The Role of Non-State Actors as Proxies in Irregular Warfare and Malign State Influence

Author: Sam Mullins

The Role of Non-State Actors as Proxies in Irregular Warfare and Malign State Influence

Author: Sam Mullins

March 2024

IRREGULAR WARFARE CENTER

www.IrregularWarfareCenter.org

Arlington, VA

Abstract

This paper explores the ways that states benefit from the activities of non-state actors (NSAs) as tools of irregular warfare (IW), with a particular focus on China and Russia. An examination of the historical relationships between state and non-state actors reveal that while proxies provide many potential advantages to their authoritarian patrons, they also present significant problems. The paper further demonstrates how China and Russia each utilizes a wide range of NSAs in a similarly broad spectrum of irregular warfare activities, including low-level persistent operations designed to erode adversaries' institutions over time, to much more kinetic operations that directly challenge the territorial integrity of other sovereign states. Implications for how to respond to these activities are discussed.

About the Author

Dr. Sam Mullins is a professor at the Daniel K. Inouye Asia-Pacific Center for Security Studies (DKI APCSS) in Hawaii. Previously, he was a professor of counter-terrorism at the George C. Marshall European Center for Security Studies in Germany, where he was awarded the Superior Civilian Service Award in March 2019. Dr. Mullins has spoken at numerous international conferences around the globe and has presented his work for a variety of government agencies including the FBI, the NYPD, the Canadian Security Intelligence Service, the Australian Federal Police, the International Special Training Centre in Germany, the NATO Centre of Excellence - Defence Against Terrorism institution in Turkey, the Chinese Ministry of Public Security, and the Indonesian National Armed Forces, among many others. He holds an MA (Hons) in Psychology from the University of Glasgow, Scotland; an MSc in Investigative Psychology, with distinction, from the University of Liverpool, UK; and a PhD from the University of Wollongong, Australia. He is the author of two books: *'Home-Grown' Jihad: Understanding Islamist Terrorism in the US and UK,* and *Jihadist Infiltration of Migrant Flows to Europe: Perpetrators, Modus Operandi and Policy Implications.*

* The author wishes to thank the Irregular Warfare Center's Michael Reese, Madison Urban, and Varsha Koduvayur for their helpful feedback, edits, and assistance in publication.

Table of Contents

Introduction

During the last decade or so, a growing international consensus has emerged that the boundaries between peace and war are becoming ever more blurred. States increasingly seek to compete with, coerce, and influence one another in ways that are widely perceived to be hostile, yet intentionally remain below the threshold of conventional war.[1] Although in some respects, this is nothing new—examples of everything from economic coercion to "fake news" can be found throughout history—such tactics have expanded and proliferated in the post-Cold War era as a result of increased globalization and advances in technology, along with the rising costs of war.[2]

Authoritarian, revisionist states like Russia and China, which have spearheaded the rise in so-called "gray-zone warfare," have also been driven by their fear of U.S. conventional military superiority. Moscow and Beijing have further demonstrated a growing sense of paranoia surrounding "color revolutions" in the former Soviet Union, and the "Arab Spring" uprisings against corrupt governments in the Middle East and North Africa. Over time, Russian and Chinese leaders came to view these events, not as legitimate manifestations of popular discontent, but as Western-orchestrated plots that amounted to a new way of warfare aimed at undermining and ultimately overthrowing autocratic regimes.[3] As a result, they have invested heavily in such tactics as disinformation, subversive economics, political interference, and use of proxies.

It is within this context that non-state actors (NSAs) have taken on an increasingly important role as tools of malign state influence. NSAs—from militant organizations to businesses and even individual citizens—have steadily grown in power and influence, thanks largely to the diffusion of technology. They also frequently operate in local social, economic, legal, and political systems. Depending on context, NSAs also enjoy significant freedom of movement internationally.[4] This provides them with unique forms of access and potential influence that states may not have, making them an attractive option to pursue certain foreign policy objectives. Thus, as the UK Ministry of Defence has observed, "[o]ld distinctions between 'peace' and 'war', between 'public' and 'private', between 'foreign' and 'domestic' and between 'state' and 'non-state' are increasingly out of date."[5]

Yet, despite the rapidly growing interest in gray-zone operations, irregular warfare (IW), and foreign interference, much of what we know about how states employ NSAs as tools of malign influence has tended to focus on *violent* non-state actors and proxy warfare, or, to a lesser degree, the use of "cyber mercenaries."[6] In addition to cases such as these, states routinely co-opt or otherwise exploit a wide variety of NSAs to exert political influence, including many which are non-violent and operate within the confines of the law.[7] However, different sorts of cases tend to be discussed separately to one another, and there has been insufficient effort to date to gain a more complete understanding of the range of NSAs that are employed by states for purposes of IW and malign state influence, the nature of their relationships with patron states, the types of activities they are involved in, or the specific sorts of challenges and opportunities they may present. This paper aims to improve our understanding of these issues, with a primary focus on the activities of China and Russia as the two most prolific practitioners of this particular form of statecraft in the world today.

The paper begins with a brief discussion of IW and malign state influence, which is fundamentally important for identifying what sort of activities may be considered politically unacceptable and thus where

NSAs may be contributing to hostile foreign agendas. The following section clarifies what is meant by the term "non-state actor" in this context and explores the varying relationships that exist with states, as well as the motivations of both parties, and associated risks and rewards. The next section draws upon the work of Lyle Morris and colleagues at the RAND Corporation to introduce a continuum of malign influence activities, ranging from kinetic operations to low-level non-kinetic activities.[8] Using this framework, the potential contribution of NSAs is discussed, demonstrating that non-state actors often represent the front line of malign state influence. The paper ends with a discussion of takeaways and considerations for how to respond to NSA political interference operations.

Irregular Warfare and Malign State Influence

While the intention here is not to get bogged down in definitional debates, some clarification of terminology is necessary. Within the U.S. Department of Defense, the most recent definition of irregular warfare describes it as "[a] form of warfare where states and non-state actors campaign to assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities."[9] According to the previously published summary of the Irregular Warfare Annex to the National Defense Strategy, irregular warfare "may employ the full range of military and non-military capabilities" to include such activities as use of proxy forces, disinformation, deception, economic coercion and covert operations.[10] By comparison, Title 50 of the United States Code defines "foreign malign influence" as "any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of a...foreign country with the objective of influencing, through overt or covert means," political, military, economic, or other policies or activities of the U.S. government or American public opinion.[11]

While the concepts of irregular warfare and malign state influence thus clearly overlap with one another, they are also complementary. The revised definition of irregular warfare helps to differentiate it from conventional forms of warfare, and thus provides a sense of where the upper limit of the gray-zone lies. The concept of malign state influence adds to this by drawing attention to mostly non-military activities, which may be pursued through overt as well as covert means, towards similar objectives.[12] More importantly still, it raises the question of what is "malign," "hostile" or otherwise goes beyond what is generally considered to be acceptable state behavior. In this way, it leads us to consider where the lower end of the gray-zone spectrum may be found.

A useful framework for thinking about and identifying problematic behavior in this context comes from Australia's Department of Home Affairs, which defines "foreign interference" (i.e. malign state influence) as "activity [that is] carried out by, or on behalf of, a foreign power, is coercive, corrupting, deceptive or clandestine, and contrary to [a targeted state's] sovereignty, values and national interests."[13] However, it is worth emphasizing that not all forms of malign state influence will necessarily clearly meet all of these criteria, and it can sometimes be difficult to judge whether a particular case qualifies or not. An alternative way of thinking about this problem, suggested by researchers Kristine Berzina and Etienne Soula at the Alliance for Securing Democracy, is simply in terms of transparency and intent.[14] The former succinctly covers both covert activities as well as those which are conducted out in the open yet are still somehow opaque. The latter may be determined not only by whether the activities in question are coercive or somehow corrupting, but also by the timing, coordination with other behaviors, and (potential) scale of effect.[15]

A final consideration, proposed by former British diplomat Charles Parton, is the question of reciprocity: *would we be allowed to conduct similar activities in the state that is responsible for conducting them in ours?*[16] Of course, there will always be a mismatch between relatively open versus closed, authoritarian systems of governance (and as Parton points out, liberal democracies should not forsake their values); however, this is a useful question to ask, in particular when assessing activities which are often highly ambiguous, may be exploiting legal loopholes, and where the ultimate intent is difficult to determine.

Non-State Actors and the State: Relationships and Motivations

Although there is no consensus definition of "non-state actor," broadly speaking, the term refers to individuals and entities that do not officially represent a government, but which nevertheless possess significant political, social, and/or economic influence.[17] It is important to recognize, however, that the lines between state and non-state actors are often blurred and sometimes exceedingly thin. This is especially the case in authoritarian regimes where the state exercises a far greater degree of control over the private sector and civil society than would be possible in a democracy.

What counts as an NSA is therefore a matter of degree. At one end of the spectrum, there are groups and individuals who largely operate autonomously, yet nevertheless sometimes have connections to and act in the interest of states. One example of this is Wikileaks and Julian Assange, who knowingly assisted Russian GRU military intelligence officers in disseminating sensitive information they had illegally obtained after hacking into the Democratic National Committee (DNC), which was clearly aimed at influencing the 2016 U.S. presidential elections.[18] In other cases, NSAs may be unwittingly manipulated by states into doing their bidding, as may be the case in some instances of elite capture, or, for example, where ordinary citizens are duped into sharing disinformation or protesting in the streets.

At the other end of the spectrum are quasi "non-state actors" that are partially integrated, and/or work in close coordination with state structures, at least some of the time; enjoy significant levels of state support (to include things like training, funding, and other resources); and are overseen and directed by government officials. Perhaps the best example of this is China's maritime militia, which consists of fishermen who retain their full-time civilian occupations, but are also trained and equipped by, and operate in coordination with, the People's Liberation Army Navy (PLAN) and Chinese Coast Guard (CCG).[19] The better trained militia units are even thought to receive generous salaries to the extent that they are no longer reliant on fishing as their primary source of income.[20] Furthermore, some individual militia members simultaneously hold positions in local government, which further complicates the picture.[21]

In order to account for this complexity, scholars have proposed a number of taxonomies to describe the varying relationships between patron states and their proxies.[22] Although they differ in their terminology, the key criterion in these models is the degree of command and control that the state is able to exercise, which corresponds to some degree to the level of resources that it is likely to provide. Simply put, NSAs

may be characterized as *autonomous*, *semi-autonomous*, or *state-directed*. These are waypoints on a dynamic spectrum of autonomy, and the relationships behind them are constantly evolving. As a result, NSAs may move up and down this sliding scale depending on changing circumstances.[23]

Of course, the true nature of relationships in this context is often deliberately obscured, and the amount of available information to be able to make a judgement is limited.[24] Nevertheless, seeking to understand and expose these connections to the extent it is possible will greatly assist with threat assessment, while furthermore helping to undermine some of the reasons why states turn to NSAs in the first place.[25] This is discussed in the following section.

State Motivations and Perceived Benefits of NSAs

Understanding state motivations and the perceived benefits of using NSAs is another essential step in making sense of their role as tools of malign influence and in looking for ways they might be countered. Perhaps the most commonly offered reason for why states choose to work through NSAs is deniability, which enables them to conduct activities or operations that might otherwise result in significant political costs. The extent to which deniability is actually plausible varies greatly, and in fact is often paper thin, particularly where overt actions are involved. Having NSAs do the dirty work may nevertheless reduce the extent to which states can be held accountable and limit the severity of any retaliation. Consider, for example, what might happen if Iranian soldiers, rather than their proxy militias, launched attacks on U.S. bases in Iraq? Proxies thus enable states to pursue limited objectives while avoiding escalation. As an added bonus, they may provide a "face-saving" mechanism in the event that they fail.[26]

Reducing the level of accountability may be thought of as one element in what Krieg and Rickli refer to as lessening the "burden of war." This refers to the collective costs of engaging in armed conflict (or more broadly, irregular warfare and malign state influence), which includes both domestic and international political costs, as well as strategic, operational, legal, and financial considerations.[27] For these authors, deniability has given way to *discretion* in the post-Cold War era, while domestic public opinion has emerged as the single most important factor which distinguishes contemporary versus historical use of surrogates.[28] This is likely to be particularly true in authoritarian states, which tend to obsess over internal state stability and arguably fear their own populations more than anything else.

This explains Russia and China's preoccupation with color revolutions and the heavy premium that they place on control of information. In Russia, for instance, leading military theorists have viewed the collapse of the Soviet Union, as well as difficulties experienced in the campaigns in Chechnya and Georgia, chiefly in *informational-psychological* rather than military terms.[29] This drove the Kremlin to tighten its control over the media during the second Chechen war in an attempt to insulate its population from what was happening in the warzone.[30] It may also partly explain Moscow's use of ostensibly private military companies (PMCs) such as the now-infamous Wagner Group, which emerged in 2014, since it does not

report PMC casualty numbers, which tend to be far higher than those of the regular military.[31] In effect, this hides the true costs of war and may have alleviated domestic pressures from groups such as the Committee for the Soldiers' Mothers of Russia, which, historically, has been a thorn in the Kremlin's side.[32]

Another key reason why states may choose to utilize NSAs for engaging in risky activities is the added ambiguity that they introduce to any given scenario. Indeed, ambiguity is widely seen as one of, if not *the* most important, defining feature of gray-zone operations, since it can complicate and delay responses, thereby giving aggressors additional time and space to pursue their objectives.[33] Where NSAs are involved in IW and malign state influence—whether it be irregular forces in eastern Ukraine, maritime militia in the South China Sea, or "private" businesses buying up property next to military installations—they increase ambiguity, both in terms of attribution and intent, and may thwart decisive action.[34]

NSAs are furthermore sometimes useful to states because of their unique skillsets or capabilities. Indeed, the GRU only turned to Wikileaks after its own attempts at distributing the information it had obtained failed to attract any attention.[35] It is also a key reason why states have turned to civilian (typically criminal) hackers to conduct operations in cyberspace. According to a U.S. Secret Service agent, commenting in 2014, "Many of the [non-state cyber] actors that we look at on a daily and weekly basis have capabilities that actually exceed the capabilities of most nation-states."[36]

Related benefits that NSAs bring to the table include *access* to places or people, along with an added sense of *credibility* and *legitimacy* that, depending on the circumstances, states may not have. Whether messages come from local power brokers; former, influential politicians; private businesses; media outlets; civil society organizations; youth groups; religious figures; social media influencers; or some other ostensibly independent entity, they are often likely to carry more weight than if they are perceived to come from foreign governments that are trying to advance a nefarious political agenda. Notably, perceptions of credibility and associated legitimacy, along with almost all of the other benefits of working through NSAs, are dependent on hiding or obscuring connections to the state. Again, it follows that if the relationship between patron state and proxy is exposed, it should help to undermine the value that NSAs provide.

NSA Motives and Problematic Behavior

It is important to understand why and how NSAs become involved in, and sometimes jeopardize or derail, state-backed IW and malign influence campaigns. In the context of proxy warfare, violent NSAs are typically keen to obtain badly needed resources, such as weapons and materiel, in order to achieve their objectives on the battlefield, which, naturally, must align with the geostrategic interests of states to some extent. The degree of mutual affinity may also be strengthened by shared ethnicity, religious beliefs, and/or political convictions.[37]

Mutual affinity is also important in understanding non-violent NSAs involved in subtler forms of malign influence, from propagandists to criminal hackers to wealthy businessmen who seek to buy political influence. Such individuals often appear to be driven, at least in part, by a genuine sense of patriotic nationalism. Yet, they also frequently stand to personally gain from their exploits. Take, for instance, Huang Xiangmo, a Chinese billionaire property developer with "very, very close" ties to the Chinese Communist Party (CCP), who was eventually declared *persona non grata* in Australia for having attempted to influence the country's politics.[38]

Throughout his time in Australia, Huang consistently spoke and acted in line with the Party's interests, making millions of dollars of political donations in the process, seemingly at his own expense. But under the CCP, these kinds of actions are rewarded with further business opportunities and other favors, meaning that self-interest almost always also plays a role.[39]

In other cases, the motivation may be more about self-preservation. Hinting at what is known to be a well-established practice, Oleg Gordievsky, the former head of the KGB office in London, once coyly admitted that "[o]ne man I know, who was caught committing a cyber crime, was given the choice of either prison or cooperation with the FSB and he went along."[40] Similarly, Russia allowed the Wagner Group to recruit thousands of convicted criminals to serve in Ukraine in return for pardoning their crimes.[41]

Others still may be drawn into malign influence activities through a careful process of social manipulation. For example, Huang's "star" recruit, then-Senator Sam Dastyari, was doubtlessly swayed by the hefty political donations, along with the lavish trips to China. Over time, it seems that he developed a profound sense of obligation and loyalty to Huang, along with a genuine, yet misguided, feeling of friendship. Thus, as the political crisis around him was deepening in October 2016—by which time he had been publicly accused by the Australian Prime Minister of taking "cash for comment" in support of Beijing—he went to Huang's home in Sydney to warn him that his phone was probably being tapped.[42] It was not until 2019 that Dastyari finally admitted that Huang may have been "directly, or indirectly, an agent of influence for the Chinese Government."[43]

Whatever their precise motivations and pathways into irregular warfare and malign state influence, even politically committed NSAs often remain fundamentally self-interested and maintain multiple interests and objectives, not all of which align with those of the state. Thus, despite all their advantages, they frequently engage in problematic behavior, which makes them a liability.[44] Continued involvement in criminality is a common example that is frequently seen among hackers in particular. Although both Russia and China are content to turn a blind eye to this, it provides opportunities for investigations and interdiction as well as strategic communications (more on this below).[45] Even Huang Xiangmo, who was quite sophisticated and already very wealthy, broke the law with some of his political donations and has been further accused of tax evasion.[46] It was also Huang's brazenness, alongside Dastyari's foolishness, that ultimately led the Australian government to ramp up its efforts to counter foreign interference and reconsider its relationship with China.

Because they are either relatively untrained, and/or to varying extents unregulated, it is commonplace for NSAs to engage in unprofessional and undisciplined conduct, which can undermine their legitimacy and effectiveness and/or expose their relationship with the state. This varies from "loose talk" about government support to committing war crimes and other human rights violations.[47] In extreme cases, NSAs can even turn directly against the state. This was demonstrated most dramatically by the Wagner Group's failed insurrection of June 2023, which saw Yevgeny Prigozhin's paramilitaries shoot down six helicopters and a Russian aircraft, briefly seize control of the strategically important city of Rostov-on-Don, and march to within 200km of Moscow, before aborting the plan and turning back.[48] Even China's tightly controlled maritime militia have reportedly been difficult to manage and have sometimes engaged in illegal fishing at times when it was expressly forbidden to avoid "causing trouble...and damaging China's international image."[49] From the perspective of countering NSA involvement in irregular warfare and malign state

influence, any such weaknesses or rifts in the relationship may present valuable opportunities that can potentially be exploited and should therefore be closely scrutinized.

The Non-State Actor Toolbox

In order to further comprehend this phenomenon, it is necessary to try and map out the broad "universe" of NSAs that are involved in irregular warfare and malign state influence, along with the different types of activities they are involved in. A useful starting point for organizing this analysis is Morris et al.'s scale of "gray zone activities," which distinguishes between three types, or levels, of effort: aggressive, moderate, and persistent.[50] Adapting this scale to maximize the degree of fit to the current focus on NSAs, the most important criteria for differentiating these levels are the degree to which the activity is: a) kinetic in nature; b) has a direct, discernible, and serious impact on national security; c) is attributable; and d) legal.[51]

More *aggressive* actions are more likely kinetic, have a direct, discernible impact, are often comparatively easy to attribute, and are at the same time often illegal. They may also be characterized as riskier, in terms of potentially provoking a robust, possibly even military response. *Moderate* activities, on the other hand, may or may not have a kinetic component, but still have some form of direct or potentially very serious impact on national security.[52] Attribution for actions at this level is still possible, though more difficult than for aggressive actions, while legality varies. Finally, *persistent* actions are a) non-kinetic and ongoing; b) challenging to attribute; c) often legal; and d) have an impact that is relatively difficult to discern. Of course, NSAs may conduct different sorts of activities at different times. However, using this framework to examine NSA behavior helps in gaining an appreciation of the range that are utilized by states, while clearly demonstrating that they are involved at all levels of irregular warfare and malign state influence. Given the complexity of these topics and constraints of space, the following discussions are intended to be illustrative, rather than exhaustive.

"Aggressive" NSAs

Perhaps the most aggressive use of NSAs as tools of political influence involves state sponsorship of terrorist and insurgent organizations. The most widely cited and clearly documented case of this today is Iran, which has made it a centerpiece of its foreign policy aimed at expanding influence in the Middle East and beyond.[53] Of course, Tehran is not alone in backing violent NSAs to advance its policies in the neighborhood, and the conflicts in Syria, Iraq, Libya, Yemen, and Israel and Palestine have given life to a resurgence of proxy warfare.[54] Russia has been deeply involved in Syria and Libya, in particular, where it has respectively worked alongside Hezbollah and other Iranian-backed proxies, and provided support to forces loyal to Libyan General Khalifa Haftar.[55] Elsewhere, Russia has cultivated and sponsored pro-Kremlin separatists in Crimea and eastern Ukraine and has harbored and allegedly directed some of the activities of the Russian Imperial Movement (RIM), which was named as a specially designated terrorist organization by the U.S. State Department in 2020 and is suspected of being behind a recent letter bomb campaign in Spain.[56]

Turning eastward, Pakistan and India have, over the years, both provided support to insurgents as part of their long-running feud with one another and more broadly as a means of exerting regional influence and

seeking to bolster their own security.[57] Meanwhile, although China, like Russia, has a history of supporting guerilla movements during the Cold War, Chinese support to militants largely dried up in the 1990s.[58] One apparent exception to this is Myanmar, where it retains significant influence over, and reportedly continues to provide material support to several ethnic armed groups—chiefly the powerful United Wa State Army (UWSA)—as a means of maintaining strategic leverage.[59] Some Indian commentators have furthermore suggested that China might provide support to insurgents in India's northeast, who operate along the border with Myanmar, but such claims have not been substantiated.[60] Separately, it has been alleged that Chinese mining companies are "bribing" (or, alternatively, being extorted by) Nigerian militants to be able to operate in the country.[61] Finally, the Democratic People's Republic of North Korea (DPRK) remains on the U.S. list of state sponsors of terrorism since being re-added by the Trump administration in November 2017. Ostensibly this was done in response to the assassination of Kim Jong-Un's half-brother in Malaysia earlier that year, although the move was widely seen to be a way of signaling Washington's broader displeasure with Pyongyang, and was not explicitly tied to allegations that North Korea had revived its historical practice of providing material support to non-state terrorist organizations.[62] Nevertheless, open source reporting suggests that, thanks to its relationship with Iran and Syria, this could indeed be the case, amid continued allegations that North Korean weapons have made their way into the hands of Palestinian militants, most notably Hamas.[63]

A second type of NSA that has been used to perform high-risk, kinetic missions is PMCs. Although this represents a growing, multi-billion dollar worldwide industry, Russia has distinguished itself for its uniquely subversive and reckless use of mercenaries. Russian PMCs have engaged not only in high intensity combat, the training of separatist militias, and the plundering of natural resources but also a range of other activities, including propaganda and disinformation campaigns.[64] In contrast to other developed nations, Russia has deliberately denied PMCs legal recognition, while turning a blind eye to repeated allegations of human rights abuses, war crimes, and other violations of international law.[65] In response to the Wagner Group rebellion, discussed above, Moscow appears to be reconsidering its approach to so-called "volunteer formations," and the future of PMCs in Russia is currently unclear.[66] Yet, given extensive PMC deployments across multiple continents (including Europe, Africa, Latin America, and Asia) and proven ability to serve the Kremlin's geostrategic goals and the financial interests of corrupt Russian elites, it seems unlikely they will be abandoned entirely.

In contrast to Russia, China's ban on PMCs appears to be genuine, and although it does make use of private *security* companies (PSCs), twenty of which operate abroad, they are officially prohibited from carrying firearms and instead play far more limited defensive roles, providing protection for projects along the Belt and Road.[67] In fact, by law, security firms in China must be at least 51% state-owned, meaning they do not strictly qualify as NSAs. However PSCs do train, collaborate, and proactively build relationships with various state and non-state entities in countries where they operate, including local security firms and militia.[68] This allows them to operate more effectively, while at the same time seeking to expand Chinese influence in competition with the United States.[69] Given that Chinese security contractors have, on several occasions, engaged in illegal activities, and their overseas footprint is only expected to grow, it is quite possible that such relationships could be leveraged for purposes of irregular warfare and malign state influence in future. It must nevertheless be emphasized that China's use of PSCs has so far been restrained.[70]

Beijing has relied rather more heavily on its maritime militia, which routinely engage in antagonistic and risky behaviors, to include such tactics as blocking, swarming, rafting together to create "semi-persistent floating outposts," and sometimes ramming other vessels.[71] To enable these activities, some militia ships are equipped with reinforced hulls and collision-absorbing rails, along with water cannons, while some also reportedly carry light weapons.[72] The net result is a formidable maritime force that, despite the problems noted above, has played a critical role in helping China to assert its territorial claims in the South and East China Seas.

A final example of NSA involvement in aggressive forms of irregular warfare and malign state influence is organized crime. In this respect, North Korea stands out as a "criminal state" that is both directly and indirectly involved in a range of organized criminal activities, including drug trafficking, counterfeiting, and cybercrime.[73] These activities are ultimately aimed at ensuring the survival of the regime, including strengthening its nuclear and conventional military capabilities, rather than necessarily being designed to directly weaken or undermine a targeted state.[74] Cyberattacks in particular may also be used for purposes of disruption, espionage, and intelligence gathering in support of interstate hostilities.

At present, Russia is most belligerent in its use of organized crime. This applies particularly to the Wagner Group, which was designated a transnational criminal organization by the U.S. Treasury Department in January 2023 for its "ongoing pattern of serious criminal activity," including the extortion of natural resources, mass executions, rape, child abductions, and physical abuse in the Central African Republic and Mali.[75] Other examples include the *Salem* and *Bashkaki* organized crime gangs, and the ultranationalist Night Wolves motorcycle club, which supported the illegal annexation of the Crimean peninsula, as well as the Donbass region of eastern Ukraine.[76] Additionally, Russia is thought to have mobilized organized crime figures on numerous occasions to carry out targeted assassinations of Moscow's enemies in Europe.[77] China is also suspected of employing organized criminals to conduct acts of political violence, albeit generally less severe, including the alleged use of gangsters to intimidate and sometimes violently suppress anti-Beijing protests in Hong Kong and Taiwan.[78] In the case of the latter, Bamboo Union triads affiliated with the fervently pro-Beijing China Unification Promotion Party (CUPP) were convicted for the attempted murder of an outspoken supporter of Taiwanese independence.[79]

"Moderate" NSAs

Besides using organized criminals as political muscle, states sometimes work with, or tolerate their activities in ways that are less directly aggressive, yet which may still be extremely damaging to others' national security over time. Based on complaints of weak regulation and inconsistent enforcement, as well as the political connections that Chinese gangsters around the world frequently seem to have, Beijing has been accused of being complicit in, and seeking financial and/or political gain from, the activities of organized criminals in the Americas, Europe, Southeast Asia and the Pacific islands.[80] To date, some of the clearest evidence of this has come from Europe, where officials at Chinese state owned banks have been convicted, and the banks heavily fined, for their role in facilitating the transfer of illicit cash flows, thought to be in the billions of euros every year, from Europe back to China.[81] Ironically, Chinese underworld figures in Italy and Spain were also reportedly involved in helping set up informal "police stations," which have

been used to monitor and control diaspora populations in coordination with authorities back in China.[82] Collectively, such arrangements benefit China economically and/or enable the expansion of political influence and control overseas, while undermining and weakening targeted countries.[83] It nevertheless remains exceptionally difficult to establish whether they result from deliberate policies, systemic corruption, or simply indifference.

Another area where attribution is notoriously difficult, and yet where states have quite clearly turned to NSAs for assistance as a matter of policy, is cyberspace. While most countries have developed their own, varying, in-house cyber capabilities, and a few, notably China and Iran, have further augmented this by establishing civilian cyber militia, authoritarian regimes continue to enlist criminal hackers to conduct online espionage, theft, and other activities in service of the state.[84] In the case of the DPRK, where public access to the internet and social media is tightly restricted, the line between state and NSA is virtually non-existent, making it nearly impossible to distinguish between official and unofficial state employees. Nevertheless, North Korean hackers do sometimes utilize outside criminal services to perform tasks such as money laundering in support of their operations.[85]

While still shrouded in secrecy, Russian and Chinese approaches to co-opting cybercriminals have been slightly less opaque. Russia initially began recruiting cybercriminals in order to boost the capabilities of its security services, particularly the FSB, during the 1990s and has continued the practice since.[86] In so doing, Russian authorities have given some of these individuals official positions, while at the same time utilizing their informal criminal networks outside of formal state structures and have generally turned a blind eye to continued criminality, as long as it is targeted abroad.[87] Though not without their problems, criminal hackers have thus contributed to some of Russia's highest profile cyber operations, including the theft of information from over half a billion Yahoo accounts in 2014 as well as the hack of the Democratic National Convention in 2016.[88]

Criminal/patriotic elements furthermore played a role in significant distributed denial of service (DDoS) attacks against Estonia in 2007, Georgia in 2008, and, to a lesser degree, in cyberattacks against Ukraine (noting that CyberBerkut, an infamous online group that attempted to sabotage the Ukrainian parliamentary elections and was once thought to consist of non-state hacktivists is, according to the U.K.'s National Cyber Security Centre, "almost certainly" operated by the GRU).[89]

China meanwhile has adopted a strikingly similar (albeit slightly less coercive) approach to working with cyber-criminals, as exemplified by the case of Tan Dailin and the group known as Advanced Persistent Threat (APT) 41, who performed contract work on behalf of the Ministry of State Security (MSS).[90] Together, they were responsible for long running espionage and parallel criminal conspiracies which impacted more than a hundred entities and individuals around the world, including Australia, Brazil, Chile, Hong Kong, India, Indonesia, Japan, Malaysia, Pakistan, Singapore, South Korea, Taiwan, Thailand, Vietnam, the United Kingdom, and United States.[91]

A very different but potentially even more serious threat comes in the form of legal private enterprise. Here, the primary concern is that Chinese companies especially, some of which are state-owned but others such as Huawei that are ostensibly independent, are investing in other countries' critical national infrastructure, systematically acquiring cutting edge and dual-use technologies, or seeking to buy property in the vicinity of military and other sensitive installations.[92] Although the role of the state is often unclear, the concern is

that such actions increase the risk of espionage, confer unfair economic advantage, contribute to China's Military-Civil Fusion strategy—which seeks to enhance the capabilities of the People's Liberation Army (PLA)—or otherwise provide strategic leverage.[93] China's National Intelligence Law of 2017, which compels all Chinese citizens and organizations to cooperate with intelligence work, has added to these fears.[94]

A final example of "moderate" malign state influence that is typical of China's playbook in particular, involves wealthy overseas patriots known as "Red Capitalists," like the previously described case of Huang Xiangmo in Australia. Similar cases have been documented in Canada and New Zealand, and related concerns have been raised in Southeast Asia.[95] Though ostensibly independent, such individuals typically have close ties to the Chinese government, occupy leading positions within United Work Front Department (UWFD) affiliated bodies in the country in question, and can be relied upon to use their wealth to cultivate political influence.[96] As we saw, one of the most important ways that they do this is through "elite capture"—befriending and effectively recruiting politicians and other influential figures who then become reliable supporters of the CCP and its interests. Red Capitalists are furthermore able to use their wealth and status to mobilize diaspora communities and provide funding for additional projects, such as cultural events and educational institutions, which can also be leveraged in support of the CCP's strategic aims. In Huang's case, it is alleged that his efforts contributed to Australia's decision to sign a controversial free trade agreement with China in 2015, while in Canada it remains an open question as to whether Chinese interference succeeded in influencing the outcome of the 2021 federal election.[97]

Wealthy Russians with ties to the Kremlin have similarly made large donations, or otherwise helped finance favored political candidates in several countries, including the United States, the United Kingdom, and France, and have lobbied against legislation or policies unfavorable to Moscow, albeit with limited success.[98]

"Persistent" NSAs

As a daily, ongoing occurrence with unclear effects, online disinformation can generally be regarded as a "persistent" threat. Although, when it is aimed at influencing the outcome of elections it must still be treated extremely seriously. By far the most well-known example of NSA involvement in online political interference is Russia's Internet Research Agency, which was established by Yevgeny Prigozhin in 2013 and became infamous for its attempts at manipulating multiple U.S. elections, beginning in 2016. Yet despite some successes, such as being able to reach millions of people online and organizing a few small protests on American streets, it "worked more like a spammy call center than a tight intelligence agency" and "unlikely... had any discernible effect on the voting behavior of American citizens."[99] The Internet Research Agency nevertheless persists, while smaller Russian-funded "troll farms," which have primarily targeted the United States, have been discovered as far afield as Ghana and Nigeria.[100] Including the United States, Russia has been accused of using cyber-enabled foreign interference tactics against 31 elections and 7 referendums in 26 states, including in Europe, Africa, and Indonesia.[101] Although it is unclear to what extent NSAs were involved in these particular operations, paid local influencers (some with connections to the Wagner Group) appear to be a regular component of Moscow's ongoing disinformation operations.[102] More broadly, there is an extremely active online network of pro-Russian "trolls," who routinely spread disinformation and viciously attack critics of the Kremlin.[103]

China also engages in online disinformation and has reportedly used cyber capabilities to try to interfere in elections in the United States, Taiwan, Vietnam, Indonesia, Malaysia, and Australia. However, again it is unclear to what extent NSAs were utilized.[104] In one instance, Chinese actors using fake online profiles helped generate support for the successful pro-Beijing Taiwanese mayoral candidate Han Kuo-yu in Kaohsiung by tirelessly promoting him on Facebook while at the same time spreading fake news to discredit his opponent.[105] Some analysts believe this was the work of a private team contracted by a Chinese company working on behalf of the CCP, though others attribute it directly to the PLA's Strategic Support Force (SSF).[106] The truth, however, is unknown. What is known more generally is that the CCP has been supported online by independent patriotic "netizens" as well as paid online commentators.[107] More recently, the internet security firm Mandiant reported that China appears to be increasingly turning to Chinese public relations firms, specifically Shanghai Haixun Technology, to conduct information operations on its behalf.[108] Similarly, researchers at the Australian Strategic Policy Institute (ASPI) have exposed a pro-Beijing influence-for-hire industry operating out of Southeast Asia with connections to organized crime.[109] These campaigns have targeted audiences in North America, Europe, the Middle East, Asia, and Australia, and have sought, not only to promote a positive image of China, but also to sow disinformation and social unrest.[110] Haixun Technology is further suspected of financing two small in-person protests in Washington DC, however, the campaign overall was judged to be of limited success.[111]

Outside of cyberspace, both China and Russia have used a variety of techniques to co-opt, infiltrate, or otherwise exploit a range of overseas traditional media organizations, educational institutions, civil society, and religious groups. Very often these activities are legal and are difficult to identify and respond to. For example, China is reported to have used a combination of inducements and punishments to quietly buy controlling stakes in previously independent Chinese media outlets in Australia and New Zealand in order to establish a monopoly on the flow of information.[112] Chinese state-run media have also paid major foreign news providers—including Australia's Fairfax Media, Sky News, and the UK's *Daily Telegraph*—to reproduce Chinese propaganda and give CCP officials a mainstream platform to promote their political agenda.[113] In the Solomon Islands, the *Solomon Star* newspaper pledged to "promote the truth about China's generosity and its true intentions" after it received a generous donation of funds and equipment from the Chinese embassy.[114] Another deal with Palau's oldest newspaper and a "Chinese business group with links to national security institutions" was aborted.[115] Separately, within the education sector, Chinese embassy and consular officials provide funding and guidance to Chinese Students and Scholars Associations (CSSAs) around the world, using them to encourage students to report on "dissident" peers, to mobilize them for political protests, and to attempt to shut down speakers or events that are offensive to the CCP, such as the Dalai Lama, Uighurs, and Falun Gong practitioners.[116] In addition, academic exchanges and partnerships with universities can be leveraged to gain access to cutting-edge dual-use technologies and in several instances have been shown to benefit the PLA.[117] Finally, the UFWD also targets Chinese civil society organizations, including churches, in order to further expand Party influence over diaspora populations and have them serve its interests.[118]

By comparison, Russia's efforts appear to be less systematic though it too has exploited a wide array of societal institutions. For example, Putin supporters, some with at least indirect connections to Russian intelligence services, have published dozens of articles in the culture section of Sweden's *Aftonbladet* newspaper which parrot the Kremlin's narratives on Ukraine, NATO, and the EU, while also repeatedly

attacking academics working to expose Russian influence operations.[119] Russian billionaire oligarchs, whose vast wealth typically comes from corruption, have donated millions of dollars to educational, cultural, and political institutions in the United States and Europe aimed at "launder[ing] their reputations and gain[ing] access to American and European high society."[120] In one instance, the FBI warned that "[t]he [Skolkovo] foundation [which partnered with the Massachusetts Institute of Technology from 2011–2022] may be a means for the Russian government to access our nation's sensitive or classified research development facilities and dual-use technologies with military and commercial application."[121] Russia furthermore seeks to influence, exploit, and mobilize ethnic Russians living abroad in pursuit of foreign policy objectives. Drawing on a playbook that dates back to the Soviet era, the Kremlin and its supporters have been accused of orchestrating pro-Russian demonstrations of varying size and intensity in numerous countries including Estonia, Germany, Ukraine, and Moldova, and have benefited from the political support of certain branches of the Orthodox Church in Ukraine, Montenegro, and Serbia.[122]

Collectively, these activities enable China and Russia to censor or manipulate information beyond their borders. They also allow them to monitor, influence, and mobilize ethnic Chinese and Russian populations living abroad. Finally, they allow both Russia and China to gain access to critical technologies needed to advance both economically and militarily. In so doing, they undermine the sovereignty and national interests of targeted states.

Concluding Remarks

As the preceding discussion has shown, China and Russia differ somewhat in their approach to using NSAs as tools of irregular warfare and malign state influence with Beijing favoring a subtler, mostly non-violent approach while Moscow is much more willing to use lethal force. Nevertheless, each utilizes a wide range of NSAs, which vary in their degree of autonomy, at every level of irregular warfare and malign state influence from low-level persistent activities, which gradually erode institutions over time, to much more kinetic operations that directly challenge the territorial integrity of targeted states. This presents both challenges and opportunities. On the one hand, NSAs add ambiguity, complicate attribution, and insulate states from their actions. They also frequently exploit legal and regulatory loopholes and are often able to advance state objectives while conferring a sense of legitimacy. Based on how extensively they are used, it is obvious that Russia and China view NSAs as valuable assets, and it seems unlikely they will be easily dissuaded or deterred from using them. On the other hand, NSAs are also frequently a liability. They inevitably have their own interests and goals, which often do not align with those of the state. They regularly engage in criminality and other unprofessional conduct that makes them vulnerable to investigation and punitive actions, and this is damaging both to themselves as well as their patron state.

Recognizing that each case is unique, responses will need to be carefully tailored, taking into account the type of activity, level of autonomy, and the specific legal and regulatory frameworks available. In making this analysis, a critical first step should be to identify the motivations and objectives of both the state and NSA in question, in order to understand the specific benefits that each party seeks to derive, and to what extent their interests align. Special attention should be given to points of divergence or conflicting interests which

might be exploited. At the same time, it must be recognized that relationships are constantly evolving, and so authorities tasked with defending against and responding to irregular warfare and malign state influence must be acutely attuned to changing dynamics and emerging rifts and be prepared to quickly react.

As a general principle, NSAs are likely to be most useful as tools of irregular warfare and malign state influence when they are able to advance state interests while simultaneously making them less accountable for their actions, in particular to their domestic populations and other key audiences whose opinion they value. Defending states should therefore work to expose relationships between patron states and proxy NSAs to the greatest extent possible and furthermore find ways of effectively communicating this to audiences that matter. Although this is unlikely to lead to an immediate cessation of activity by itself, together with other measures (such as targeted sanctions, or official designations as agents of a foreign government, it should theoretically devalue the NSA in question and negatively impact their ability to operate, while imposing reputational costs on the state. This, in effect, is the core argument for "naming and shaming": the idea that exposing the unacceptable activities of states like China and Russia will ultimately deter them from continuing down this path.

Some officials and experts have concluded that naming and shaming has failed.[123] This assumes, first of all, that a reduction or cessation of malign activity is the only objective. Secondly, that efforts to date have been communicated effectively to the right audiences. However, besides impacting China and Russia directly, an intermediate objective of naming and shaming should be to encourage allies and partners to have the courage to expose similar activities within their borders as a means of gradually building international pressure. More could be done to encourage this. In addition, existing legal mechanisms for identifying and designating ostensible NSAs as agents of a foreign state have been criticized in several countries on multiple grounds.[124] Such legislation should be re-examined with a view to making it more dynamic, preferably including the ability to recognize state and non-state relationships as a continuum, rather than all-or-none, while at the same time ensuring it cannot be abused. [125] Finally, the way that information about irregular warfare and malign state influence is communicated and shared could be greatly improved. For instance, U.S. indictments of state-sponsored hackers are periodically made public, dutifully accompanied by a press release from the Department of Justice. Yet this is currently done on a sporadic case-by-case basis, with little effort to create a coherent overarching narrative that would demonstrate the scale, interconnectedness, and impact of these activities, including for foreign partners. This could be addressed relatively easily, for example, by creating an open access foreign interference portal that served as a database of all relevant cases, with readily available statistics and graphics to help illustrate activity geographically and over time. Ideally, this would be available in multiple languages. Universities, think tanks, and journalists would be able to analyze these data, produce new insights and further amplify the message.

Finally, defending states must recognize that just as NSAs are on the front line of irregular warfare and malign state influence, all too often they are also the immediate victims and therefore the first line of defense. Authorities can boost their capabilities in the first instance simply by raising awareness and assisting with the design of regulatory responses (as, for example, with the University Foreign Interference Taskforce in Australia).[126] In turn, NSAs, including open-source intelligence firms, internet security companies,

think tanks, and others, can and do play key roles in exposing malign state influence. States should seek to regularly engage these actors and harness their capabilities while ensuring they are protected from any form of retaliation.

This paper sought to demonstrate the ways in which authoritarian states, in particular China and Russia, make use of or otherwise stand to benefit from the actions of NSAs at all levels of irregular warfare and malign state influence. Though far from comprehensive, it is obvious from this discussion that NSAs form an indispensable and important component of these states' strategies to weaken and gain advantage over their opponents. Nevertheless, there is a great deal of room for further research. Much of the activity in question that we know about has been directed against the United States and its Western allies. Partly, this is because they are China and Russia's main adversaries and so naturally tend to be targeted. Partly, it is because some, notably Australia and Canada, have recently awoken to what has been happening in their societies and have thus brought more activities to light than others. However, it is almost certainly also a product of missing information about malign activities that are happening elsewhere. Much more needs to be done to expose and document Chinese, Russian, and wider use of irregular warfare and malign state influence within Asian and Pacific countries, in particular, about which comparatively little is known, especially as it relates to NSAs operating below the "aggressive" level.[127] Fundamentally, as referenced above, much more needs to be done to compile systematic databases of irregular warfare and malign state influence activities that would enable deeper understanding of how these efforts combine as a coordinated whole.

Further research examining counter-strategies used against NSAs would also be beneficial, particularly exploring the impact of different approaches to naming and shaming, which seek to expose relationships between patron states and their non-state proxies. Since NSAs differ in motivations, level of autonomy, and the type of activities they are involved in, these variables must also be accounted for. For example, NSAs that are highly nationalistic, state-directed, and aggressive would unlikely be easily dissuaded or deterred, suggesting that direct, punitive and sometimes even kinetic counter-measures would be most appropriate. By contrast, NSAs that are primarily self-interested, relatively autonomous, and less aggressive might be more vulnerable to informational or administrative interventions. Ideas such as these should be explored.

Although the phenomenon of states using NSAs for purposes of irregular warfare and malign state influence is certainly not new, it appears to have grown in significance as revisionist powers seek to take advantage of new opportunities that have arisen in the aftermath of the Cold War. Historically, as great power competition has intensified, so too has the tendency toward proxy war.[128] If this has any bearing on the current geopolitical context, taking into account contemporary modes of "warfare," NSAs may play an even greater role in future. Yet, our knowledge of this shadowy form of statecraft remains fragmented and incomplete. The more we are able to shed light on it, the more likely we will be able to blunt its impact and appeal.

Endnotes

1 See Elisabeth Braw, *The Defender's Dilemma: Identifying and Deterring Gray-Zone Aggression* (Washington, DC: American Enterprise Institute, 2022); Mark Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War* (New Haven and London: Yale University Press, 2022).
2 Ibid.
3 Rush Doshi, *The Long Game: China's Grand Strategy to Displace American Order* (New York: Oxford University Press, 2021); "GT Investigates: US wages global color revolutions to topple govts for the sake of American control" *The Global Times*, December 2, 2021, https://www.globaltimes.cn/page/202112/1240540.shtml; Oscar Jonsson, *The Russian Understanding of War: Blurring the Lines Between War and Peace* (Georgetown University Press, 2019);
4 National Intelligence Council, *Nonstate Actors: Impact on International Relations and Implications for the United States* (Federation of American Scientists Intelligence Resource Program, 2007) https://irp.fas.org/nic/nonstate_actors_2007.pdf.
5 Ministry of Defence, *Integrated Operating Concept* (Bristol: UK Ministry of Defence, 2021), p.5 https://www.gov.uk/government/publications/the-integrated-operating-concept-2025.
6 See, for example: Andreas Krieg and Jean-Marc Rickli, *Surrogate Warfare: The Transformation of War in the Twenty-First Century* (Washington, DC: Georgetown University Press, 2019); Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018); Magnus Normark, *How States Use Non-State Actors: A Modus Operandi for Covert State Subversion and Malign Networks* (Helsinki: European Centre of Excellence for Countering Hybrid Threats, 2019), https://www.hybridcoe.fi/wp-content/uploads/2020/07/HybridCoE_SA_15_Non-state-Actors.pdf; Stephen Watts et al., *Proxy Warfare in Strategic Competition: State Motivations and Future Trends* (Santa Monica, CA: RAND Corporation, 2023), https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA307-2/RAND_RRA307-2.pdf.
7 See, for example: Jessikka Aro, *Putin's Trolls: On the Frontlines of Russia's Information War Against the World* (New York: IG Publishing, 2022); Braw, *The Defender's Dilemma*; Galeotti, *The Weaponisation of Everything;* Clive Hamilton, *Silent Invasion: China's Influence in Australia* (Melbourne: Hardie Grant Books, 2018); Stacie L. Pettyjohn and Becca Wasser, *Competing in the Gray Zone: Russian Tactics and Western Responses* (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2791/RAND_RR2791.pdf.
8 Lyle J. Morris et al., *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War* (Santa Monica, CA: RAND Corporation, 2019), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2942/RAND_RR2942.pdf.
9 Patrick Tucker, "As irregular warfare comes to a crossroads, Congress chips in," *Defense One*, December 17, 2023, https://www.defenseone.com/policy/2023/12/irregular-warfare-comes-crossroads-congress-chips/392821/.
10 *Summary of the Irregular Warfare Annex to the National Defense Strategy* (Washington, DC: United States Department of Defense, 2020), https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF.
11 U.S.C. 50, War and National Defense, 44, §3059, accessed July 12, 2023, https://uscode.house.gov/view.xhtml?req=(title:50%20section:3059%20edition:prelim)#:~:text=The%20term%20%22foreign%20malign%20influence,through%20overt%20or%20covert%20means%2D.
12 While the latest definition clearly alludes to the fact that irregular warfare can be conducted for legitimate reasons (i.e., to assure, rather than coerce states or other groups), the focus of this paper is on activities conducted with hostile intent.
13 "Defining foreign interference" *Department of Home Affairs*, undated, accessed July 12, 2023, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/defining-foreign-interference.
14 Kristine Berzina and Etienne Soula, "Conceptualizing Foreign Interference in Europe", March 18, 2020, *Alliance for Securing Democracy*, https://securingdemocracy.gmfus.org/wp-content/uploads/2020/03/Conceptualizing-Foreign-Interference-in-Europe.pdf.
15 Ibid.
16 Charles Parton, *China-UK Relations: Where to Draw the Border Between Influence and Interference?* (London: Royal United Services Institute for Defence and Security Studies, 2019), https://static.rusi.org/20190220_chinese_interference_parton_web.pdf.
17 National Intelligence Council, *Nonstate Actors: Impact on International Relations and Implications for the United States*.
18 Eduard Kovacs, "Senate: WikiLeaks Knowingly Assisted Russian Influence Effort Before 2016 Election" *Security Weekly*, August 19, 2020, https://www.securityweek.com/senate-wikileaks-knowingly-assisted-russian-influence-effort-2016-election/.
19 Shuxian Luo and Jonathan Panter, "China's Maritime Militia and Fishing Fleets: A Primer for Operational Staffs and Tactical Leaders," *Military Review*, January-February 2021, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JF-21/Panter-Maritime-Militia-1.pdf.
20 Conor Kennedy and Andrew Erickson, "China Maritime Report No. 1: China's Third Sea Force, The People's Armed Forces Maritime Militia: Tethered to the PLA," *China Maritime Studies Institute*, March 2017, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1000&context=cmsi-maritime-reports.
21 Masaaki Yatsuzuka, "How China's maritime militia takes advantage of the grey zone," Australian Strategic Policy Institute, January 16, 2023, https://www.aspistrategist.org.au/how-chinas-maritime-militia-takes-advantage-of-the-grey-zone/.
22 See, for example, Krieg and Rickli, *Surrogate Warfare*; Maurer, *Cyber Mercenaries*.
23 Krieg and Rickli, *Surrogate Warfare*; Maurer, *Cyber Mercenaries*.
24 Note that it is frequently difficult, if not impossible, to distinguish genuine NSAs from undercover intelligence operatives or covertly run front organizations and it is likely that the two worlds are frequently (and deliberately) intertwined. A key difference is that NSAs are not professionals, and are more likely to have their own, separate agendas, which may not always align with the interests of the state.
25 See Normark, *How States Use Non-State Actors*.
26 See Austin Carson, *Secret Wars: Covert Conflict in International Politics* (Princeton, NJ: Princeton University Press, 2019).
27 Krieg and Rickli, *Surrogate Warfare*.
28 Ibid, 125-126.

29 Jonsson, *The Russian Understanding of War*, ch.3.
30 Ibid.
31 Seth Jones et al., *Russia's Corporate Soldiers: The Global Expansion of Russia's Private Military Companies* (Washington, DC: Center for Strategic and International Studies, 2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210721_Jones_Russia%27s_Corporate_Soldiers.pdf?VersionId=7fy3TGV3HqDtRKoe8vDq2J2GGVz7N586; Kimberly Marten, "Russia's Use of Semi-State Security Forces: the Case of the Wagner Group," *Post-Soviet Affairs* 35, no.3 (2019): 181–204.
32 Jennifer Mathers and Natasha Danilova, "The Ukraine war and Russian soldiers' mothers" *Social Europe*, January 10, 2023, https://www.socialeurope.eu/the-ukraine-war-and-russian-soldiers-mothers#:~:text=One%20of%20Russia%27s%20best%2Dknown,the%20rights%20of%20conscripted%20soldiers.
33 Braw, *The Defender's Dilemma*; Javier Jordan, "International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict", *Journal of Strategic Security* 14, no. 1 (2020): 1–24; Andrew Mumford and Pascal Carlucci, "Hybrid Warfare: The Continuation of Ambiguity by Other Means", *European Journal of International Security* 8, no. 2 (2022): 192–206.
34 Note, however, that this is not always necessarily the case. Focusing on use of violent NSAs in proxy warfare, Jonathan Wilkenfeld and colleagues at the University of Maryland found that proxy usage often leads to violence escalation (though this typically seems to be directed against the proxy, rather than the sponsoring state, and so may still be beneficial). See Jonathan Wilkenfeld et al., "Escalation Management in Gray Zone Crises: The Proxy Factor," *International Studies Quarterly*, 66 (2022): 1–14.
35 Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Picador, 2020), ch.28.
36 Kevin Cirillia, "Hackers Have Powers Beyond Most Countries, Expert Says," *The Hill*, October 20, 2014, cited in Maurer, *Cyber Mercenaries*, x.
37 Krieg and Rickli, *Surrogate Warfare*, ch.5.
38 Ben Doherty and Helen Davidson, "Huang Xiangmo: alleged agent of Chinese influence exiled from Australia now on Hong Kong electoral body," *The Guardian*, October 19, 2021, https://www.theguardian.com/australia-news/2021/oct/20/huang-xiangmo-alleged-agent-of-chinese-influence-exiled-from-australia-now-on-hong-kong-electoral-body; Hamilton, *Silent Invasion*, ch.4; Fergus Hunter, "Sam Dastyari quits key parliamentary positions after more damaging China revelations," *The Sydney Morning Herald*, November 30, 2017, https://www.smh.com.au/politics/federal/sam-dastyari-quits-key-parliamentary-positions-after-more-damaging-china-revelations-20171130-gzvl0l.html..
39 Anne-Marie Brady, *Magic Weapons: China's political influence activities under Xi Jinping* (Washington, DC: Wilson Center, 2017), 17, https://www.wilsoncenter.org/sites/default/files/media/documents/article/magic_weapons.pdf; Hamilton, *Silent Invasion*, 55.
40 Maurer, *Cyber Mercenaries*, 96.
41 "Russia's Wagner mercenaries halt prisoner recruitment campaign – Prigozhin," *Reuters*, February 9, 2023, https://www.reuters.com/world/europe/russias-wagner-mercenaries-halt-prisoner-recruitment-campaign-founder-prigozhin-2023-02-09/.
42 Hamilton, *Silent Invasion*, ch.4; Nick McKenzie, James Massola, and Richard Baker, "Labor senator Sam Dastyari warned wealthy Chinese donor Huang Xiangmo his phone was bugged," *The Sydney Morning Herald*, November 29, 2017, https://www.smh.com.au/politics/federal/labor-senator-sam-dastyari-warned-wealthy-chinese-donor-huang-xiangmo-his-phone-was-bugged-20171128-gzu14c.html..
43 Tom Rabe, Kate McClymont, and Alexandra Smith, "Dastyari, ICAC and the Chinese 'agent of influence,'" *The Sydney Morning Herald*, August 29, 2019, https://www.smh.com.au/politics/nsw/dastyari-icac-and-the-chinese-agent-of-influence-20190829-p52m6e.html.
44 Krieg and Rickli, *Surrogate Warfare*, ch.5; Watts et al., *Proxy Warfare in Strategic Competition*.
45 Maurer, *Cyber Mercenaries*, ch.6–7.
46 Rabe, McClymont, and Smith, "Dastyari, ICAC and the Chinese 'agent of influence.'"
47 See, for example: "CAR: Russian Wagner Group harassing and intimidating civilians – UN experts," *UN Human Rights Office of the High Commissioner*, October 27, 2021, https://www.ohchr.org/en/press-releases/2021/11/car-russian-wagner-group-harassing-and-intimidating-civilians-un-experts; "The people behind Chengdu 404," *Intrusion Truth*, July 23, 2022, https://intrusiontruth.wordpress.com/2022/07/23/the-people-behind-chengdu-404/.
48 "Assessing the Wagner Group's Aborted Run on Moscow: What Comes Next?," *International Crisis Group*, June 29, 2023, https://www.crisisgroup.org/europe-central-asia/caucasus/russia-internal/assessing-wagner-groups-aborted-run-moscow-what-comes.
49 Xia Zhangying, *Nansha qundao yuyeshi* [A history of fisheries in the Nansha Islands] (Bejing: Haiyang chubanshe, 2011), 209–13, cited by Luo and Panter, "China's Maritime Militia and Fishing Fleets" 14–15.
50 Morris et al, *Gaining Competitive Advantage in the Gray Zone*.
51 These criteria are derived from Morris et al's description of each level of activity. However, their version differs slightly in its inclusion of military (i.e., state) activities; a preoccupation with whether there is a threat to territory; and in their focus on the South China Sea. The adapted scheme presented here is closely comparable to the original, but, in this author's assessment, more accurately categorizes the activities of NSAs in irregular warfare and malign state influence.
52 Note that this differs slightly from Morris et al's description of this level, which they see as involving "direct action, though often in non-military form" to include such actions as cyber-attacks and economic coercion (Morris et al, *Gaining Competitive Advantage in the Gray Zone*, 137).
53 Krieg and Rickli, *Surrogate Warfare*, ch.7; Watts et al., *Proxy Warfare in Strategic Competition*, ch.6.
54 Emadeddin Badi, "Russia Isn't the Only One Getting Its Hands Dirty in Libya," *Foreign Policy*, April 21, 2020, https://foreignpolicy.com/2020/04/21/libyan-civil-war-france-uae-khalifa-haftar/; Frank Hoffman and Andrew Orner, "The Return of Great-Power Proxy Wars," *War on the Rocks*, September 2, 2021, https://warontherocks.com/2021/09/the-return-of-great-power-proxy-wars/.
55 "Exploiting Chaos: Russia in Libya," *Center for Strategic and International Studies*, September 23, 2020, https://www.csis.org/blogs/post-soviet-post/exploiting-chaos-russia-libya; Nicole Grajewski, "The Evolution of Russian and Iranian Cooperation in Syria," *Center for Strategic and International Studies*, November 17, 2021, https://www.csis.org/analysis/evolution-russian-and-iranian-cooperation-syria.
56 Edward Wong, Julian Barnes, and Eric Schmitt, "Russian Agents Suspected of Directing Far-Right Group to Mail Bombs in Spain," *The New York Times*, January 22, 2023, https://www.nytimes.com/2023/01/22/us/politics/russia-spain-letter-bombs.html.
57 S. Paul Kapur and Sumit Ganguly, "The Jihad Paradox: Pakistan and Islamist Militancy in South Asia" *International Security* 37, no.1 (2012): 111–141; Avinash Paliwal and Paul Staniland, "Strategy, Secrecy, and External Support for Insurgent Groups," *International Studies Quarterly* 67 (2023), https://doi.org/10.1093/isq/sqad001.

58 Watts et al., *Proxy Warfare in Strategic Competition*, ch.5.
59 *China's Role in Myanmar's Internal Conflicts* (Washington, DC: United States Institute for Peace, 2018), 29, https://www.usip.org/sites/default/files/2018-09/ssg-report-chinas-role-in-myanmars-internal-conflicts.pdf; "Myanmar's Generals Aren't Happy With China—and It's No Longer a Secret," *The Irrawaddy*, July 3, 2020, https://www.irrawaddy.com/opinion/editorial/myanmars-generals-arent-happy-china-no-longer-secret.html.
60 Abhijnan Rej, "China Aiding Rebel Groups in India's Northeast: Report," *The Diplomat*, December 9, 2020, https://thediplomat.com/2020/12/china-aiding-rebel-groups-in-indias-northeast-report/.
61 "Chinese 'bribed Nigerian militants for access to vast mineral reserves,'" *The Times*, April 15, 2023.
62 Krishnadev Calamur, "North Korea's Terrorism Designation Isn't Entirely About Terrorism" *The Atlantic*, November 20, 2017, https://www.theatlantic.com/international/archive/2017/11/north-korea-state-sponsor-terrorism/546386/; Benjamin Young, "A Revolutionary State: North Korea's Support of Non-State Actors, Past Policies and Future Issues," *Korea Economic Institute of America*, October 5, 2017, https://keia.org/publication/a-revolutionary-state-north-koreas-support-of-non-state-actors-past-policies-and-future-issues/.
63 Samuel Ramani, "North Korea's Covert Alliance With Iran Aligned Militias in the Middle East," *38 North*, October 23, 2023, https://www.38north.org/2023/10/north-koreas-covert-alliance-with-iran-aligned-militias-in-the-middle-east/.
64 Jones et al, *Russia's Corporate* Soldiers.
65 Jones et al, *Russia's Corporate* Soldiers; Marten, "Russia's use of Semi-State Security Forces."
66 Nathan Hodge, "Wagner 'does not exist': Why Putin claims a rift in the mercenary group," *CNN*, July 14, 2023, https://www.cnn.com/2023/07/14/europe/russia-putin-wagner-prigozhin-tensions-intl/index.html#:~:text=%E2%80%9CWagner%20PMC%20does%20not%20exist,legal%20entity%2C%E2%80%9D%20he%20said; Paul Sonne, "Wagner Founder Rebuffs Order Over Fighter Contracts With Russian Military," *The New York Times*, June 11, 2023, https://www.nytimes.com/2023/06/11/world/europe/wagner-russia-defense-ministry-contract.html.
67 Gabriel Honrada, "China private security companies making a BRI killing," *Asia Times*, November 1, 2022, https://asiatimes.com/2022/11/china-private-security-companies-making-a-bri-killing/.
68 Paul Nantulya, "Chinese Security Firms Spread along the African Belt and Road," *Africa Center for Security Studies*, June 15, 2021, https://africacenter.org/spotlight/chinese-security-firms-spread-african-belt-road/.
69 Kai Liao, "SOF's Pivot to Great Power Competition and Its Implications to China," paper presented at the International Studies Association Asia-Pacific Conference, Waseda University, Tokyo, August 9, 2023.
70 Sergey Sukhankin, "An Anatomy of the Chinese Private Security Contracting Industry" *Jamestown Foundation*, January 3, 2023, https://jamestown.org/program/an-anatomy-of-the-chinese-private-security-contracting-industry/.
71 Gaute Friis, "Gray Zone Tactics Playbook: Rafting" *SeaLight*, July 15, 2023, https://www.sealight.live/posts/gray-zone-tactics-playbook-rafting; Gaute Friis, "Introducing China's Maritime Gray Zone Tactics Playbook" *SeaLight*, July 5, 2023, https://www.sealight.live/posts/introducing-china-s-maritime-gray-zone-tactics-playbook; Gregory B. Poling, Harrison Prétat, and Tabitha Grace Mallory, *Pulling Back the Curtain on China's Maritime Militia* (Washington, DC: Center for Strategic and International Studies, 2021), https://www.csis.org/analysis/pulling-back-curtain-chinas-maritime-militia.
72 Kennedy and Erickson, "China Maritime Report No. 1," 10–11.
73 Brian Hill, "The State as a Transnational Criminal Organization: A North Korea Case Study" *Journal of Indo-Pacific Affairs* (January–February 2023), https://media.defense.gov/2023/Feb/02/2003154183/-1/-1/1/06%20HILL_FEATURE.PDF/06%20HILL_FEATURE.PDF; Zhongmin Liu, "Criminal State: Understanding Narcotics Trafficking Networks in North Korea" *Journal of Financial Crime* 26 no. 4 (2019): 1014–1026; "North Korea Cyber Threat Overview and Advisories" *Cybersecurity and Infrastructure Security Agency*, accessed July 22, 2023, https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea.
74 "North Korea 'stole $2bn for weapons via cyber-attacks,'" *BBC News*, August 7, 2019, https://www.bbc.com/news/world-asia-49259302.
75 U.S. Treasury Department, "Treasury Sanctions Russian Proxy Wagner Group as a Transnational Criminal Organization," January 26, 2023, https://home.treasury.gov/news/press-releases/jy1220.
76 Mark Galeotti, *Putin's Wars: From Chechnya to Ukraine* (Oxford: Osprey Publishing, 2022), 172; Jack Losh and Sebastien Rabas, "Putin's Angels: The Bikers Battling for Russia in Ukraine," *The Guardian*, January 29, 2016, https://www.theguardian.com/world/2016/jan/29/russian-biker-gang-in-ukraine-night-wolves-putin..
77 Mark Galeotti, "Crimintern: How the Kremlin uses Russia's criminal networks in Europe," European Council on Foreign Relations, April 18, 2017, https://ecfr.eu/publication/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe/; Galeotti, *The Weaponisation of Everything*, 114–115.
78 J. Micheal Cole, "Nice Democracy You've Got There. Be a Shame If Something Happened to It," *Foreign Policy*, June 18, 2018, https://foreignpolicy.com/2018/06/18/nice-democracy-youve-got-there-be-a-shame-if-something-happened-to-it/; Galeotti, *The Weaponisation of Everything*, 115; Lynette Ong, "In Hong Kong, are 'thugs for hire' behind the attacks on protesters? Here's what we know about these groups," *The Washington Post*, July 24, 2019, https://www.washingtonpost.com/politics/2019/07/24/hired-guns-attacked-protesters-hong-kong-this-is-who-they-are-want-they-want/.
79 "Court upholds jail terms in Holger Chen shooting," *Taipei Times*, January 16, 2023, https://www.taipeitimes.com/News/taiwan/archives/2023/01/16/2003792692; J. Michael Cole, "Violent Incidents in Taiwan Linked to Organized Crime, Possible China Links," *Global Taiwan Institute*, November 4, 2020, https://globaltaiwan.org/2020/11/violent-incidents-in-taiwan-linked-to-organized-crime-possible-china-links/.
80 Sam Cooper, "How China made Canada a global node for narcos and cyber-criminals," *Sunday Guardian*, May 15, 2021, https://sundayguardianlive.com/news/china-made-canada-global-node-narcos-cyber-criminals; Vanda Felbab-Brown, "China's role in the fentanyl crisis," *Brookings Institute*, March 31, 2023, https://www.brookings.edu/testimonies/chinas-role-in-the-fentanyl-crisis/; Bertil Lintner, "Why the US bit back at China's 'Broken Tooth,'" *Asia Times*, December 12, 2023, https://asiatimes.com/2020/12/why-the-us-bit-back-at-chinas-broken-tooth/; Nick McKenzie, "'Illegal, malign': China's state-sponsored crime stretches across Pacific," *Sydney Morning Herald*, May 19, 2023; Sebastian Rotella, "Outlaw Alliance: How China and Chinese Mafias Overseas Protect Each Other's Interests," *ProPublica*, July 12, 2023, https://www.propublica.org/article/how-beijing-chinese-mafia-europe-protect-interests.

81 Rotella, "Outlaw Alliance."
82 Ibid.
83 See Cüneyt Gürer and Francesca E. Strat, "Transnational Organized Crime in the Gray Zone: The Authoritarian IW Toolbox and Strategic Competition" *Irregular Warfare Center*, June 13, 2023, https://irregularwarfarecenter.org/publications/perspectives/transnational-organized-crime-in-the-gray-zone-the-authoritarian-iw-toolbox-and-strategic-competition/..
84 Maurer, *Cyber Mercenaries*; Robert Sheldon and Joe McReynolds, "Civil-Military Integration and Cybersecurity: A Study of Chinese Infromation Warfare Militias," in Jon R. Lindsay, Tai Ming Cheung and Derek S. Reveron (Eds) *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (Oxford: Oxford University Press, 2015), 188–224.
85 U.S. Department of Justice, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," February 17, 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.
86 Galeotti, *The Weaponisation of Everything*, 111–112; Andrew Kramer, "How Russia Recruited Elite Hackers for Its Cyberwar," *The New York Times*, December 29, 2016, https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html; Maurer, *Cyber Mercenaries*, 96.
87 Frank Bajak, "How the Kremlin provides a safe harbor for ransomware," *Associated Press*, April 16, 2021, https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999; Andrew Kramer, "Hacker Is a Villain to Russia and the United States, for Different Reasons," *The New York Times*, March 16, 2017, https://www.nytimes.com/2017/03/16/world/europe/russian-hacker-fsb-agent-dmitry-dokuchaev.html; Maurer, *Cyber Mercenaries*, 95–96.
88 Kramer, "Hacker Is a Villain to Russia and the United States, for Different Reasons,"; U.S. Department of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," March 15, 2017, https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.
89 Jon Bateman, *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications* (Washington, DC: Carnegie Endowment for International Peace, 2022), https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657; Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn: Cooperative Cyber Defence Centre of Excellence, 2010), https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf; Maurer, *Cyber Mercenaries*, 96–103; "Reckless campaign of cyber attacks by Russian military intelligence service exposed," *National Cyber Security Centre*, October 23, 2018, https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed..
90 Adam Kozy, "Testimony before the U.S.-China Economic and Security Review Commission Hearing on "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States,"" *U.S.-China Economic and Security Review Commission*, February 17, 2022, https://www.uscc.gov/sites/default/files/2022-02/Adam_Kozy_Testimony.pdf; U.S. Department of Justice, "Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally," September 16, 2020, https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer..
91 U.S. Department of Justice, "Seven International Cyber Defendants, Including "Apt41" Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally."
92 Braw, *The Defender's Dilemma*, 56–82; Hamilton, *Silent Invasion*, 150–179.
93 Ibid.
94 Braw, *The Defender's Dilemma*, 67; Hamilton, *Silent Invasion*, 76; Veerle Nouwens and Alexander Neill (Eds), *Malign Interference in Southeast Asia: Understanding and Mitigating Economic and Political Interference and Information Operations* (London: Royal United Services Institute for Defence and Security Studies, 2022), https://static.rusi.org/malign-interference-in-southeast-asia.pdf.
95 "A guide to foreign interference and China's suspected influence in Canada," *The Globe and Mail*, May 22, 2022; Brady, *Magic Weapons*; Nouwens and Neill (Eds) *Malign Interference in Southeast Asia*; Catrin Owen, "Yikun Zhang, the millionaire at the centre of the political donations trial," *Stuff*, October 5, 2022, https://www.stuff.co.nz/national/crime/129949313/yikun-zhang-the-millionaire-at-the-centre-of-the-political-donations-trial.
96 Brady, *Magic Weapons*.
97 "A guide to foreign interference and China's suspected influence in Canada;" Hamilton, *Silent Invasion*, 130.
98 Aro, *Putin's Trolls*, ch.6; Ruth May, "How Putin's oligarchs funneled millions into GOP campaigns," *Dallas News*, May 8, 2018, https://www.dallasnews.com/opinion/commentary/2018/05/08/how-putin-s-oligarchs-funneled-millions-into-gop-campaigns/; Paul Sonne, "A Russian bank gave Marine Le Pen's party a loan. Then weird things began happening," *The Washington Post*, December 27, 2018, https://www.washingtonpost.com/world/national-security/a-russian-bank-gave-marine-le-pens-party-a-loan-then-weird-things-began-happening/2018/12/27/960c7906-d320-11e8-a275-81c671a50422_story.html; Seth Thévoz and Peter Geoghegan, "Revealed: Russian donors have stepped up Tory funding," *Open Democracy*, November 5, 2019, https://www.opendemocracy.net/en/dark-money-investigations/revealed-russian-donors-have-stepped-tory-funding/..
99 Rid, *Active Measures*, 408.
100 Clarissa Ward et al., "Russian election meddling is back – via Ghana and Nigeria – and in your feeds," *CNN*, April 11, 2020, https://www.cnn.com/2020/03/12/world/russia-ghana-troll-farms-2020-ward/index.html..
101 Sarah O'Connor et al., *Cyber-Enabled Foreign Interference in Elections and Referendums* (Barton ACT: Australian Strategic Policy Institute, 2020), https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2020-10/Cyber%20enabled%20foreign%20interference_0.pdf?VersionId=QnX7Dz7akMiLSP5xHWYYo8ZitxOt2_i7.
102 Deutsche Welle (@dwnews), "Russia is spreading disinformation and anti-West propaganda in Africa via local influencers paid by Moscow officials — and even the Wagner group," Twitter, July 30, 2023, https://twitter.com/dwnews/status/1685886304821641216.
103 Aro, *Putin's Trolls*.
104 O'Connor et al., *Cyber-Enabled Foreign Interference in Elections and Referendums*.
105 Paul Huang, "Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate," *Foreign Policy*, June 26, 2019, https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/.

106 Ibid.
107 Henry Farrell, "The Chinese government fakes nearly 450 million social media comments a year. This is why," *The Washington Post*, May 19, 2016, https://www.washingtonpost.com/news/monkey-cage/wp/2016/05/19/the-chinese-government-fakes-nearly-450-million-social-media-comments-a-year-this-is-why/; Maurer, *Cyber Mercenaries*, ch.7.
108 Ryan Serabian and Daniel Kapellmann Zafra, "Pro-PRC "HaiEnergy" Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites," *Mandiant*, August 4, 2022, https://www.mandiant.com/resources/blog/pro-prc-information-operations-campaign-haienergy; Ryan Serabian et al., "Pro-PRC HaiEnergy Campaign Exploits U.S. News Outlets via Newswire Services to Target U.S. Audiences; Evidence of Commissioned Protests in Washington, D.C.," *Mandiant*, July 24, 2023, https://www.mandiant.com/resources/blog/pro-prc-haienergy-us-news..
109 Albert Zhang and Danielle Cave, "China's cyber interference and transnational crime groups in Southeast Asia," *ASPI Strategist*, July 24, 2023, https://www.aspistrategist.org.au/chinas-cyber-interference-and-transnational-crime-groups-in-southeast-asia/.
110 Serabian and Kapellmann Zafra, "Pro-PRC "HaiEnergy" Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites"; Serabian et al., "Pro-PRC HaiEnergy Campaign Exploits U.S. News Outlets via Newswire Services to Target U.S. Audiences; Evidence of Commissioned Protests in Washington, D.C."; Zhang and Cave, "China's cyber interference and transnational crime groups in Southeast Asia.".
111 Serabian and Kapellmann Zafra, "Pro-PRC "HaiEnergy" Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites"; Serabian et al., "Pro-PRC HaiEnergy Campaign Exploits U.S. News Outlets via Newswire Services to Target U.S. Audiences; Evidence of Commissioned Protests in Washington, D.C.".
112 Brady, *Magic Weapons*, 35–39; Hamilton, *Silent Invasion*, 61–67; Nick McKenzie et al., "The Chinese Communist Party's power and influence in Australia," *ABC News*, June 3, 2017, https://www.abc.net.au/news/2017-06-04/the-chinese-communist-partys-power-and-influence-in-australia/8584270.
113 Hamilton, *Silent Invasion*, 142; Jim Waterson and Dean Sterling Jones, "Daily Telegraph stops publishing section paid for by China," *The Guardian*, April 14, 2020, https://www.theguardian.com/media/2020/apr/14/daily-telegraph-stops-publishing-section-paid-for-by-china.
114 Bernadette Carreon and Aubrey Belford, "Solomon Islands Newspaper Promised to "Promote China" in Return for Funding," *Organized Crime and Corruption Reporting Project*, July 30, 2023, https://www.occrp.org/en/daily/17884-solomon-islands-newspaper-promised-to-promote-china-in-return-for-funding.
115 Ibid.
116 Bethany Allen-Ebrahimian, "China's Long Arm Reaches into American Campuses," *Foreign Policy*, March 7, 2018, https://foreignpolicy.com/2018/03/07/chinas-long-arm-reaches-into-american-campuses-chinese-students-scholars-association-university-communist-party/.
117 Hamilton, *Silent Invasion*, 269–281; Sandra Petersmann and Esther Felden, "China's quantum leap — Made in Germany," *Deutsche Welle*, June 13, 2023, https://www.dw.com/en/chinas-quantum-leap-made-in-germany/a-65890662.
118 Hamilton, *Silent Invasion*, 319–321; Alex Joske, *The Party Speaks for You: Foreign Interference and the Chinese Communist Party's United Front System* (Canberra: Australian Strategic Policy Institute, 2020), https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2020-06/The%20party%20speaks%20for%20you_0.pdf?VersionId=gFHuXyYMR0XuDQOs.6JSmrdyk7MralcN.
119 Aro, *Putin's Trolls*, ch.10; Martin Kragh and Sebastian Åsberg, "Russia's strategy for influence through public diplomacy and active measures: the Swedish case," *Journal of Strategic Studies* 40 no. 6 (2017): 773–816.
120 Majlie de Puy Kamp and Isabelle Chapman, "'It's shameful': Russian-linked billionaires have given enormous sums of money to the West's leading educational and cultural institutions," *CNN*, May 11, 2022, https://www.cnn.com/2022/05/11/us/russian-oligarchs-philanthropy-ukraine-war-invs/index.html.
121 Ibid.
122 Una Aleksandra et al.,*Hybrid Threats: A Strategic Communications Perspective* (Riga: NATO Strategic Communications Centre of Excellence, 2019), 80–81, 84–85, https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/79; Vitalie Calugareanu and Robert Schwartz, "Pro-Russian group pays protesters in Moldova," *Deutsche Welle*, October 15, 2022, https://www.dw.com/en/pro-russian-group-pays-protesters-in-moldova/a-63446784; Jane Cowan, "Evidence pro-Russian demonstrators in eastern Ukraine being paid: White House," *ABC News*, April 7, 2014, https://www.abc.net.au/news/2014-04-08/pro-russian-demonstrators-in-ukraine-paid/5373834; Stefan Meister, "The "Lisa case": Germany as a target of Russian disinformation," *NATO Review*, July 25, 2016, https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html; Rid, *Active Measures*; Ivana Stradner and George Barros, "How Kremlin Uses the Church in Europe's East," *American Enterprise Institute*, December 10, 2021, https://www.aei.org/op-eds/how-kremlin-uses-the-church-in-europes-east/.
123 Braw, *The Defender's Dilemma*, 116; Kozy, "Testimony before the U.S.-China Economic and Security Review Commission Hearing on "China's Cyber Capabilities."
124 Tom Blackwell, "Criticized as toothless, Australia's foreign-influence registry a warning as Canada plans its own," *National Post*, March 31, 2023, https://nationalpost.com/news/canada/criticized-as-toothless-australias-foreign-influence-registry-a-warning-as-canada-plans-its-own; Nick Robinson, "The Foreign Agents Registration Act Is Broken," *Foreign Affairs*, July 22, 2019, https://foreignpolicy.com/2019/07/22/the-foreign-agents-registration-act-is-broken/.
125 For a similar argument, see: Jeremy Reeves, *A New Typology for State-Sponsored International Terrorism,* [Unpublished Master's Thesis] (Monterey, CA: Naval Postgraduate School, 2011), https://www.hsdl.org/?view&did=699794.
126 "Countering foreign interference in education and research" *Department of Home Affairs*, accessed July 29, 2023, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/in-education-and-research#:~:text=The%20University%20Foreign%20Interference%20Taskforce,sector's%20response%20to%20foreign%20interference.
127 See Morris et al., *Gaining Competitive Advantage in the Gray Zone*; Nouwens and Neill (Eds) *Malign Interference in Southeast Asia*.
128 Ryan Grauer and Dominic Tierney, "The Arsenal of Insurrection: Explaining Rising Support for Rebels," *Security Studies*, 27 no. 2 (2018): 263–295.

IWC PRESS