overseas, and renditions.[7]

Finally, this re-edition could have been better understood with a historical framework. Georgetown University Press should have considered including not only a review of the prolific author's career but also an introduction to the origins of the Western-Soviet confrontation. An explanation of how CI (initially known as "X2" or "XX") raised as a crucial activity in the silent war between intelligence agencies would have been illustrative as well. This was crucial, at least according to Raymond Garthoff, who has concluded

that the most notable accomplishments of espionage of the US and the USSR were for CI purposes.[8]

About the Author:
Edgar Iván Espinosa is a graduate of the William J. Perry Center for Hemispheric Defense Studies (CHDS) at the National Defense University (NDU). He is currently pursuing an MA in Intelligence and International Security at King's College London. Edgar holds a double major in Political Science and International Relations from the Mexican Autonomous Institute of Technology (ITAM). He has lectured at Mexico's Naval War College (CESNAV), National Defense College and the Military Intelligence School (EMI). *The author expresses his gratitude to the Chevening Scholarships, the UK government's global scholarship programme, funded by the Foreign and Commonwealth Office (FCO) and partner organisations, for making possible this review.*

Endnotes

1. John Ehrman, "Toward a Theory of CI: What are We Talking About When We Talk about Counterintelligence?" *Studies in Intelligence* 53:2 (2009), 5-20. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no2/toward-a-theory-of-ci.html; Ronald Kessler, *Spy Vs Spy: Stalking Soviet Spies in America* (New York: McMillan Publishing, 1988); and Ronald Kessler, *Escape from the CIA: How the CIA Won and Lost the Most Important KGB Spy Ever to Defect to the U.S* (Pocket Star Books, 1992).
2. Katherine L. Herbig and Martin F. Wiskoff, "Espionage Against the United States by American Citizens 1947-2001," Technical Report 02-5, (PERSEREC, 2002) https://fas.org/sgp/library/spies.pdf
3. For a comprehensive recount of some of the most damaging espionage cases in the US see Michael J. Sulick, *American Spies: Espionage Against the United States from the Cold War to the Present* (Washington, DC: Georgetown University Press, 2013).
4. A discussion of covert action as a tool for American foreign policy can be found in William J. Daugherty, "Covert action: Strengths and Weaknesses" in *The Oxford Handbook of National Security Intelligence*. Oxford Handbooks, ed. Loch K. Johnson. (Oxford: Oxford University Press, 2010).
5. Aktivnyye meropriyatiya, or "active measures," range from simple propaganda and forgery to assassination, terrorism and everything in between. For further analysis see Richard H. Shultz and Godson, Roy, *Dezinformatsia: Active Measures in Soviet Strategy* (Washington: Pergamon Press, 1984); and Dennis Kux, "Soviet Active Measures and Disinformation: Overview and Assessment" *Parameters* 15:4 (1985), 19-28.
6. James M. Olson, "The Ten Commandments of Counterintelligence," *Studies in Intelligence* (Fall-Winter 2001) https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/fall_winter_2001/article08.html
7. For a deep discussion on the ethics of these tactics see James M. Olson, *Fair Play: The Moral Dilemmas of Spying* (Washington, D.C.: Potomac Books, 2007).
8. Raymond L. Garthoff, "Foreign Intelligence and the Historiography of the Cold War," *Journal of Cold War Studies* 6:2 (2004), 21-56.