Chapter 10

Rogues, Disrupters, and Spoilers in an Era of Great Power Competition

By Bryce Loidolt, Mariya Omelicheva, and James Przystup

This chapter reviews the interests and behavior of Russia, Iran, and North Korea, so-called rogue, disrupter, and spoiler states. Motivated by goals ranging from a desire for regime survival to aspirations for regional dominance and even global relevance, these countries threaten to divert U.S. attention and resources away from the imperatives of Great Power competition and draw the United States into escalating and destructive crises. At first glance, then, there might appear to be strong incentives for China to form enduring, fully cooperative relationships with each of these countries. Yet this chapter also finds that Russian, Iranian, and North Korean provocative behavior is not uniformly beneficial for China, and the prospect of a robust and fully cooperative anti-U.S. axis in 2020 remains remote. U.S. policymakers should anticipate the threat from each of these states to persist, but not necessarily to become more pronounced, as U.S.-Chinese competition intensifies.

As the United States continues to move into an era of Great Power competition featuring long-term rivalry and the prospect of Great Power transition with China, it will continue to encounter destabilizing activities from so-called rogue, disrupter, and spoiler states and regimes. We define this group of countries as those that lack the military and long-term economic power and/or transnational cultural appeal to match U.S. power globally or stabilize an alternative international political order. These states also tend to confront the United States below the threshold of active armed conflict and across multiple domains.[1] In defining this category of states based both on material and nonmaterial attributes as well as on conduct, this chapter reaches across what are often subjective, analytically blurry, and historically contingent concepts and definitions.[2] Although many countries meet the criteria identified above, this chapter focuses specifically on the challenges posed by the Russian Federation, the Islamic Republic of Iran, and the Democratic People's Republic of Korea (DPRK).

Notably, the grouping of these three countries within the same analytic category is a departure from the National Defense Strategy and the National Security Strategy, both of which describe the DPRK and Iran as rogue regimes and Russia as a near-peer competitor

on a par with China.[3] This categorizing also deviates from the other chapters in this volume that treat Russia as a near-peer Great Power competitor. This change is intentional. The inclusion of Russia and exclusion of China—whose behavior is sometimes consistent with the definitional criteria offered above—is not intended to argue that Russian foreign policy lacks a desire for global relevance or that Russia is currently unable to compete with the United States. It is also not intended to sidestep the dimensions of Chinese behavior consistent with rogue, disrupter, or spoiler states. Instead, we posit that Russia and China's divergent economic trajectories imply a divergence in their future military strength. If Russian material power continues to decline and China's increases in the years to come, then Moscow's somewhat debatable status as a contemporary Great Power will recede even further.[4] Thus, the alternative view of Moscow offered in this chapter may be an increasingly useful lens through which to analyze and understand Russian behavior and its implications for an era that becomes increasingly dominated by a U.S.-China Great Power dyad.[5]

The DPRK, Iran, and Russia are motivated by a combination of regime survival, aspirations for regional dominance and sometimes global relevance, as well as an inclination to confront the United States, which they all see as the main obstacle to their own aspirations. And lacking a proactive vision for or means to stabilize an alternative international order, these countries employ a variety of coercive instruments—ranging from proxy warfare to direct military threats—to pursue their interests.[6] Moreover, their development of nuclear weapons and, in some cases, proliferation of ballistic missiles poses a serious threat to regional stability.

Through these activities, each of these countries threatens to undermine the security of U.S. allies and partners, erode U.S. credibility and influence abroad, and mire the United States and its allies in a labyrinth of internal challenges by impairing the legitimacy of their democratic political processes. Although such coercive activities tend to fall below a threshold that would prompt a conventional military response from the United States, they also risk escalating into potentially lethal crises. These states could not only divert U.S. attention and resources away from longer term objectives but also draw the United States into more distracting and costly confrontations.

Costs for the United States imply benefits for China, naturally raising the troubling specter of a more robust strategic alignment among these states against the United States. Indeed, China's security and economic relationships with Russia, Iran, and the DPRK often serve to constrain U.S. power. Welcoming the diversionary and constraining benefits of these countries' activities, Beijing could seek to strategically instigate these states' destabilizing behavior to the detriment of the United States.

This chapter finds, however, that Russian, Iranian, and North Korean provocative behavior is not uniformly beneficial for China, and the prospect of a robust and fully cooperative anti-U.S. axis in 2020 remains remote. U.S.-Chinese competition will yield limited prospects for burden-sharing between Beijing and Washington in comprehensively addressing Russian, Iranian, or DPRK conduct that is harmful to the United States. Given the negative externalities, the behavior of each country likely limits the depth of its relationship with Beijing.

China will need to balance the costs that these states can inflict on the United States and its allies with the potential spillover effects rogue and spoiler activities can have on

Beijing's economic interests and strategic partnerships. Ultimately, U.S. policymakers can anticipate neither fully cooperative nor obstructive responses from China to address the challenges each of these countries poses to regional stability.

The remainder of this chapter begins with an overview of the interests and behavior of the Russian Federation, the Islamic Republic of Iran, and the DPRK—paying specific attention to how these states' activities affect U.S. security interests. The second section turns to a discussion of China's relationship with these countries as well as the positive and negative consequences that their behaviors have for Chinese interests. It concludes with a projection for how these security challenges might evolve over the next 5 years and the implications for U.S.-China strategic competition.

Russian Federation

As detailed in chapter 3a of this volume, Russia's foreign policy is motivated by Great Power aspirations, a desire to reconstitute a sphere of influence in a multipolar world, and the desire for a buffer zone along its western, southern, and eastern borders to protect the country from potential security threats.[7] Russian leadership views the unipolar world dominated by the United States as the gravest threat to its national interests. Russia perceives the United States as a dangerous meddler in the domestic affairs of sovereign states and as a rogue disrupter of stability in the Middle East and other parts of the world. This shift in Russian foreign policy from cooperation to competition with the United States did not occur all at once in 2014 but, rather, in the mid-1990s, when Russia's foreign policy establishment, disillusioned with the lack of reciprocity to its accommodation and integration with the West, began conceiving of a unipolar world as inimical to its own national interests.

As delineated in chapter 3b of this book, while Russia tends to pursue its interests through unconventional means of coercive influence, its conventional military capabilities loom large.[8] Beginning in Ukraine in 2014, Russia's disinformation campaign and use of "little green men" were deemed effective substitutes for the direct application of military power, and in Syria, Russia's military proxies have allowed the Kremlin to plan and direct military actions under the cover of plausible deniability. Yet it is improved conventional military capabilities—rapidly deployable force; air defense; command, control, intelligence, surveillance, and reconnaissance; long-range strikes—that have been equally, if not more, decisive for Moscow in both theaters.[9] Conventional military power has helped Moscow sustain pressure on Kyiv; in Syria, Russia's expeditionary capabilities have forged it into a key powerbroker in the conflict. Russia's gray zone tactics, which encompass psychological, cyber, computer network, proxy warfare, and electronic operations, are thus complementary to its conventional military capabilities.

Together with its information warfare in Ukraine, Moscow's interference in U.S. domestic politics represents a blueprint for a so-called strategy of active defense. Discussed by a chief architect of Russia's military doctrine, General Valery Gerasimov, this preemptive strategy encompasses a range of information tactics applied to destabilize potential threats to Russia's interests.[10] These approaches include the use of Internet trolls (government-funded individuals who exploit social cleavages through fake blogs, offensive and inflammatory comments, and false information for sowing discord or swaying public opinion); leaking adverse, sensitive, or misleading information on foreign government officials

and institutions; and using government-funded mass media to disseminate propaganda favoring Russia. Releasing a significant amount of sensitive information or disinformation ahead of foreign elections or at the height of an international crisis involving Russia, using trolls and bots to amplify it, and publicizing these findings on Russia-sponsored outlets are used synergistically to orchestrate Russia's information strategy.[11]

The spread of Russia's cyber intrusions and operations—ranging from the distributed denial-of-service (DDoS) and Structured Query Language injection attacks to phishing and eavesdropping—speaks to the sophistication of the country's cyber tools and institutional architecture for implementing them. The latter combines multiple security agencies with vast expertise in foreign and domestic intelligence-gathering with proxy-cyber activists, the so-called patriotic hackers, cyber criminals, and even legitimate cyber tech firms. Outsourcing cyber attacks allows Russia to create plausible deniability and lower the risks and costs associated with controversial foreign information campaigns. These attacks can also be used to sabotage critical physical infrastructure—banks, state institutions, and power plants—on a massive scale (as they did in Estonia, Georgia, Ukraine, and Montenegro). Multiple international organizations, including the World Anti-Doping Agency and the Organisation for the Prohibition of Chemical Weapons (OPCW), have also been targets of Russia's cyber attacks.[12] Russia's hacking attempt at the chemical weapons watchdog took place against the backdrop of the OPCW's ongoing investigation into the 2018 use of a military-grade nerve agent attack against Sergei Skripal in the United Kingdom.[13]

Proxies and mercenaries are other assets that allow Russia to accomplish its objectives without resorting to conventional military means. Russian mercenaries have fought alongside regular forces in complex battlespaces in Syria and eastern Ukraine and have operated in various capacities in the Central African Republic (CAR), Libya, Sudan, and even Venezuela. In all these contexts, the presence of Russian private military companies (PMCs) on the ground has allowed the Kremlin to play a critical role in security policies of these states. Because Russia's PMCs, in particular the Wagner Group, rely on the profits from natural resources seized on behalf of regimes in Syria, Sudan, or CAR for reimburse for their military service, their involvement in conflicts redirect the supported governments' operational priorities. Furthermore, in Sudan and CAR, Wagner has not only operated in a combat role but also provided these regimes with training, site defense, and security provision for top-level officials.[14]

Of course, Russia also employs more traditional means, using diplomacy, foreign aid, and arms transfers to pursue its strategic objectives. For example, in the United Nations Security Council, Russia has continued to veto resolutions aimed at investigating or sanctioning Bashar al-Asad's use of chemical weapons and wider brutality during the Syrian civil war.[15] In Latin America, Russia has extended critical economic support to the embattled regime of Nicolás Maduro in Venezuela, stymying hopes for a democratic transition and undermining regional stability.[16] Additionally, through its arms transfers, Russia has sought to exploit or otherwise create strategic daylight between the United States and its allies.[17] Moscow has upped the ante through coercive messaging to Western audiences, stressing Russian resolve for nuclear retaliation and touting its purported superiority in hypersonic and other weapons systems.[18] Russia often accompanies these announcements

with displays of force in massive wargames and provocative air force maneuvers near North Atlantic Treaty Organization (NATO) territory.[19]

These activities from Russia have far-reaching consequences for political stability, societal harmony, and continuous functioning of democratic institutions in its immediate neighborhood and around the world. Cyber attacks on physical infrastructure, particularly when they are combined with political trolling, not only have immediate grim consequences but also stimulate public fear, disengagement, and mistrust in the ability of the government to protect citizens. Information operations and the use of proxies have allowed Russia to maintain or expand its political and military influence (and supplant that of the United States) in many theaters around the world at relatively low cost. Turkey's status and NATO's continued viability and integrity are also in question, as Ankara is being pulled away from the West by the conflict. The unresolved war in Ukraine threatens to transform into a frozen conflict that would preclude Kyiv's integration into an array of liberal, democratic, and open European states. By offering security to embattled autocratic leaders in Africa, Russia also threatens to undermine U.S. interests by weakening local governance; this elevates Moscow's geopolitical posture and its material gains derived from weapons sales and access to natural resources.

The Islamic Republic of Iran

A mix of ideational and material factors motivates Iranian foreign policy behavior and underpins Iran's pursuit of regional interests. Iranian foreign policy revolves around the survival of the Islamic Republic in the face of perceived internal and external threats. Although the revolutionary zeal that characterized Iranian foreign policy throughout the 1980s has withered, Iran seeks to displace U.S. and Israeli regional dominance. Iran has often framed its policies in defensive terms. The Chief of Staff of the Iranian Armed Forces, Major General Mohammad Baqeri, declared in early 2019, "Regional enemies should know that in addition to [a] doctrine of peace, Iran has a strong military presence."[20] Nevertheless, Iran has been able to exploit the instability generated by the Arab Spring to counter what it views as U.S. and Israeli imperialist hegemony in the region, while also shoring up traditional allies and creating new ones in the Levant.[21]

Hampered by economic sanctions, particularly after the U.S. May 2018 withdrawal from the Joint Comprehensive Plan of Action (JCPOA), and facing a hostile geopolitical environment, Iran has been unable to address the threats to its national security through conventional military power. Since the Iran-Iraq War, the Islamic Republic has not had access to the foreign inputs required to rebuild and modernize its conventional military forces; it also lacks the requisite indigenous defense industrial base to do so unilaterally.[22] Moreover, the devastating Iran-Iraq War has been seminal in shaping Iran's force structure decisions, creating a strong inclination among Iranian decisionmakers to avoid conventional warfare altogether.[23] As a result, Iran pursues its goals through a more asymmetric approach that aims to coerce and deter the United States and Israel, as well as rival Arab Gulf states, without prompting a conventional military response from its better equipped and more militarily proficient adversaries.

Iran's regional defense strategy relies on several instruments of coercion, deterrence, and defense, each of which can be calibrated to meet an array of threats. First, Iran has

developed a standoff strike capability that allows it to credibly threaten military, economic, and civilian targets within its rival's borders.[24] These weapons, which include ballistic and cruise missiles and unmanned aerial vehicles (UAVs), afford Iran not only a lower cost but also a plausibly deniable alternative to manned aircraft. In many ways, this obviates Iran's need for an air force capable of long-range precision strikes.[25] For example, on September 14, 2019, an attack using a combined 25 missiles and drones allowed Iran to jeopardize roughly half of Saudi Arabia's oil output. Moreover, in response to the U.S. killing of Islamic Revolutionary Guard Corps (IRGC) Qods Force commander Qassem Suleimani and Kata'ib Hizballah commander Abu Mahdi al-Mohandis, Iran fired more than a dozen ballistic missiles at two Iraqi bases hosting U.S. and coalition personnel in January 2020.[26]

Iran maintains several capabilities that have allowed it to disrupt global shipping in the Strait of Hormuz, a key maritime chokepoint. Although Iran has continued to threaten to close down the strait, the technical requirements and subsequent countermeasures that such an attempt would instigate make this prospect unlikely.[27] Nevertheless, Iran has several options that it could employ in various combinations to affect the calculus of the shipping industry, raising the costs of transiting the Strait of Hormuz and threatening to constrain the global energy supply; they include shore-based antiship cruise missiles, naval mines, armed IRGC navy speed boats, and UAVs.[28] The continued, albeit recently less prevalent, incidence of provocative behavior by the Iranian navy demonstrated a willingness to obstruct maritime traffic by attacking civilian tankers in the gulf with limpet mines in June 2019.[29]

Next, Iran maintains an array of militant clients that, although varying in the degree of their responsiveness to Tehran, allows Iran to extend its influence to neighboring countries, forming what Iranian officials commonly refer to as the "Axis of Resistance."[30] This includes longstanding clients such as Lebanese Hizballah and Hamas, as well as the Ansar Allah or Houthi rebels in Yemen, al-Ashtar Brigades in Bahrain, and the Afghan Fatimiyun and Pakistani Zaynabiyun Brigades that fight in Syria.[31] Iran's diverse network of militant partners also contains several Shia groups in Iraq, encompassing long-term Iranian partners such as Asaib Ahl al-Haq, Kataib Hizballah, and the Badr Organization, as well as recent iterations of smaller so-called special groups, that, although lesser in terms of pure numbers, are suspected to have closer ties to Tehran.[32] These clients allow Iran to extend its political influence while offering it additional platforms from which it can attack U.S. and allied interests.

Iran has also sponsored terrorist attacks farther abroad, beyond areas where Iran lends support to militant proxies in the Middle East. For example, throughout the 1990s, Iranian operatives supported or directly executed a series of assassinations of Iranian dissidents in Europe.[33] In 2018, law enforcement authorities in Belgium, France, and Germany arrested Iranian operatives—including a government official—who had planned to bomb a political rally in France.[34] IRGC-led plots to attack Western and Israeli targets have also been disrupted in Nigeria, Kenya, Uruguay, and the United States.[35]

Iran has recently expanded its cyber activities to offensive intrusions and attacks on foreign companies.[36] From September 2012 through January 2013, a hacker group known as the Izz al-Din al-Qassam Cyber Fighters carried out several DDoS attacks against U.S. financial institutions. Moreover, Iran is suspected to be behind the August 2012 cyber attack on Saudi Aramco as well as a 2016 attack that affected the Saudi General Authority for Civil Aviation and the Central Bank.[37]

Finally, since the U.S. withdrawal from the JCPOA, Iran has gradually resumed its nuclear enrichment activities. In 2018, Iran prepared to expand its manufacturing and enrichment capacity, remaining within the JCPOA-prescribed limits.[38] In the wake of the U.S. killing of Qassem Suleimani, Iran also announced that it would be abandoning operational limits imposed by the nuclear deal.[39]

Though not by any means an existential threat to the United States, Iran's set of coercive options and activities presents hazards to the stability of U.S. partners, allies, and regional interests. Beyond the recent U.S. strikes against Suleimani and Katib Hizballah facilities, U.S. allies and partners in the Middle East have come into conflict with Iranian-backed clients. This includes the Saudi-led coalition in Yemen as well as Israel, which has taken a more forward-leaning role in striking Iranian-backed proxies in Iraq and Syria.[40] Iran's activities in the Strait of Hormuz, including the June 2019 downing of a U.S. UAV and the seizing of civilian tankers, further risk instigating tit-for-tat escalations that could significantly disrupt maritime traffic through a key strategic chokepoint—just as a resumption in Iran's nuclear activities could spark a dangerous regional conflict.[41]

Democratic People's Republic of Korea

The DPRK operates more as a quasi-criminal enterprise than a legitimate nation-state.[42] At its core, the Kim Jong-un government is most concerned with sustaining its family enterprise and ensuring the survival of the regime at all costs. It also prioritizes the reunification of the Korean Peninsula as a means to the end of regime survival and an endstate of itself.[43] This apparent lack of international ambition on the part of the Kim regime might suggest an attenuated threat to global stability, but its activities have far-reaching consequences for U.S. security interests in the new era of Great Power competition.

Through the development of weapons of mass destruction, use of chemical weapons, and aggressive posturing of its conventional forces, the DPRK threatens regional stability and global norms. North Korea is estimated to have somewhere between 15 and 60 nuclear warheads, as well as approximately 650 ballistic missiles that could threaten cities in South Korea, Japan, and eastern China.[44] It has also tested intercontinental ballistic missiles that could be capable of striking the United States.[45] At the same time, North Korea continues to pose a conventional threat to South Korea and Japan. The People's Army, an estimated 1.2 million in strength, is overwhelmingly forward-deployed toward the Demilitarized Zone in an offensive posture.[46] Kim has also pursued more advanced conventional capabilities, including more precise artillery and ballistic missile capabilities as well as UAVs.[47] In this environment, North Korea's nuclear arsenal provides Pyongyang with the potential for nuclear blackmail, allowing it to engage in lower level conventional provocations and, at the same time, affect South Korean and U.S. decisions on kinetic responses or induce economic concessions.

Underscoring the criminal nature of the regime, in February 2017, the DPRK carried out the assassination of Kim's half-brother using the nerve agent VX in Malaysia.[48] North Korea's malign behavior has historically extended beyond Asia and included weapons transfers to hostile states and armed groups in the Middle East. Iran has been accused of being "one of the two most lucrative markets for DPRK military-related cooperation."[49] Pyongyang has indeed engaged in an ongoing relationship with Iran featuring sales and

the transfer of military technology that has served to advance the development of Tehran's ballistic missile programs.[50] The DPRK has also pursued military cooperation and technology transfers in the Sudan and offered small arms and ballistic missiles to the Houthi rebels in Yemen through a Syrian intermediary.[51] North Korea has also exported the SCUD-D, a newly tested advanced short-range ballistic missile, to Syria.[52]

To sustain the regime in the face of international sanctions and condemnation, North Korea has resorted to a wide range of illegal activities that violate global norms. Pyongyang has employed its cyber capabilities to hack banks across the globe, reportedly carrying out successful cyber heists against banks in Bangladesh, Chile, Guatemala, India, Kuwait, Mexico, Pakistan, the Philippines, South Korea, Taiwan, Turkey, and Vietnam.[53] These attacks can be quite lucrative; it has been reported that in one such attack against the Central Bank of Bangladesh in 2016, North Korea netted $81 million.[54] A United Nations Security Council report estimates that in total the DPRK may have acquired as much as $2 billion through its cyber operations.[55] North Korean cyber operations have also targeted media outlets that it deems critical of its policies or of Kim in particular.[56]

Currency counterfeiting and narcotics trafficking have helped the regime generate funds and offset the effects of sanctions. In the late 1970s, Pyongyang began to put counterfeit U.S. currency into circulation, featuring "supernotes"—phony bills of remarkably high quality—of $50 and $100 denominations. There is a high degree of uncertainty regarding the value of this activity; estimates range from $1.25 million to $250 million per annum.[57] Since the 1970s, when Pyongyang began to sponsor opium cultivation and the production of opiates, North Korean diplomats have been arrested in antinarcotics operations across the globe. As of 2007, North Korea has been linked to drug seizures in at least 20 countries.[58] In the 1990s, North Korea reportedly began manufacturing crystal methamphetamine for exports using Chinese triads, the Japanese Yakuza, and the Russian mafia as distribution channels.[59] To weaken the effect of sanctions on North Korea's exports, Pyongyang has moved to step up production of illicit drugs to earn the hard currency needed to fund its nuclear and missile development programs.[60]

North Korea thus represents a multidimensional threat to the prosperity and security of the United States and its allies in the Indo-Pacific region, as its nuclear weapons, ballistic missiles, and conventional posture place several U.S. allies at risk. The DPRK's willingness to use chemical weapons and its involvement in transnational criminal activity similarly violate international norms, and the aforementioned cyber operations have important consequences for the security of the global financial sector.

Rogue, Disrupter, and Spoiler State Behavior and U.S.-China Competition

Beijing currently maintains collaborative, if sometimes distant, relations with Russia, Iran, and the DPRK. China shares with all of these countries a general displeasure with U.S. hegemony and dominance of international institutions. Iran is considered a "comprehensive strategic partner" by Beijing, and Chinese-Iranian cooperation spans the economic and security spheres.[61] With respect to the former, since 2005, Chinese investments in and contracts with Iran have topped $27 billion.[62] And China has reportedly assisted in developing Iran's ballistic missiles, antiship mines, fast-attack boats, and other weapons technology.[63] In

2018, China also imported $15 billion worth of oil from Iran.[64] China and Russia maintain a "comprehensive cooperative" strategic partnership, which may be emblematic of deepening Sino-Russian cooperation.[65] In addition to regular diplomatic and military exchanges under the auspices of regional and international organizations, Russia agreed to assist China in building a strategic missile early-warning system and may view a relationship with China as a valuable avenue through which it can challenge the United States.[66] China's share of Russia's trade and investments has also grown.[67] While Beijing officially continues to support United Nations sanctions on North Korea, cross-border trade with North Korea has bolstered regime stability. In July 2019, the *South China Morning Post* reported a 14.3 percent increase in China's trade with North Korea in the first half of 2019, amounting to $1.25 billion.[68] President Xi Jinping's visit to Pyongyang in June 2019 stands as a clear indication of China's political and economic support for the DPRK.

Although Chinese interests in maintaining relationships with each state are distinct, ranging from shared hostility toward the United States to China's energy needs and desire to maintain a peaceful neighborhood, China's behavior has the consequence of insulating Russia, Iran, and the DPRK from the costs of their provocative behavior. In the case of Iran and the DPRK, economic relations with Beijing offer relief from international sanctions. Additionally, Iran has relied on China for advanced conventional capabilities. Chinese trade and largesse similarly offer Russia an economic lifeline. China has also been willing to purchase Russian combat aircraft and surface-to-air missile systems despite U.S. sanctions.[69]

In turn, each state's provocative activities offer some important perks for Beijing. First, China benefits from having additional voices questioning the value and wisdom of U.S. hegemony and international norms. This benefit is perhaps most apparent in the cyber domain, where both Russia and China have advocated for a different set of norms on cyber and information security that emphasizes state sovereignty and prioritizes constraints on the free flow of information over the safeguarding of critical cyber infrastructure and networks.[70]

The diversionary benefits of each country's behavior are also considerable. Iranian provocations tie U.S. resources down in a volatile and often hostile region rather than the Indo-Pacific.[71] Indeed, since May 2019, the United States has deployed 14,000 additional troops to the Middle East, coinciding with a rise in tensions between Iran and the United States.[72] China similarly benefits from Russia's propensity for distracting the United States from China's potentially destabilizing and convention-breaking activities around the world.[73]

These countries' behavior also poses important risks for Beijing, however: for one, the prospect of crisis escalation between the United States and any of these countries would be enormously costly for China. China's objectives toward the Korean Peninsula and North Korea in particular have remained consistent since the beginning of the nuclear crisis in the early 1990s. China seeks to avoid war on the peninsula and inhibit the collapse of the North Korean regime, while also pursuing the peaceful denuclearization of the DPRK. As a result, China likely views U.S.-DPRK sabre rattling with a degree of alarm. Thus, while seeking the survival of the Kim regime as a major priority, Beijing has continued to encourage diplomatic engagement between Washington and Pyongyang even as it offsets the effects of U.S. sanctions.[74] An active conflict in the Persian Gulf that could come about as a result

of U.S.-Iranian tensions would similarly be devastating to China, which relies on the Gulf states for roughly 45 percent of its energy imports.[75]

Next, Iranian and Russian behavior could frustrate China's other strategic partnerships. China maintains a diverse and somewhat contradictory alliance portfolio in the Middle East, including not only Iran but of some its regional adversaries as well. China relies heavily on Saudi Arabia for its energy needs and has pursued a relationship with Israel in part to acquire advanced technologies. Any increase in destabilizing Russian behavior in Africa could similarly complicate Beijing's relationships with states in that region.[76]

This balance of risks and benefits has likely motivated China's policies of cautious enablement—rather than complete endorsement—of North Korean, Russian, and Iranian activities. Even as it maintains rather friendly relations with Moscow, Beijing has refused to recognize the independence of Abkhazia and South Ossetia after the Russo-Georgian war of 2008, and abstained from, rather than vetoing, the 2014 United Nations resolution condemning Moscow's seizure of Crimea.[77] The pursuit of a diplomatic path toward the denuclearization of the Korean Peninsula remains a priority for China, even as it alleviates the effects of economic pressure. Beijing has likewise continued to engage with Tehran, while also responding to Iran's calls for more confrontational policies toward Washington and proposed accession into the Shanghai Cooperation Organization with little enthusiasm.[78]

Conclusion

Russia, Iran, and the DPRK pose a threat within and beyond their respective regions. Russia is the most materially capable of these states and has deftly employed a mix of information, cyber, and proxy warfare to foment instability and erode the legitimacy of democratic political processes across the globe. The threats of Iran and the DPRK are more pronounced in their immediate regions but still undertake activities and behaviors that are global in scope. Iran has demonstrated a willingness to employ its precision-strike capabilities against civilian targets within Saudi borders and is located in a geopolitically sensitive region. Additionally, DPRK missile tests pose a danger to proximate states. Through their cyber intrusions, chemical weapons use, and other coercive and convention-breaking behavior, all of these states threaten to erode international norms.

Each country's provocative behavior can tie down U.S. resources while undermining Washington's global standing. This naturally produces a strong set of incentives for Beijing to build and maintain partnerships with all three of these states, and by establishing bilateral relationships that often span the economic and security domains, China can shield these states from some of the costs of what the United States perceives to be malign behaviors.

Nevertheless, the negative repercussions—real and potential—that each state's behavior poses for China inhibit the extent of these relationships. Iranian escalatory actions threaten China's energy supplies and regional partners, just as destabilizing behavior from Russia might complicate its relations with African states. DPRK recalcitrance and coercive threats also have the potential to yield a miscalculation and a devastating confrontation on the Korean Peninsula. Somewhat paradoxically, the more China insulates these countries from the costs of their activities through more in-depth cooperation, the more Beijing risks increasing the audacious behaviors that can threaten China's key interests.

China is likely well aware of these risks. Beijing will thus be unlikely to deepen its cooperation with these countries solely as a means of confronting and frustrating the United States; instead, U.S. policymakers can expect Beijing to adopt a more delicate approach that seeks to limit, but not completely eliminate, malign behavior. In turn, this means that U.S. policymakers should be cautiously optimistic that the prospects of an in-depth, fully cooperative bi- or multilateral anti-U.S. strategic alliance taking hold across these states will remain remote.

U.S. policymakers may even be able to identify cooperative space with Beijing in addressing some of the more detrimental dimensions of Iranian, Russian, and DPRK actions. With respect to Iran, the United States could find common ground with China in limiting Tehran's destabilizing activities in the Persian Gulf and its anti-Israel proxies, many of which threaten not only global energy supplies but also important Chinese partners.[79] The United States might similarly be able to leverage Chinese support for containing the destabilizing effects of Russian activities in Africa, just as it can rely to some degree on Chinese diplomatic support in reigning in Kim Jong-un.

Even so, U.S. policymakers should harbor no illusions regarding the potential for more robust cooperation from Beijing in implementing comprehensive punitive measures against any one of these countries. China will instead seek to keep Russian, Iran, and DPRK behaviors below a tolerable threshold. The United States can thus anticipate the threat of these states to persist, but not necessarily to become more pronounced, as it moves forward into a new era of Great Power competition marked by increasing rivalry with China.

The authors thank Mike Eisenstadt, John Parker, Shane Smith, and other reviewers for their thoughtful comments on earlier drafts of this chapter.

Notes

[1] On measures short of armed conflict, commonly referred to as gray zone tactics or political warfare, see, for example, Michael Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle Barracks, PA: Army War College Press, December 2015); Van Jackson, "Tactics of Strategic Competition: Gray Zones, Redlines, and Conflicts Before War," *Naval War College Review* 70, no. 3 (Summer 2017), 39–62; Linda Robinson et al., *Modern Political Warfare: Current Practices and Possible Responses* (Santa Monica, CA: RAND, 2018).

[2] Since the end of the Cold War, states have often been referred to by the term *rogue* if they pursue or proliferate weapons of mass destruction; provide material support for terrorist, mercenary, or other nonstate proxies; or habitually violate the principles, norms, and practices of the post–Cold War international order. See, for example, Kelly P. O'Reilly, "Perceiving Rogue States: The Use of the 'Rogue State' Concept by U.S. Foreign Policy Elites," *Foreign Policy Analysis* 3, no. 4 (October 2007), 295–315; Michael Rubin, *Dancing with the Devil: The Perils of Engaging Rogue Regimes* (New York: Encounter Books, 2014), 2–10; Mary Caprioli and Peter F. Trumbore, "Rhetoric Versus Reality: Rogue States in Interstate Conflict," *Journal of Conflict Resolution* 49, no. 5 (October 2005), 770–791; Thomas H. Henriksen, "The Rise and Decline of Rogue States," *Journal of International Affairs* 54, no. 2 (Spring 2001), 349–373; Maria Gabrielsen Jumbert, "How Sudan's 'Rogue' State Label Shaped U.S. Responses to the Darfur Conflict: What's the Problem and Who's in Charge?" *Third World Quarterly* 35, no. 2 (March 2014), 284–299. The phrase *spoiler state* has historically been reserved for countries with enough economic clout to "do damage to the [international financial] system, but not substantial enough to stabilize it." See, for example, Charles P. Kindleberger, "Dominance and Leadership in the International Economy: Exploitation, Public Goods, and Free Rides," *International Studies Quarterly* 25, no. 2 (June 1981), 242–254. The term *spoiler* to describe this category of country appears in David A. Lake, "International Economic Structures and American Foreign Economic Policy, 1887–1934," *World Politics* 35, no. 4 (July 1983), 517–543. And *disrupter* describes states that employ "short-of-war tactics and techniques" in an effort to "disrupt the established international system as well as delegitimize the United States as the leading power of the current world order." See, for example, Isaiah Wilson III and Scott Smitson, "Solving America's Gray-Zone Puzzle," *Parameters* 46, no. 4 (Winter–Spring 2016), 65. For other terms policymakers have used to describe these states, see Gerry J. Simpson, *Great Powers and Outlaw States: Unequal Sovereigns in the International Legal Order* (Cambridge, UK: Cambridge University Press, 2004); Anthony Lake, "Confronting Backlash States," *Foreign Affairs* 73, no. 2 (March–April 1994), 45–55; Ronald Reagan, "The New Network of Terrorist States," *Studies in Conflict and Terrorism* 9, no. 2 (1987), 101–112.

[3] *Summary of the National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense, 2018), 2; *National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 26.

[4] See chapter 1 for this volume's three-attribute operational definition of a Great Power, which consists of unusual capabilities, truly global behavior, and Great Power status attribution by other states in the system. See chapter 3a for a review of how Russia's power tools make its long-term retention of Great Power status uncertain.

[5] On the material and nonmaterial limitations of Russian power and influence, see James Dobbins, Howard J. Shatz, and Ali Wyne, *Russia Is a Rogue, Not a Peer; China Is a Peer, Not a Rogue* (Santa Monica, CA: RAND, 2018); Peter B. Zwack and Marie-Charlotte Pierre, *Russian Challenges from Now into the Next Generation: A Geostrategic Primer*, INSS Strategic Perspectives 29 (Washington, DC: NDU Press, March 2019); Daniel R. Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence [ODNI], February 13, 2018), 36–37, available at <www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA—-Unclassified-SSCI.pdf>.

[6] For more on Russia's lack of a proactive ideology for crafting an alternative world order—especially in comparison to the United States and China—see chapter 3a of this volume.

[7] Thomas Graham, "Let Russia Be Russia: The Case for a More Pragmatic Approach to Moscow," *Foreign Affairs*, November/December 2019, available at <www.foreignaffairs.com/articles/russia-fsu/2019-10-15/let-russia-be-russia>; Julia Gurganus and Eugene Rumer, *Russia's Global Ambitions in Perspective* (Washington, DC: Carnegie Endowment for International Peace, 2019); Mariya Y. Omelicheva, "Critical Geopolitics on Russian Foreign Policy: Uncovering the Imagery of Moscow's International Relations," *International Politics* 53, no. 6 (2016), 708–726.

[8] For an overview of Russian military capabilities, see *Russia Military Power: Building a Military to Support Great Power Aspirations*, DIA-11-1704-161 (Washington, DC: Defense Intelligence Agency [DIA], 2017), available at <www.dia.mil/portals/27/documents/news/military%20power%20publications/russia%20military%20power%20report%202017.pdf>.

[9] Nicole Ng and Eugene Rumer, *The West Fears Russian Hybrid Warfare: They're Missing the Bigger Picture* (Washington, DC: Carnegie Endowment for International Peace, July 2019), available at <https://carnegieendowment.org/2019/07/03/west-fears-russia-s-hybrid-warfare.-they-re-missing-bigger-picture-pub-79412>.

[10] Valery Gerasimov, "Vektory razvitiya voennoi strategii," *Krasnaya Zvezda* [Red Star] (Moscow), April 3, 2019, available at <http://redstar.ru/vektory-razvitiya-voennoj-strategii/>; Dara Massicot, "Anticipating a New Russian Military Doctrine in 2020: What It Might Contain and Why It Matters," *War on the Rocks*, September 9, 2019, available at <https://warontherocks.com/2019/09/anticipating-a-new-russian-military-doctrine-in-2020-what-it-might-contain-and-why-it-matters/>. See also *Assessing Russian Activities and Intentions in Recent U.S. Elections*, Intelligence Community Assessment 2017-01D (Washington, DC: ODNI, January 6, 2017), available at <www.dni.gov/files/documents/ICA_2017_01.pdf>.

[11] Andrei Soldakov and Irina Borogan, "Russia's Approach to Cyber: The Best Defense Is a Good Offence," in *Hacks, Leaks, and Disruptions: Russian Cyber Strategies*, ed. Nicu Popescu and Stanislav Secrieru (Paris: European Union Institute for Security Studies, 2018), 15–24. Additional detail on Russian social media and information operations is provided in chapter 7 of this volume.

[12] For further information, see Soldakov and Borogan, "Russia's Approach to Cyber," 15–24.

[13] Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community*, 8.

[14] Andrew Linder, "Russian Private Military Companies in Syria and Beyond," *New Perspectives in Foreign Policy*, no. 16 (Fall 2018), 17–21; Nathaniel Reynolds, *Putin's Not-So-Secret Mercenaries: Patronage, Geopolitics, and the Wagner Group* (Washington, DC: Carnegie Endowment for International Peace, 2019).

[15] "Russia's 12 UN Vetoes on Syria," *RTE* (Dublin), April 11, 2018, available at <www.rte.ie/news/world/2018/0411/953637-russia-syria-un-veto/>.

[16] John E. Herbst and Jason Marczak, *Russia's Intervention in Venezuela: What's at Stake?* Policy Brief (Washington, DC: Atlantic Council, September 12, 2019), available at <www.atlanticcouncil.org/in-depth-research-reports/report/russias-intervention-in-venezuela-whats-at-stake/>.

[17] Henry Meyer and Ilya Arkhipov, "Russia Wants to Sell Its Missiles to U.S. Allies," *Bloomberg*, June 22, 2018, available at <www.bloomberg.com/news/articles/2018-06-22/russia-wants-to-sell-its-missiles-to-u-s-allies>.

[18] David Brennan, "Russia Deploys First of 'Invulnerable' Hypersonic Missiles Putin Claims Can Defeat Any American Defenses," *Newsweek*, December 27, 2019, available at <www.newsweek.com/russia-deploys-first-invulnerable-hypersonic-missiles-putin-defeat-american-defenses-1479362>.

[19] Elias Groll, "Russian Military Escalates Provocation Campaign in Europe," *Foreign Policy*, October 30, 2014, available at <https://foreignpolicy.com/2014/10/30/russian-military-escalates-provocation-campaign-in-europe/>.

[20] "Besides Doctrine of Peace, Iran Has Strong Military Presence: Commander," Islamic Republic News Agency (IRNA), January 1, 2019, available at <https://en.irna.ir/news/83154430/Besides-doctrine-of-peace-Iran-has-strong-military-presence>. For an overview of Iranian strategic culture, see Michael Eisenstadt, *The Strategic Culture of the Islamic Republic of Iran: Operational and Policy Implications* (Quantico, VA: Marine Corps University Press, 2011).

[21] For an overview, see, for example, Michael Eisenstadt, *Operating in the Gray Zone: Countering Iran's Asymmetric Way of War* (Washington, DC: Washington Institute for Near East Policy, 2020); DIA, *Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance* (Washington, DC: DIA, 2019), available at <www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Iran_Military_Power_LR.pdf>.

[22] Anthony H. Cordesman et al., *U.S.-Iranian Competition: The Gulf Military Balance—I* (Washington, DC: Center for Strategic and International Studies [CSIS], 2013); Michael Wahid Hanna and Dalia Dassa Kaye, "The Limits of Iranian Power," *Survival* 57, no. 5 (September 2015), 173–198; DIA, *Iran Military Power.*

[23] Michael Eisenstadt, *Iran After Sanctions: Military Procurement and Force-Structure Decisions* (London: International Institute for Strategic Studies, December 2017), available at <www.washingtoninstitute.org/uploads/Documents/opeds/Eisenstadt20171219-IISS-chapter.pdf>.

[24] For an overview of several of these, see Seth Jones et al., *Iran's Threat to Saudi Critical Infrastructure: The Implications of U.S.-Iranian Escalation* (Washington, DC: CSIS, 2019).

[25] Shahryar Pasandideh, "Under the Radar, Iran's Cruise Missile Capabilities Advance," *War on the Rocks*, September 25, 2019, available at <https://warontherocks.com/2019/09/under-the-radar-irans-cruise-missile-capabilities-advance/>; Sitakanta Mishra, "Cruise Missiles: Evolution, Proliferation and Future," *Journal of Defence Studies* 6, no. 3 (July 2012), 139–142; Dennis M. Gormley, *Dealing with the Threat of Cruise Missiles* (New York: Routledge, 2013).

[26] Mike R. Pompeo, "Department of State Remarks to Traveling Press," *The Iran Primer*, September 19, 2019, available at <http://iranprimer.usip.org/index.php/blog/2019/sep/18/pompeo-briefing-saudi-attacks>; Natasha Turak, "Drone and Missile Debris Proves Iranian Role in Aramco Attack, Saudi Defense Ministry Claims," CNBC, September 18, 2019, available at <www.cnbc.com/2019/09/18/

saudi-arabia-drone-and-missile-debris-proves-iranian-role-in-attack.html>; Jon Gambrell, Aya Batrawy, and Fay Abuelgasim, "Mike Pompeo Calls Drone Attacks on Saudi Oilfields 'An Act of War' by Iran," Associated Press, September 18, 2019, available at <www.businessinsider.com/pompeo-drone-attacks-saudi-oilfields-act-of-war-by-iran-2019-9>; "DOD Statement on Iranian Ballistic Missile Attacks in Iraq," Department of Defense, January 7, 2010, available at <www.defense.gov/Newsroom/Releases/Release/Article/2052103/dod-statement-on-iranian-ballistic-missile-attacks-in-iraq/>.

[27] Sidharth Kaushal, "Shutdown Showdown: How the Strait of Hormuz Factors into the U.S.-Iran Crisis," *The National Interest*, July 7, 2019, available at <https://nationalinterest.org/feature/shutdown-showdown-how-strait-hormuz-factors-us-iran-crisis-65596?page=0%2C1>; Caitlin Talmadge, "Closing Time: Assessing the Iranian Threat to the Strait of Hormuz," *International Security* 33, no. 1 (Summer 2008), 82–117; Abhijit Singh, "'Dark Chill in the Persian Gulf'—Iran's Conventional and Unconventional Naval Forces," *Maritime Affairs* 6, no. 2 (February 2011), 108–132; Ilan Goldenberg, Jessica Schwed, and Kaleigh Thomas, *In Dire Straits? Implications of U.S.-Iran Tensions for the Global Oil Market* (Washington, DC: Center for a New American Security, 2019).

[28] "Iran Says Has Built 'Smart' Remote-Controlled Submarine," *Eurasia Review*, January 22, 2012, available at <www.eurasiareview.com/22012012-iran-says-has-built-smart-remote-controled-submarine>; DIA, *Iran Military Power*, 51–56.

[29] *Outlaw Regime: A Chronicle of Iran's Destructive Activities* (Washington, DC: Department of State, 2018), 27–30, available at <www.state.gov/outlaw-regime-a-chronicle-of-irans-destructive-activities/>; Jim Garamone, "Selva Details Iranian Oil Attacks, Need for International Efforts," Department of Defense, June 19, 2019, available at <www.defense.gov/explore/story/Article/1879849/selva-details-iranian-oil-attacks-need-for-international-efforts/>; Robert Burns, "U.S. Military Official: Iran Naval Forces Halt 'Provocations,'" Associated Press, March 15, 2018, available at <https://apnews.com/a36e23a8d549464caaea7dc1932babae/US-military-official:-Iran-naval-forces-halt-%27provocation>.

[30] "Iran Making Progress on Basis of Rationality, Resistance in Int'l Arena," IRNA, August 2, 2019, available at <https://en.irna.ir/news/83421453/Iran-making-progress-on-basis-of-rationality-resistance-in-int-l>.

[31] For overviews, see Afshon Ostovar, "The Grand Strategy of Militant Clients: Iran's Way of War," *Security Studies* 28, no. 1 (October 2018), 159–188; *Outlaw Regime*, 9–17; Seth G. Jones, *War by Proxy: Iran's Growing Footprint in the Middle East* (Washington, DC: CSIS, 2019).

[32] Joseph Felter and Brian Fishman, *Iranian Strategy in Iraq: Politics and "Other Means"* (West Point, NY: Combating Terrorism Center, 2008); Michael Knights, "Iran's Expanding Militia Army in Iraq: The New Special Groups," *CTC Sentinel* 12, no. 7 (August 2019).

[33] Daniel Byman, "Iran, Terrorism, and Weapons of Mass Destruction," *Studies in Conflict & Terrorism* 31, no. 3 (February 2008), 169–181; Bruce Hoffman, *Recent Trends and Future Prospects of Iranian Sponsored International Terrorism* (Santa Monica, CA: RAND, 1990); Michael Rubin, "Iran's Revolutionary Guards—A Rogue Outfit?" *Middle East Quarterly* 15, no. 4 (Fall 2008), 37–48.

[34] "France Blames Iran for Foiled Paris Bomb Plot," BBC News, October 2, 2018, available at <www.bbc.com/news/world-europe-45722523>.

[35] *Outlaw Regime*, 15–17.

[36] Michael Eisenstadt, *Iran's Lengthening Cyber Shadow* (Washington, DC: Washington Institute for Near East Policy, 2016).

[37] "Iranian Regime Malign Activities During Negotiations with Iran and During JCPOA," Department of State, October 17, 2019, available at <www.state.gov/iranian-regime-malign-activities-during-negotiations-with-iran-and-during-jcpoa/>.

[38] Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community*, 10.

[39] "Iran Takes Final Step by Abandoning JCPOA Restrictions," IRNA, January 5, 2020, available at <https://en.irna.ir/news/83622509/Iran-takes-final-step-by-abandoning-JCPOA-restrictions>.

[40] David M. Halbfinger, Ben Hubbard, and Ronen Bergman, "The Israel-Iran Shadow War Escalates and Breaks into the Open," *New York Times*, August 28, 2019, available at <www.nytimes.com/2019/08/28/world/middleeast/israel-iran-shadow-war.html>; Nadav Ben Hour and Michael Eisenstadt, "The Great Middle Eastern War of 2019," Washington Institute for Near East Policy, August 20, 2018, available at <www.washingtoninstitute.org/policy-analysis/view/the-great-middle-eastern-war-of-2019>.

[41] "Iran Seizes British Tanker in Strait of Hormuz," BBC News, July 20, 2019, available at <www.bbc.com/news/uk-49053383>.

[42] *National Security Strategy of the United States of America*, 46. The nature of the North Korean regime is exemplified by the sanctions imposed on Pyongyang by the international community. United Nations Security Council (UNSC) resolutions now operative include UNSC 825, May 11, 1993; UNSC 1695, June 15, 2006; UNSC 1718, October 14, 2006; UNSC 1874, June 12, 2009; UNSC 2087, January 22, 2013; UNSC 2094, March 7, 2013; UNSC 2270, March 2, 2016; UNSC 2321, November 30, 2016; UNSC 2356, June 2, 2017; UNSC 2371, August 5, 2017; UNSC 2375, September 3, 2017; and UNSC 2397, December 22, 2017. In addition, the United States, South Korea, Japan, Australia, Russia, and the European Union have adopted individual country sanctions on North Korea. See Eleanor Albert, "What to Know About Sanctions on North Korea," *Council on Foreign Relations*, July 16, 2019, available at <www.cfr.org/backgrounder/what-know-about-sanctions-north-korea>; James Schoff, "Making Sense of UN Sanctions on North Korea," Carnegie Endowment for International Peace, n.d., available at <https://carnegieendowment.org/publications/interactive/north-korea-sanctions>.

[43] *Summary of the National Defense Strategy of the United States of America*, 2.

[44] Gian Gentile, *Four Problems on the Korean Peninsula: North Korea's Expanding Nuclear Capabilities Drive a Complex Set of Problems* (Santa Monica, CA: RAND, 2019).

[45] Nuclear Threat Initiative, "North Korea," August 2019, available at <www.nti.org/learn/countries/north-korea/>.

[46] Andrew Scobell and John M. Sanford, *North Korea's Military Threat: Pyongyang's Conventional Forces, Weapons of Mass Destruction, and Ballistic Missiles* (Carlisle Barracks, PA: Strategic Studies Institute, 2007).

[47] Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community*, 28.

[48] Ibid., 8.

[49] UNSC, "Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)," S/2019/171, February 21, 2019, 34, available at <www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2019_171.pdf>.

[50] Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community*, 8.

[51] UNSC, "Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)," February 21, 2019, 44–45.

[52] UNSC, "Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)," S/2019/691, July 31, 2019, 135, available at <www.securitycouncilreport.

org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2019_691.pdf>.

[53] "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups," Department of the Treasury, September 13, 2019, available at <https://home.treasury.gov/index.php/news/press-releases/sm774>; "North Korean Hackers Blamed for Wave of Cyberattacks on Banks," *South China Morning Post* (Hong Kong), October 3, 2018, available at <www.scmp.com/news/asia/east-asia/article/2166869/north-korean-hackers-blamed-wave-cyberattacks-banks>; UNSC, "Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)," July 31, 2019, 109–112.

[54] Jim Finkle, "Cyber Security Firm: More Evidence North Korea Linked to Bangladesh Heist," Reuters, April 3, 2017, available at <www.reuters.com/article/us-cyber-heist-bangladesh-northkorea-idUSKBN1752I4>.

[55] UNSC, "Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)," July 31, 2019, 4.

[56] "Update on Sony Investigation," Federal Bureau of Investigation, December 19, 2014, available at <www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation?utm_campaign=emailImmediate&utm_medium=email&utm_source=national-press-releases&utm_content=386194>; David Sanger, David Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More," *New York Times*, October 15, 2017, available at <www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html>.

[57] Greg Walters, "North Korea's Counterfeit Benjamins Have Vanished," *Vice News*, March 16, 2016, available at <www.vice.com/en_us/article/vb8pk9/north-korea's-counterfet-benjamins-have-vanished>. Also see Sheena Chestnut Greitens, *Illicit: North Korea's Evolving Operations to Earn Hard Currency* (Washington, DC: Committee for Human Rights in North Korea, 2014).

[58] Raphael F. Perl, *Drug Trafficking and North Korea: Issues for U.S. Policy*, RL32167 (Washington, DC: Congressional Research Service, January 25, 2007).

[59] Mike Ives, "Crystal Meth Is North Korea's Trendiest Lunar New Year's Gift," *New York Times*, February 12, 2019; Kim Young Il, "North Korea and Narcotics Trafficking: A View from the Inside," *North Korea Review* 1, no. 1 (March 2004).

[60] Julian Ryall, "North Korea 'Ramps Up Manufacture of Illegal Drugs' amid Sanctions," *Deutsche Welle*, August 21, 2017, available at <www.dw.com/en/north-korea-ramps-up-manufacture-of-illegal-drugs-amid-sanctions/a-40169753>.

[61] For an overview of Chinese-Iranian relations, see Ariane Tabatabai and Dina Esfandiary, *Triple-Axis: Iran's Relations with Russia and China* (New York: Bloomsbury Publishing, 2018); Scott W. Harold and Alireza Nader, *China and Iran: Economic, Political, and Military Relations* (Santa Monica, CA: RAND, 2012).

[62] Derek Scissors, "China Global Investment Tracker," American Enterprise Institute, available at <www.aei.org/china-global-investment-tracker/>.

[63] Harold and Nader, *China and Iran*, 6–7.

[64] "Bilateral Trade Between China and Islamic Republic of Iran in 2018, Product: 2709 Petroleum Oils and Oils Obtained from Bituminous Minerals, Crude," International Trade Commission. Most of these imports took place prior to the reimposition of U.S. sanctions and the expiration of U.S. waivers. See Dan Katz, "Despite Sanctions, China Is Still Doing (Some) Business with Iran," Atlantic Council, October 1, 2019, available at <www.atlanticcouncil.org/blogs/iransource/despite-sanctions-china-is-still-doing-some-business-with-iran/>.

[65] Vassily Kashin, "Tacit Alliance: Russia and China Take Military Partnership to New Level," Carnegie Moscow Center, October 22, 2019.

[66] Ibid.; Dmitri Trenin, "U.S. Obsession with Containment Driving China and Russia Closer," Carnegie Moscow Center, July 31, 2019.

[67] Rajeswari Pillai Rajagopalan, "Russia-China Strategic Alliance Gets a New Boost with Missile Early Warning System," *The Diplomat*, October 25, 2019, available at <https://thediplomat.com/2019/10/russia-china-strategic-alliance-gets-a-new-boost-with-missile-early-warning-system/>.

[68] Le Jeong-ho, "China-North Korea Trade Up 14.3 Percent in First Half to US$1.25 Billion," *South China Morning Post* (Hong Kong), July 24, 2019, available at <www.scmp.com/news/china/diplomacy/article/3019940/chinas-first-half-trade-north-korea-recovers-old-allies>.

[69] Marshall Billingslea, *Statement Before the U.S. House Financial Services Subcommittee on Monetary Policy and Trade*, September 26, 2018, available at <https://home.treasury.gov/news/press-releases/sm496>.

[70] See, for example, James Carden, "Time to Pursue an International Cyber Treaty?" *The Nation*, April 30, 2019, available at <www.thenation.com/article/international-cyber-treaty-russia-china-dnc/>; United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," A/C.1/73/L.27, October 22, 2018, available at <https://undocs.org/A/C.1/73/L.27>; United Nations General Assembly, "Developments in the Field of Information and Telecommunications in the Context of International Security," A/C.1/73/L.37, October 18, 2018, available at <https://undocs.org/A/C.1/73/L.37>.

[71] John W. Garver, "Is China Playing a Dual Game in Iran?" *The Washington Quarterly* 34, no. 1 (Winter 2011), 75–88.

[72] "DOD Statement on Deployment of Additional U.S. Forces and Equipment to the Kingdom of Saudi Arabia," Department of Defense, October 11, 2019, available at <www.defense.gov/Newsroom/Releases/Release/Article/1987575/dod-statement-on-deployment-of-additional-us-forces-and-equipment-to-the-kingdo/>.

[73] Andrea Kendall-Taylor and David Shullman, "A Russian-Chinese Partnership Is a Threat to U.S. Interests," *Foreign Affairs*, May 14, 2019, available at <www.foreignaffairs.com/articles/china/2019-05-14/russian-chinese-partnership-threat-us-interests>.

[74] Shannon Tiezzi, "Why China Isn't Mourning the Collapse of the Trump-Kim Summit," *The Diplomat*, March 1, 2019, available at <https://thediplomat.com/2019/03/why-china-isnt-mourning-the-collapse-of-the-trump-kim-summit/>.

[75] Alexander Simoes and César Hidalgo, *The Economic Complexity Observatory: An Analytical Tool for Understanding the Dynamics of Economic Development*, Workshops at the 25th AAAI Conference on Artificial Intelligence, August 2011, available at <https://oec.world>.

[76] Vita Spivak, "Russia and China in Africa: Allies or Rivals?" Carnegie Moscow Center, October 25, 2019, available at <https://carnegie.ru/commentary/80181>. For an overview of Russian activities in Africa, see Paul Stronski, *Late to the Party: Russia's Return to Africa* (Washington, DC: Carnegie Endowment for International Peace, 2019).

[77] Leon Aron, "Are Russia and China Really Forming an Alliance?" *Foreign Affairs*, April 4, 2019, available at <www.foreignaffairs.com/articles/china/2019-04-04/are-russia-and-china-really-forming-alliance>. For an alternative view, see Kendall-Taylor and Shullman, "A Russian-Chinese Partnership Is a Threat to U.S. Interests."

[78] Alex Vatanka, "China's Great Game in Iran," *Foreign Policy*, September 5, 2019, available at <https://foreignpolicy.com/2019/09/05/chinas-great-game-in-iran/>.

[79] Brett McGurk, "China's Risky Middle East Bet," *The Atlantic*, April 29, 2019, available at <www.theatlantic.com/ideas/archive/2019/04/chinas-risky-middle-east-bet/588166/>.