Negotiating [Im]plausible Deniability:

Strategic Guidelines for U.S. Engagement in Modern Indirect Warfare

By Kyle Atwell, Joshua M. Portzer, and Daphne McCurdy

American adversaries such as Russia and Iran are persistently challenging U.S. interests around the world through indirect attacks. Rather than threaten the United States head-on, these competitors employ nebulous tools like private military contractors, proxies, and cyber-driven disinformation campaigns that are difficult to attribute, enabling plausible deniability, and muddle the distinction between violent and nonviolent actions. The frequency and ubiquity of these incidents—whether in Syria, Afghanistan, or even back home—suggest that indirect attacks will remain a primary tactic in geopolitical competition for the foreseeable future. Yet, the implications of these indirect means of competition for U.S. policy are not well understood. The centerpiece of these attacks is adversaries' ability to threaten U.S. interests repeatedly over time and geographies while obfuscating the seriousness of the threat and keeping the acts below the threshold of public attention. We find that by mitigating domestic political pressure in the targeted state to react decisively, indirect attacks provide that state the benefit of decision space for how to respond. The aggregate implication for national security is that the use of indirect attacks may have the overall effect of *reducing* the level of conflict in the international system by increasing opportunities to offramp escalation. For this to be true, however, states must take advantage of the space to leverage other tools like diplomacy to reduce tensions.

Indirect Attacks: Defining the Problem

U.S. policymakers increasingly recognize that geopolitical competition is taking place in the blurred operational space between peace and war. The 2017 National Security Strategy notes that adversaries and competitors have become adept at seeking to alter the status quo by "operating below the threshold of open military conflict and at the edges of international law."[1] Similarly, the 2018 National Defense Strategy cautions that "revisionist and rogue regimes have increased efforts short of armed conflict by expanding coercion to new fronts, violating principles of sovereignty, exploiting ambiguity, and deliberately blurring the lines between civil and military goals."[2]

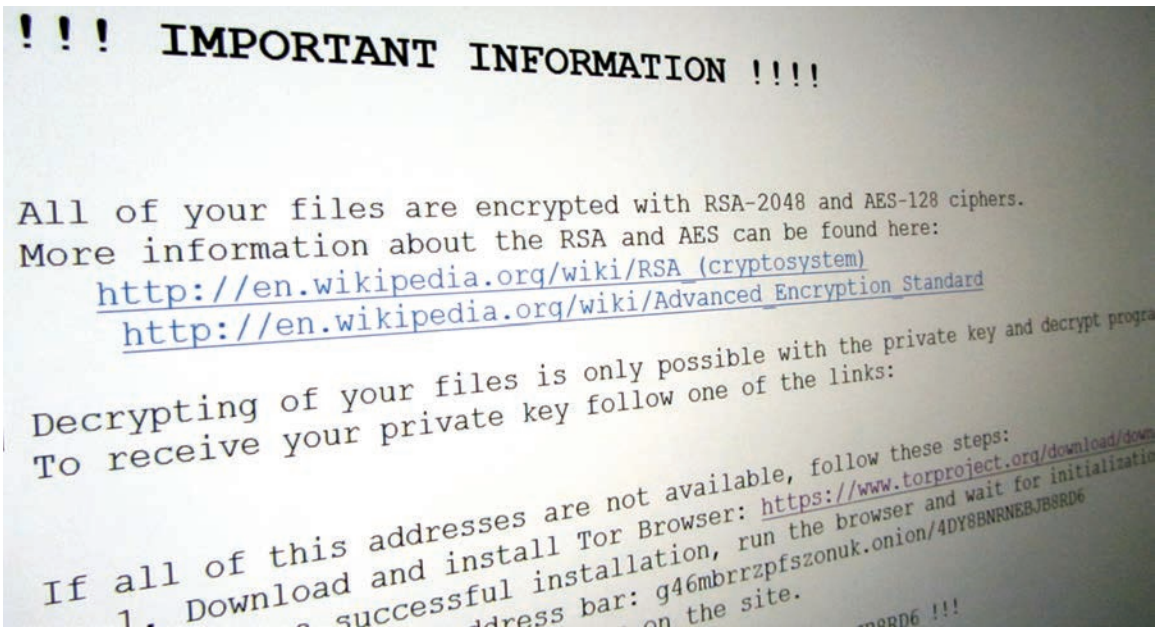
Kyle Atwell is an active-duty U.S. Army Officer, Ph.D. student in Security Studies at Princeton University, and Co-Director of the Irregular Warfare Initiative." Joshua Portzer is an active duty naval flight officer currently stationed in Jacksonville, Florida. He is a current Presidential Leadership Scholar (2020-2021). Daphne McCurdy is a Senior Associate at the Center for Strategic and International Studies and a fellow at The Century Foundation.

While this form of competition is galvanizing attention, there has been extensive debate over the specific lexicon to describe the challenge set. This includes grey zone conflict, political warfare, irregular warfare, new generation warfare, and hybrid warfare. The focus of this article is on a specific tactic commonly used in this type of competition, which we refer to as *indirect attacks*. These attacks threaten U.S. interests through both violent and nonviolent means but below the threshold of a *direct,* conventional military conflict. Indirect attacks include the use of mercenaries, local proxy militia, and hacking and disinformation campaigns to exploit social divisions.[3]

A defining feature of indirect attacks is "ambiguity—about the ultimate objectives, the participants, whether international treaties and norms have been violated, and the role that military forces should play in response."[4] Contributing to this ambiguity is the deliberate use of plausible deniability. Aggressors obscure involvement in an attack often by using ostensibly nonstate actors, such as private military companies, as well as through cyber operations that are difficult to attribute and sometimes reinforced by public statements of denial by officials. The use of plausible deniability allows a state to damage U.S. interests in a way that convolutes its ability to respond decisively.

Attacking U.S. Interests Abroad: War by (Many) Other Means

While not exclusive to Russia, Moscow's efforts to challenge the United States provide a case study of the use of indirect attacks, including those against U.S. partners, U.S. forces abroad, and most brazenly against the U.S. population itself. The pattern is consistent: Russia employs nonstate actors with close links to the regime, like the Wagner Group and the Internet Research Agency, and/or directly hires hackers adept at hiding their identities to attack U.S. interests and then denies any direct control or affiliation with them, often with plausible deniability so thin that *implausible deniability* would be a more accurate term to describe it.

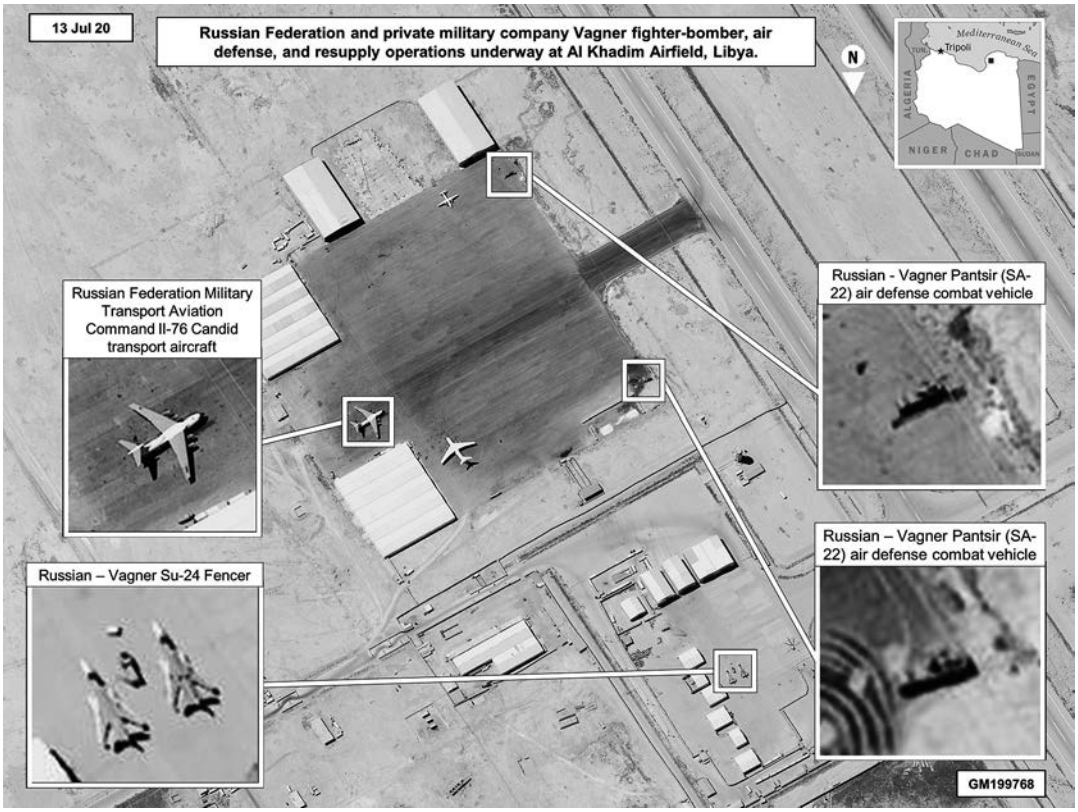


Locky is ransomware malware released in 2016. It is delivered by email and after infection will encrypt all files that match particular extensions." (Christiaan Colen, March 15, 2017)

Russia's annexation of Crimea is a well-known case that provides insights into the use of ostensibly nonstate actors to enable implausible deniability. Russia worked through a myriad of nonstate actors to include a citizens militia that "lacked any unit markings, but had all the bearing of professional Russian combat forces" while being controlled operationally by Russian military services.[5] Russia also employed other indirect means to influence the Crimea conflict, including state media (*Russia Today* and *Channel One*) disseminating propaganda to craft a narrative that legitimized action against Ukraine's sovereignty.[6] In these ways, Russia seized physical territory from another sovereign state that was pursuing deeper ties with the West while implausibly claiming it was not directing the effort.

While Crimea provides an essential springboard, there are other instances of Russian indirect attacks that have generally remained below the threshold of public acceptance or awareness, to include multiple kinetic engagements against the U.S. military around the world. In Syria, a battalion (approximately 500 soldiers) that included Russian mercenaries from the Wagner Group attacked an American Special Operations Force's outpost, resulting in a four-hour firefight and hundreds of casualties.[7] Similar to its statements denying Russian forces in Crimea, the Kremlin spokesperson stated, "We only handle the data that concerns Russian forces… We don't have data about other Russians who could be in Syria."[8]

In another example, in June 2020, Russia was accused of paying bounties to Afghan fighters to kill



Russian air defense equipment, including SA-22s, are present in Libya and operated by Russia, the Wagner Group or their proxies." (Courtesy U.S. Africa Command, July 13, 2020)

U.S. and coalition forces. Even if direct bounty payments are not occurring, Russia is cooperating with and supporting the Taliban as it actively fights American troops.[9]

In addition to Afghanistan and Syria, Russia has also threatened U.S. interests in Libya. Most directly, Russian-affiliated groups were accused by U.S. Africa Command (AFRICOM) Commanding General Stephen J. Townsend of downing a U.S. drone, providing hundreds of ground forces from the Wagner Group (the same private security company suspected of attacking the U.S. outpost in Syria) in support of General Khalifa Haftar, and sending 14 fighter aircraft to Libya. Russia denies all of these activities. For example, while a UN report identified Russian, Belarussian, Moldovan, Serbian, and Ukrainian fighters in Libya, President Vladimir Putin stated that fighters in Libya neither represented Moscow nor were paid by the state.[10] AFRICOM provided evidence that the jets came from Russia and stopped in Syria en route for a paint job to hide their Russian origins. Nonetheless, the head of the defense committee in the upper house of the Russian parliament called the claim "stupidity" and suggested the aircraft came from another African country.[11] While this response is implausibly deniable, it still serves its intended purpose to obfuscate the facts and keep the story below the level of public acceptance.

Bringing it Home—Russia Attacks America Directly, Maybe

Russia's disinformation activities during the 2016 U.S. presidential campaign showcase the complexities surrounding contemporary cyber-based acts. The United States is not the sole target of Russia's election meddling, as multiple European states have faced "cyber hacking, fake news, [and] disinformation" to include "extensive use of both paid creators of fake content and 'troll farms.'"[12] The latter feature is also prevalent in the #BlackLivesMatter and #BlueLivesMatter campaigns that appeared in 2016 as an attempt to sow discord within American society. Scores of actors identified by social media companies belonged to the Russian Internet Research Agency (RU-IRA), which is owned by Yevgeny Prigozhin, a close ally of Putin's.[13] Additionally, the RU-IRA used numerous bots to amplify the white noise online by retweeting messages from agents and other bots alike.[14] At the same time, hackers directly linked to state intelligence, like the Russian Military Intelligence and the Foreign Intelligence Service, have also sought to upend the political landscape in the United States, most notably by breaking into the Democratic National Committee's emails.[15]

When asked by journalists about interference in Western elections in 2017, President Putin denied state support for cyber attackers and social media trolls but called them patriotic: "If they are patriotic, they contribute in a way they think is right, to fight against those who say bad things about Russia."[16] These efforts to divide American society from within continue today. Both China and Russia are suspected of actively encouraging through social media the 2020 race protests in the U.S. triggered by the suffocation of an African American, George Floyd, by a white police officer.[17,18] However, the tenuous evidence for these attacks, combined with their orientation around real U.S. domestic fractures, keeps the role of U.S. rivals off center stage. This presents a serious security threat while failing to garner the public attention to respond to it.

These examples are not intended to represent the holistic picture of Russian attacks against U.S. interests around the world. Nor do we suggest that indirect attacks are unique to Russia. Rather, these examples demonstrate how states leverage indirect attacks against the United States to provide a veil of implausible deniability. The centerpiece of these attacks is adversaries' ability to attack U.S. interests repeatedly over time and geographies (even

attacking U.S. personnel and destroying military equipment) while obfuscating the seriousness of the threat and keeping the acts below the threshold of public attention.

Indirect Attacks: Challenge or Opportunity?

While indirect attacks are often viewed as posing a challenge to liberal democracies, they also provide an opportunity for targeted states like the United States to manage conflict. Because these tactics push the bounds of international law and norms, there is a concern that they advantage authoritarian states like Russia and China. While rivals are able to lie and deny their actions, open societies with a free press and democratic accountability may be more likely to hold their leaders to account for such deceit. Indeed, Thomas Rid argues that, "For liberal democracies in particular, disinformation represents a double threat: being at the receiving end of active measures will undermine democratic institutions—and giving into the temptation to design and deploy them will have the same result. It is impossible to excel at disinformation and at democracy at the same time."[19]

Even the 2017 National Security Strategy acknowledges this imbalance.

Repressive, closed states and organizations, although brittle in many ways, are often more agile and faster at integrating economic, military, and especially informational means to achieve their goals. They are unencumbered by truth, by the rules and protections of privacy inherent in democracies, and by the law of armed conflict. They employ sophisticated political, economic, and military campaigns that combine discrete actions. They are patient and content to accrue strategic gains over time—making it harder for the United States and our allies to respond.[20]

A second major concern with these types of tactics is that their ambiguity can unwittingly beget escalation. With differing threat perceptions as to which attacks constitute hostile acts, lack of clarity as to the motivations and identities behind the attacks, and no clear norms around retaliation, indirect means of competition can sow so much confusion as to engender an excessively aggressive response.[21] This is especially the case with the use of plausible deniability. If the target state does not know who is attacking, it will be difficult to understand why they are being attacked and what behavior the unknown attacker wants to change.[22] Related, the outsourcing of these challenges to proxy forces or mercenaries to whom a state does not want attribution or direct control undermines command structures and constrains a sponsor's ability to exert control over the degree of escalation.[23] As a result, even though these methods are employed precisely to avoid a large-scale conflict, by muddling the threat environment, they can actually lead to escalation.

However, this ambiguity also presents a real opportunity for liberal democracies like the United States, where public opinion shapes decisionmaking about waging war, by providing the space for policymakers to eschew unnecessary escalation in favor of intentional, measured responses. The reality is that even if indirect attacks blur the nature of the threat, policymakers are often equipped with intelligence to ultimately determine their origins. By contrast, the public's understanding of indirect attacks is often confused, which reduces public calls for escalatory retaliation. First, each individual event fails to sustain public ire since there is doubt about whether an accused state is truly responsible. The fact that the aforementioned force-on-force attack pitting Russian mercenaries (alongside Syrian partners) against Americans in Syria did not sustain public outrage or attention is a case in point. Second, the connection between multiple attacks over time and across geographies is not conceptualized as a continuous campaign or systematic threat in the public psyche. Even when the media covers an individual attack—for

example, Russia allegedly paying bounties for the killing of American troops in Afghanistan revealed in summer 2020—the public debate focuses on whether the allegation is legitimate rather than building a narrative that this is one of a series of geographically dispersed attacks that collectively form a systematic strategy of indirect warfare.

This confusion is exacerbated by the 24-hour news cycle, which further complicates the ability to demonstrate a serious threat because the incidents, already muddled due to unclear attributability, are overtaken by other news. Take, for example, how the U.S. intelligence community's statement accusing the Kremlin of election interference in 2016 was overshadowed by the infamous "Access Hollywood" recording of President Donald Trump released the same day.[24]

In this way, indirect attacks provide the space for the United States to step down from the brink. There are many reasons that even a targeted state might prefer not to respond to an indirect attack; to avoid armed conflict, sidestep domestic political pains associated with state-to-state conflict, avoid associated economic burdens, and avoid legitimizing the transgressing country's forces as being worth confronting.[25] Not attributing attacks to a state gives the targeted state a diplomatic and political offramp. This is particularly applicable in the cases of implausible deniability, where it would be all too easy to challenge an attacking state's clearly false alibi. Often, the United States has the intelligence tools at its disposal to call out an attacking state, but it chooses not to, either to protect intelligence sources or to avoid escalation.

Indirect attacks, when viewed from this perspective, can take a more optimistic tone. While a threat, it is a preferred alternative to direct conflict that prevailed before the Cold War. It also suggests that a key imperative for U.S. strategists is not just how to hold rivals accountable for hostile indirect attacks but also how to do so while avoiding escalation to higher forms of conflict or political hazards. This can be a dangerous line to walk, especially when the public begins to rally around the need to respond to attacks by rivals. Cycles of escalation can take on a life of their own, cornering politicians into aggressive action that may build toward direct war.

Decision Space

Administrations leverage the decision space afforded by indirect attacks to pursue strategic or political imperatives, which often leads to de-escalation, as mentioned above, but can also allow for retaliation when needed. A case in point is the varying ways the United States has responded to hostile activities from Iran and Russia. Both states have supported attacks on U.S. forces in Iraq, Afghanistan, and Syria to include likely resourcing attacks that resulted in U.S. casualties. However, the differing ways the United States has responded to each attack demonstrates how indirect means give U.S. policymakers the maneuverability and flexibility to tailor their positions based on a calculus of the strategic and political imperatives of each attack individually and in the aggregate.

Iran has leveraged proxies against the United States extensively. An example is Iran's support for Hezbollah. At times, "Iranian officials played direct roles on different Hezbollah councils," and the armed wing of the proxy group "professed obeisance to Ayatollah Khomeini . . . and incorporated his decisions into their formal decision-making process."[26] Iran, in turn, continued to fund Hezbollah, and by 2010 "had hundreds of paramilitary forces in Lebanon" as well as Iraq.[27] A decade later, Iran's proxy attacks, including supporting direct attacks against U.S. troops in Iraq, would be a key justification for the killing of Iranian General Qasem Soleimani.[28] The day after Soleimani's death, President Trump warned that "[t]he Iranian regime's aggression in the region, including the use of proxy fighters to destabilize

Funeral of Qassem Soleimani killed in an American drone attack. Soleimani was an Iranian major general in the Islamic Revolutionary Guard Corps (IRGC)." (saeediex / Shutterstock.com, Jan 7, 2020)

its neighbors, must end and it must end now."[29] A majority of Americans supported Trump's decision to target Soleimani, demonstrating that indirect attacks provide the decision space to retaliate if policymakers are able to convince the public of the significance of the threat.[30] By contrast, after Iran attacked the world's biggest oil processing facility in Saudi Arabia in September 2019, Trump walked back earlier comments that the United States was "locked and loaded" to respond to the incident, saying it was "too early to know for sure" whether Iran was behind the incident and not offering any intelligence to prove Iranian culpability.[31] This approach gave the President the space to avoid retaliation after calculating that a war over oil markets would be too disruptive.

Russia is another example where the United States has at times taken a more measured position and other times escalated to advance its interests. While the United States responded aggressively to Wagner Group militias attempting to seize the Conoco gas field in eastern Syria in February 2018, more recently, the United States has conspicuously avoided any response to allegations that Russia provided incentives to Afghan fighters for the assassination of U.S. and coalition forces. There is little doubt Russia is actively working against U.S. interests in Afghanistan, though the scale of the support is still in question. However, the essential question becomes whether the United States should respond to these attacks, and how.

Russian activities against U.S. interests in Afghanistan would certainly arouse public ire if they were direct and explicit, potentially obligating U.S. political leaders to respond. Such a forced response would put U.S. decisionmakers into a corner. Indeed, after U.S. service members in Syria

were injured in skirmishes with Russian forces in August 2020, the United States was compelled to respond by redeploying troops to the area the following month. On the other hand, indirect attacks do not prevent U.S. retaliation; the United States could likely justify counteractions domestically, even based on incomplete information, if there was the will to do so among U.S. political leaders (as it did against Iran with the Soleimani strike or against Russian mercenaries in Syria). However, U.S. interests in Russia go beyond a single case, and different politicians may have unique political preferences for how to respond. The decision space provided by plausible deniability serves as an advantageous tool to avoid public demands for escalation while keeping the door open to do so.

A central deduction from these examples is that an individual indirect attack on its own does not need to dictate a cycle of escalation or a country's strategic approach to a region or bilateral relationship. When preferred, the targeted state can make plausible deniability implausible and respond with force; alternatively, it can choose to avoid escalation and, ideally, give itself space to resolve issues diplomatically. The key point is that indirect attacks present an opportunity, but it is up to policymakers to take advantage of such an opening to advance its strategic priorities through other tools.

Looking Forward

Concerns that the use of indirect attacks might disadvantage liberal democracies and incentivize them to adopt undemocratic and opaque policies to strengthen their position in geopolitical competition are misguided. Our analysis suggests that this mode of competition actually requires strengthening U.S. democratic principles rather than abandoning them. First, U.S. adversaries seek to exploit the deep polarization and mistrust in U.S. politics to advance their agendas, suggesting that efforts to build a more resilient, democratic society would also help undermine meddling by external actors. Second, by giving policymakers the space to respond deliberatively rather than capriciously, indirect attacks present an opportunity for liberal democracies to reduce tensions. Policymakers must seize this space to pursue diplomatic initiatives and to invest in tools for better understanding the systemic and cumulative effect of these indirect attacks in order to hold adversaries accountable, but without leading to escalation. In doing so, indirect attacks may actually reduce the level of conflict in the international system and reinforce the importance of democracy for peace in the world. PRISM

Notes

[1] National Security Strategy of the United States of America (Washington, DC: The White House, December, 2017), available at < https://www.hsdl.org/?view&did=806478>.

[2] Summary of the 2018 National Defense Strategy of the United States of America (Washington, DC: Department of Defense, 2018), available at < https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

[3] Sean Monaghan, "Countering Hybrid Warfare: So What for the Future Joint Force?" *PRISM* 8, no. 2 (2019), available at <https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf>.

[4] David Barno and Nora Bensahel, "Fighting and Winning in the 'Gray Zone'," *War on the Rocks*, May 19, 2015, available at <https://warontherocks.com/2015/05/fighting-and-winning-in-the-gray-zone/>.

[5] Graeme P. Herd, "Crimea as a Eurasian Pivot in 'Arc of Conflict': Managing the Great Power Relations Trilemma," in Violence and the State, Matt Killingsworth, Mathew Sussex, and Jan Pakulski, 2015, 107–127.

[6] Joshua P. Mulford, "Non-State Actors in the Russo-Ukrainian War," *Connections: The Quarterly Journal* 15, no. 2 (2016), 89–107; Herd, "Crimea as a Eurasian Pivot" in 'Arc of Conflict'," 107–127.

[7] Thomas Gibbons-Neff, "How a 4-Hour Battle Between Russian Mercenaries and U.S. Commandos Unfolded in Syria," *New York Times*, May 24, 2018. The United States reportedly had no casualties, while then-CIA director Mike Pompeo claimed the United States killed hundreds of Russians.

[8] Ivan Nechepurenko et al., "Dozens of Russians Are Believed Killed in U.S.-Backed Syria Attack," *New York Times*, February 13, 2018.

[9] Mujib Mashal and Michael Schwirtz, "How Russia Built a Channel to the Taliban, Once an Enemy," New York Times, July 13, 2020.

[10] "Wagner, Shadowy Russian Military Group, 'Fighting in Libya'," BBC, May 7, 2020, available at <https://www.bbc.com/news/world-africa-52571777>.

[11] "Top Russian Lawmaker Denies That Military Sent Warplanes to Libya," *Military Times*, May 27, 2020, available at <https://www.militarytimes.com/news/your-military/2020/05/27/top-russian-lawmaker-denies-that-military-sent-warplanes-to-libya/#:~:text=Top%20Russian%20lawmaker%20denies%20that%20military%20sent%20warplanes%20to%20Libya,-The%20Associated%20Press&text=MOSCOW%20%E2%80%94%20A%20senior%20Russian%20lawmaker,offensive%20on%20the%20capital%2C%20Tripoli>.

[12] Michele A. Flournoy, "Russia's Campaign Against American Democracy: Toward a Strategy for Defending Against, Countering, and Ultimately Deterring Future Attacks," in The World Turned Upside Down: Maintaining American Leadership in a Dangerous Age, Nicholas Burns et al. (Washington, DC: The Aspen Institute, 2017), 177–187.

[13] Ahmer Arif, Leo G. Stewart, and Kate Starbird, "Acting the Part," *Proceedings of the ACM on Human-Computer Interaction* 2, no. 20 (2018), 1–27.

[14] Ibid.; Jack Brown, "An Alternative War: The Development, Impact, and Legality of Hybrid Warfare Conducted by the Nation State," *Journal of Global Faultlines* 5, no. 1–2 (2018), 58–82.

[15] Craig Timberg, "Russian Hackers who stole DNC emails failed at social media. WikiLeaks helped," *Washington Post,* November 12, 2019.

[16] Sam Pudwell, "Putin Blames 'Russian Patriots' for Cyber Attacks on Foreign Elections," *Silicon.co.uk*, November 5, 2019. THE ONLY REFERENCE I CAN FIND FOR THIS IS THE FOLLOWING: Sam Pudwell, "Putin: 'Russian Patriots,' Not Government, Responsible for Foreign Election Cyber Attacks," *Silicon.co.uk*, June 2, 2017.

[17] Jake Wallis, "Twitter Data Shows China Using Fake Accounts to Spread Propaganda." Real Clear Defense, June 12, 2020, available at <https://www.realcleardefense.com/articles/2020/06/12/twitter_data_shows_china_using_fake_accounts_to_stoke_division_in_us_115374.html>.

[18] Oleksandr Danylyuk, "Protests, a Pandemic and Evidence of a Hybrid War," C4ISRNET, June 5, 2020, available at <https://www.c4isrnet.com/opinion/2020/06/05/protests-a-pandemic-and-evidence-of-a-hybrid-war/>.

[19] Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus, and Giroux, 2020), 11.

[20] *2017 National Security Strategy* (Washington, DC: The White House, 2017).

[21] Frank G. Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *PRISM* 7, no. 4 (November 2018), available at <https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/>.

[22] Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013).

[23] Candace Rondeaux, "De-Coding the Wagner Group: Analyzing the Role of Private Military Security Contractors in Russian Proxy Warfare," *New America,* November 7, 2019, available at <https://www.newamerica.org/international-security/reports/decoding-wagner-group-analyzing-role-private-military-security-contractors-russian-proxy-warfare/>.

[24] Brennan Weiss, "Obama's former Homeland Security Secretary says the 'Access Hollywood' tape overshadowed Russia's 2016 election interference," *Business Insider,* March 21, 2018, <https://www.businessinsider.com/jeh-johnson-says-access-hollywood-tape-overshadowed-russia-meddling-2018-3>.

[25] *Department of Defense Law of War Manual* (Washington, DC: Office of General Counsel, 2015), available at <https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190>.

[26] Daniel Byman and Sarah E. Kreps. "Agents of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism," *International Studies Perspectives* 11, no. 1 (2010), 1–18.

[27] Ibid.

[28] Nasser Karimi and Jon Gambrell. "Iran's Popular Gen. Soleimani Became an Icon by Targeting US," AP, January 3, 2020, available at <https://apnews.com/article/3bb7af59e8b1bfd3e15222a98395ee85>.

[29] Robert Burns, Lolita C. Baldor, and Zeke Miller, "Trump: Aim of Killing Iranian General Was to 'Stop a War'," AP, January 4, 2020, available at <https://apnews.com/article/2742111f6d0489313da688557d1123e8>.

[30] Scott Clement and Emily Guskin, "A slim majority of Americans approve of Trump's Soleimani strike," *The Washington Post*, January 28, 2020.

[31] Zachary Cohen, Kylie Atwood, and Ryan Browne, "Trump says it looks like Iran was behind Saudi oil field attack," CNN, September 16, 2019, available at <https://www.cnn.com/2019/09/16/politics/trump-saudi-oil-facility-attack-iran/index.html>.