Marine with 3rd Battalion, 7th Marine Regiment, 1st Marine Division, scales wall during counter-IED training at Marine Corps Air Ground Combat Center, Twentynine Palms, California, July 25, 2019 (U.S. Marine Corps/Colton Brownlee)

Countering Threat Networks to Deter, Compete, and Win

Competition Below Armed Conflict with Revisionist Powers

By Vayl S. Oxford

The current geopolitical environment is the most complex, dynamic, and dangerous the United States has ever faced. During the Cold War, the Nation squared off against a superpower rival in the Soviet Union, and since its collapse, the United States has battled an assortment of rogue regimes and violent extremist organizations (VEOs). While rogue regimes and VEOs remain a threat to U.S. and allies' security, the United States must also contend with the threat posed by not one but two major state competitors, China and Russia, each fielding significant nuclear and conventional forces.[1] The 2018 National Defense Strategy directs the Department of Defense (DOD) to focus on "long-term, strategic competition" with these two "revisionist powers," whose regional and global ambitions are at odds with those of the United States and its allies, while also continuing to keep rogue regimes and VEOs at bay.[2]

Vayl S. Oxford is Director of the Defense Threat Reduction Agency.

As a Department, we are well versed in deterring state adversaries from initiating major armed conflicts against ourselves or our allies by maintaining nuclear and conventional forces capable of imposing severe costs against overt, direct military aggression by any state actor. However, the scope of the threat posed by revisionist powers extends well beyond these types of hostilities. While the United States must continue to seek cooperation with Russia and China in areas where our interests align, we must also recognize those areas where Moscow and Beijing seek to challenge U.S. military primacy and undermine the Nation and its allies. In such cases, the United States must be prepared to counter a broad range of malign activities carried out below the threshold of state-on-state armed conflict. These global threat networks can include leveraging rogue states, VEOs, and witting and unwitting actors in the private sector. To counter the efforts of revisionist powers to exploit the competition continuum between war and peace, we must recalibrate existing tools and approaches—including those initially developed after 9/11 to counter VEOs—in order to regain the initiative in the present era of Great Power competition.

The Defense Threat Reduction Agency (DTRA), which I have the honor to lead, is the DOD combat support agency responsible for enabling the Defense Department, the U.S. Government, and our international partners to counter and deter transregional and multidomain weapons of mass destruction (WMD) and improvised threat networks.[3] In this capacity, DTRA plays a key role in ongoing U.S. efforts to illuminate and dismantle VEO threat networks. As DOD refocuses on the long-term challenge posed by revisionist powers, I believe it is critically important to consider applying the best practices and lessons learned from combating nonstate networks to similarly uncover and counter the covert and deniable machinations of state actors and their global networks. These revisionist powers employ their own networks and exploit the networks of other state and nonstate entities. Applying our countering threat networks toolkit to reveal and stymie revisionist power activities across the conflict continuum is an important component of broader efforts to compete with Beijing and Moscow below the level of armed conflict.

This article describes the competition continuum and illustrates some of the actions of Russia and China within this space, identifies tools and approaches first developed to counter nonstate threat networks that can be adapted to counter revisionist powers and their global threat networks across the competition continuum, and discusses the potential benefits and possible risks of the United States pursuing these courses of action.

Competition Continuum

U.S. security is underpinned by a robust, flexible nuclear deterrent and powerful conventional forces. These capabilities deter potential adversaries from launching direct attacks against the United States due to the certain and severe costs Washington can impose in response.

Nuclear deterrence and conventional forces, however, cannot forestall all forms of aggression. Moreover, the current threat environment is described as a world of long-term competition that is exacted through a combination of cooperation, competition below armed conflict, and armed conflict.[4] While state adversaries seek to avoid direct armed conflict with the United States, revisionist powers have shrewdly calculated the thresholds below which they can operate to further their own interests—often at the expense of the United States or its allies—without triggering an automatic U.S. military response. General Joseph Votel, former commander of U.S. Central Command, described this "gray zone" between peace and armed conflict as a space "characterized by intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war."[5] Russia and China view the United States as the principal obstacle to realization of their regional and global ambitions. Both revisionist powers operate across the competition continuum as part of a broader, ongoing campaign to undermine U.S.-led alliances and regional security arrangements, erode U.S. global power and leadership, and challenge the rules-based international order. These efforts include several components.

Covert, Deniable Hybrid Operations. Russia used military forces operating without clearly identifiable national military markings as part of its illegal seizure and annexation of Crimea, deploying these forces across Ukraine's borders while denying its direct military involvement.[6] These "little green men" provide Russia a covert means to seize key targets or stir up internal dissent as a pretext for military intervention.[7] Similarly, China has deployed a supposed "fishing fleet" of ships in the Western Pacific that operates as a shadow maritime militia.[8] These vessels often loiter near disputed areas, harassing the maritime craft of other nations as part of China's broader effort to force other parties to drop their claims to reefs, islands, and waters. In both cases, these forces allow Moscow and Beijing to pursue key national objectives while simultaneously denying responsibility. Even if improbable, these denials can complicate efforts to attribute their involvement and organize a response.

Use of WMD for Assassination on Foreign Soil. With the attempted assassination of Sergei Skripal in Salisbury, United Kingdom, in March 2018,[9] Russia demonstrated its willingness to use advanced chemical weapons on the soil of a North Atlantic Treaty Organization (NATO) member.[10] In conducting the attack, Moscow violated the Chemical Weapons Convention, showed contempt for international norms, and demonstrated that it is prepared to employ a sophisticated WMD with little consideration of collateral damage. Moreover, in its efforts to hinder an international investigation by the Organization for the Prohibition of Chemical Weapons, Moscow was joined by Beijing, which often shares Russia's general opposition to greater international transparency or accountability.[11]

Supporting Nonstate Proxies. Russia has embraced the use of nonmilitary

actors, such as private security companies, to advance its interests. These mercenaries (often former Russian military personnel) remain involved in the ongoing Ukrainian conflict and participated in an ill-fated February 2018 attempt to attack a combined Kurdish and U.S. force engaged in anti–Islamic State (IS) operations in Syria.[12] Similar to little green men, private military companies can operate below the threshold of state-on-state armed conflict while the Kremlin publicly denies involvement.

Enabling/Failing to Prevent Proliferation of Weapons and Sanctions Enforcement. Russia and China have a decidedly mixed record regarding the proliferation of weapons or dual-use items (goods or technologies that can have civilian or military applications), including items associated with WMD or improvised threats. The State Department, for example, has reported that China continues "to supply missile programs of proliferation concern" and that Russia remains engaged in dual-use activities that raise questions regarding its compliance with the Biological Weapons Convention.[13] In addition, terrorists and insurgents building improvised explosive devices (IEDs) in Syria, Iraq, and Afghanistan regularly procure items from both countries, including fertilizer purchased from Russian suppliers and electronic components purchased from Chinese suppliers.[14]

More broadly, Russia's and China's enforcement of sanctions against bad actors—including states illegally pursuing WMD and their delivery systems (or seeking to sell them)—is often lax. This is sometimes due to a lack of capacity to enforce sanctions; in other cases, it reflects a deliberate decision to deprioritize enforcement or allow these activities to continue. The United States, for example, has provided Beijing with photographic evidence of North Korean ships illegally loading petroleum from vessels (registered to third nations) just off China's coastline, well within an area where Chinese naval or coast guard craft should challenge and halt these types of transfers. Russia has also allowed similar practices, and both Beijing and Moscow have blocked efforts at the United Nations (UN) to publicly report these violations,[15] reducing the effectiveness of UN sanctions against Pyongyang.[16]

Challenging, Breaching, and Infiltrating Sovereign Boundaries (Land, Sea, and Air). Despite frequently emphasizing the importance of sovereignty to deflect criticism of internal activities, Russia and China have increasingly challenged sovereign boundaries in the land, sea, and air domains. As noted, Russian little green men infiltrated Ukrainian territory, leading several NATO members and partners that border Russia to step up efforts to secure their borders and monitor Russian military activity near their territories. Moscow and Beijing have also engaged in the provocative behavior of sending military aircraft and ships on patrols or excursions that are violations or near violations of U.S., allied, or partner airspace or waters. U.S., British, and Japanese aircraft, for example, have scrambled to intercept Russian bombers that have entered national airspace or air defense identification zones; the Japanese government reported conducting nearly 1,000 of these intercepts against Chinese or Russian aircraft in the past year.[17] In addition, in the last 2 years, Japan, Vietnam, and the Philippines have charged China with violating their territorial waters, using ships to engage in provocative, dangerous behavior that has resulted in the collision and sinking of vessels (as well as many near misses).

It is clear from these examples that Beijing and Moscow are engaged in a broad range of activities below the threshold of state-on-state armed conflict to challenge the United States and its allies in a manner that they believe will not result in a U.S. military response. In order to meet this challenge, the United States can draw on the lessons learned from countering nonstate threat networks in Iraq, Afghanistan, and around the world. For all their important differences, state and nonstate actors seeking to do harm to the United States and its allies employ similar means, and several of the tools honed during 18 years of battling terrorists and insurgents have utility in shedding light on, and pushing back against, Russia and China across the competition continuum.

Countering Threat Networks

The U.S. military developed its current concept of threat networks in the years after 9/11 due to a recognition that many of the insurgents and terrorists encountered by U.S. and coalition forces were not confined by borders or rigid state or bureaucratic structures.[18] These threat networks usually sought to remain hidden from view, eschewing uniforms or other identifying characteristics in order to blend in with civilian populations. Many had links or ties with communities across state borders that allowed them to recruit additional members and draw financial support from multiple sources. In many cases, they also cultivated transnational supply chains, including legitimate businesses unaware of the intended end use of their products.

In response, the U.S. Armed Forces developed a methodology and strategy for countering these nonstate threat networks that combined aspects of military engagement, security cooperation, and deterrence to apply steady pressure while disrupting their direct and indirect sources of support.[19]

Threat Network Illumination. To target threat networks, the totality of the network must be understood—including the relationships that allow them to operate. Numerous tools and skill sets are levied against the network, coupled with specialized U.S. human capital and partner nation governments and agencies. When effectively collected and assessed, this information sheds light on a threat network's internal and external relationships and reveals key nodes (such as their leadership and critical enablers). As David Richard Doran notes, "Understanding how adversaries use threat networks globally to compete with us below the threshold of traditional armed conflict is a critical first step to identifying opportunities" to mitigate their effects. This detailed picture of a threat network informs actions to exploit, disrupt, or degrade the network and ultimately scatter or collapse the larger interconnected structure.[20]

Ukrainian soldiers decontaminate vehicles as part of simulated chemical exposure event during field training exercise portion of Rapid Trident 2019, September 24, 2019, near Yavoriv, Ukraine (U.S. Army National Guard/Amanda H. Johnson)

Teaming to Defeat Networks. In many cases, however, the illuminated threat network reveals a complex entity with links and nodes across multiple jurisdictions and borders. To disrupt and defeat such networks, we must build teams across DOD, its U.S. Government partners, and with foreign counterparts to bring together the expertise, capabilities, and authorities necessary to isolate and take action against key network nodes. As Admiral Kurt Tidd, former commander of U.S. Southern Command, noted in March 2018, in order to combat nonstate threat networks that can include "drug traffickers, human smugglers, terrorist supporters, arms dealers and money launderers," it is vital for the U.S. Government to "integrat[e] our expertise and tools with those of committed [foreign] partners to remain more adaptive and capable than adversaries who exploit or target our citizens."[21] Dismantling a network may require, for example, combined operations by the United States and allied and partner governments, to include financial, customs, law enforcement, and military task force activities that starve VEOs of resources, prevent them from adding recruits, uncover their weapons caches and hideouts, and allow for the apprehension and prosecution or elimination of their leadership. In many cases, DOD is in a supporting role to an interagency or international partner that has the placement and authority to take the actions that maintain or achieve U.S. objectives.[22]

DTRA and its U.S. Government and international partners have worked hard to illuminate the activities of nonstate threat networks and assemble combined teams to counter the multifaceted challenge posed by this type of adversary. This experience, described in two case studies below, provides tools and templates that can prove valuable to countering malign activities short of armed conflict by major powers that employ similar methods.

Developing a Toolkit to Illuminate Threat Networks

Beginning in 2003, U.S. forces began encountering IEDs on the roads and highways of Iraq and soon thereafter in Afghanistan. These low-cost devices were soon inflicting injuries, causing fatalities, and slowing operations by U.S. forces deployed across both countries.[23] The U.S. Army responded to this threat by forming a task force, the Joint IED Defeat Organization, which evolved over time to become a core mission of DTRA.

Early U.S. Government efforts to counter IEDs struggled to assess large volumes of information collected from multiple sources on insurgents, the types of attacks carried out, and the variations of explosive devices employed. In addition to the challenge of sifting through mountains of data, different stakeholders faced serious technical challenges when they attempted to share this

Marine dresses in chemical, biological, radiological, and nuclear defense gear for sensitive site exploitation training during exercise Eager Lion 2019 in Jordan, August 27, 2019 (U.S. Marine Corps/Rhita Daniel)

information with each other. In response, U.S. Government teams developed cutting-edge analytical tools to integrate hundreds of data sets from previously disparate platforms and partners. DTRA continues to work hand-in-glove with its U.S. Government partners to enable information-sharing and continue integration of new data sets to further improve the fidelity of analyses of VEO strategies, tactics, and day-to-day operations. These teams also pioneered processes bringing together regional and functional subject matter experts directly with programmers in order to tailor existing tools to meet unique requirements. This nimble approach to metadata analytics helps DOD keep pace with threat networks that constantly adapt in response to U.S., allied, and partner actions against them.

All the tools described above improve U.S. commanders' situational awareness and ability to execute decisive actions against a threat network's key nodes. In the IED and improvised threat space, DTRA's flexible, evolving toolkit has provided timely and actionable assessments to effectively target key nodes associated with VEO improvised threats in Iraq, Afghanistan, and Syria.

Building Regional Partnerships

The devastation and chaos of the Syrian civil war pose an ongoing threat to regional security and stability, including several U.S. partners and allies. In addition to representing an acute humanitarian crisis, this flow of people raises a host of security concerns for nearby states, one of which is preventing VEO fighters and weapons—including chemical weapons or precursors—from leaving Syria. At various stages of the country's civil conflict, the security of Syrian government stocks of chemical weapons was in doubt, raising the possibility they could be seized by a terrorist organization or fall into the hands of an enterprising smuggler. In addition, IS's success in developing its own chemical weapons prompted fears it might attempt to remove these weapons from Syria to conduct attacks on U.S. allies or partners in the Middle East or further abroad.

Based on these threats, the United States, together with key allies such as the United Kingdom, partnered with Jordan and Lebanon to better protect their borders and prevent bad actors from smuggling chemical weapons, precursor materials, or other WMD-related items into their countries. Meeting this objective required a comprehensive, around-the-clock monitoring of borders that run along rough terrain, often in remote areas far from existing infrastructure. Operationally, smugglers and IS fighters needed to be distinguished from civilian refugees, while weapons, dual-use items, and other improvised

threat materials needed to be detected and identified. The scope of the challenge required developing innovative, purpose-built "hardware and software" solutions for each partner state that brought together best practices from multiple actors, from local border guards to British military trainers and U.S. information technology engineers.

In Jordan, DTRA played a central role in orchestrating and developing the Jordan Border Security Program, which to date has provided a layered defense across more than 400 kilometers of border.[24] The program, which will soon fully transition to the Jordanian government, has taken a holistic approach to countering the threat of potential WMD proliferation through enhanced border detection and response capabilities. Physical barriers are provided where appropriate, while improved situational awareness is supplied by a network of watch towers equipped with sensors, radars, and other surveillance technology. Information streams are connected to battalion-, brigade-, and national-level operations centers, where they can be combined with other data or assessments that allow Jordanian authorities to quickly determine which resources to deploy to mitigate a threat. In circumstances where border personnel suspect the presence of a possible WMD or chemical, biological, radiological, or nuclear material, the program has also equipped and trained specialized mobile units to quickly respond and conduct an initial assessment of the potential WMD threat. Tying all this technical equipment and know-how together is a set of robust training programs for Jordanian border, law enforcement, military, technical, and disaster response personnel, as well as an equipment repair facility to ensure Jordanian officials can sustain the system's operations. Similarly, DTRA has partnered with Southeast Asian nations to improve the security of their maritime domains against WMD trafficking by nonstate actors, as well as trafficking by rogue regimes such as North Korea and Iran.

These projects have significantly enhanced the capacity of key U.S. partners to detect and interdict WMD and related materials at their borders. This WMD-focused assistance has broader second-order effects, improving these partner nations' overall border security and aiding their capabilities to apprehend VEO members and sympathizers and to identify and intercept conventional weapons. Critically, these combined U.S., allied, and partner teams provided the dynamic collaboration required to counter threat networks in and around Syria as well as trafficking networks in the South China Sea and nearby waters. As the National Defense Strategy emphasizes, this bolsters U.S. partnerships in parts of the world where revisionist powers are eager to exert malign influence through regional partnerships at the expense of U.S. objectives.

Application to Great Power Competition

State and nonstate actors differ in many critical ways, including the scale and scope of resources available to pursue their objectives. The methods utilized to counter nonstate threat networks, however, can provide a way ahead for uncovering the covert networks employed by state actors across the competition continuum, including Chinese and/or Russian use of deniable assets, proxies, and covertly funded, supported, or enabled nonstate actors. China and Russia work to keep their covert, hybrid activities cloaked or, at the very least, screened by misinformation; if revealed, they assess their networks will become fragile or ineffective or otherwise become a liability.

The toolkit developed to illuminate nonstate threat networks thus represents a potentially powerful means to push back against China and Russia across the competition continuum. For example, further exposing the web of Chinese and Russian complicity with North Korea's sanctions evasion (by identifying specific ships involved, their links back to Chinese or Russian firms, and the exact location of illicit transfers) provides U.S. decision-makers with expanded options to increase pressure on them to fully enforce UN sanctions.

Uncovering the connections with proxies can also provide U.S. decision-makers with options to counter this type of activity. The Chinese or Russian government entities involved with nonstate proxies can be identified by a demarche and/or targeted by sanctions. If the United States chooses to go public with information on the extent of Russian or Chinese state involvement, this could have a chilling effect on the proxy's future ability to conduct its operations; once the association is public, China or Russia may cease its support to the now-exposed proxy, thus degrading its malign activity. In other cases, this threat illumination can uncover how these states employ parastate actors for the purposes of espionage or even kinetic action abroad and in turn allow the United States and its allies response options such as demarches or other types of disruptive actions against Beijing or Moscow.

In addition, projects to secure land and maritime boundaries against illicit WMD smuggling networks provide U.S. partners and allies with critical capabilities to identify and interdict proliferation of WMD-related materials, dual-use items, and delivery systems tied to Russia or China. Disrupting these networks can help prevent proliferation of these materials to nonstate actors seeking WMD capabilities.

These efforts to prevent proliferation of WMD and related materials across land borders also build broader partner nation border security capabilities that can be applied to U.S. and allied efforts to stymie certain Chinese and Russian activities below the level of armed conflict. Moscow has breached land boundaries to move forces, seize strategic territory, undermine institutions, and conduct covert attacks (including with WMD), while China repeatedly interferes with maritime boundaries in its efforts to bully its neighbors into accepting its control over the Western Pacific. DTRA's efforts to help Jordan better detect and interdict WMD and related materials at its borders and to help the Southeast Asian nations detect and interdict WMD trafficking in their maritime domains are also relevant to countering revisionist power efforts to

Bahrain Defense Force servicemember showcases protective chemical and biological protective suit to exercise participants of United Arab Emirates Union Defense Force, at Al Wathba, UAE training facility, as part of exercise Leading Edge, January 28, 2013 (U.S. Marine Corps/Leon M. Branchaud)

infiltrate and interfere with the sovereign space of U.S. allies and partners.

The United States has a range of options to counter Russia and China across the competition continuum, including tools and approaches honed during the battle against VEOs. Now that the United States recognizes the challenge posed by Moscow and Beijing within this space, it is important that we adapt to meet the strategic environment in which we now operate.

Potential Risks

In doing so, however, it is also critical to proceed carefully, deliberately, and, wherever possible, in tandem with allies and partners. State and nonstate threat networks share a number of features and operating procedures, but the risks in countering state networks are significantly higher and must be factored into the calculus of U.S. decisionmakers. When engaging with nonstate threat networks in the past, the United States could act without the risk of initiating a strategic conflict that posed an existential threat to the country. In the future, the United States will need to carefully consider whether to target a key node of a state network—such as a foreign military intelligence official funneling weapons to a nonstate proxy—if undertaking such an action could prompt a retaliatory attack on U.S. forces. Moreover, in addition to the immediate costs incurred, this response by a revisionist power could potentially escalate to a state-on-state armed conflict.

Another risk is that many revisionist power malign activities involve (sometimes witting, sometimes unwitting) third-party actors. The potential consequences of alienating third parties must also be taken into account, particularly as long-term success in countering Russia and China will require deepened cooperation with current and new U.S. partners or allies.

Conclusion

Russia and China use a wide range of unconventional methods to achieve their objectives of undermining international order and fracturing U.S.-led regional security architectures. Thanks to robust U.S. nuclear and conventional capabilities, these state actors remain deeply wary of the risks of direct armed conflict with the United States and its allies and partners. This has pushed their competition with the United States below the threshold of state-on-state armed conflict that is neither a stable peace nor a hot war.

The United States has demonstrated the capability to operate across the conflict continuum, though we must take steps to adapt our operations to this

new strategic environment and increase the capacity to conduct such actions on a larger scale to counter revisionist and rogue states' global threat networks. Tools and approaches developed to reveal and dismantle nonstate threat networks have considerable value in countering the malign activities of state adversaries and their agents and proxies. As the United States gears up for the challenge posed by revisionist powers, DTRA stands ready to support U.S., allied, and partner efforts to illuminate adversary threat networks and enable action to exploit, disrupt, and defeat these networks and their operations. **JFQ**

Notes

[1] Kristina Hummel, "A View from the CT Foxhole: Vayl S. Oxford, Director, Defense Threat Reduction Agency," *CTC Sentinel* 12, no. 3 (March 2019), 11, available at <https://ctc.usma.edu/view-ct-foxhole-vayl-s-oxford-director-defense-threat-reduction-agency/>.

[2] *Summary of the 2018 National Defense Strategy: Sharpening the American Military's Competitive Edge* (Washington, DC: Department of Defense [DOD], 2018), 2.

[3] "Statement of Vayl Oxford," House Armed Services Committee, Subcommittee on Intelligence and Emerging Threats and Capabilities, April 3, 2019, available at <https://armedservices.house.gov/?a=Files.Serve&File_id=C5D34C82-5AE0-4753-B798-47C9DE77919E>. The phrase *improvised threats* refers to improvised explosive devices (IEDs), unmanned aerial systems, and other threats to U.S., allied, and partner forces that are sourced, developed, assembled, and employed outside of the processes associated with the more formal, structured, and deliberate development of weapons associated with weapons fielded by state armed forces.

[4] Joint Doctrine Note 1-19, *Competition Continuum* (Washington, DC: The Joint Staff, June 3, 2019), v, available at <www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf>.

[5] Joseph L. Votel et al., "Unconventional Warfare in the Gray Zone," *Joint Force Quarterly* 80 (1st Quarter 2016), 102, available at <https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/>.

[6] "Top NATO Commander Concerned About 'Little Green Men' in Moldova," Reuters, September 17, 2014, available at <www.atlanticcouncil.org/blogs/natosource/top-nato-commander-concerned-about-little-green-men-in-moldova>.

[7] Robert R. Leonhard, Stephen P. Phillips, and Johns Hopkins University Applied Physics Laboratory Assessing Revolutionary and Insurgent Strategies (ARIS) Team, *"Little Green Men": A Primer on Modern Russian Unconventional Warfare, Ukraine 2013–2014* (Fort Bragg, NC: U.S. Army Special Operations Command, July 2016), available at <www.jhuapl.edu/Content/documents/ARIS_LittleGreenMen.pdf>.

[8] Gregory B. Poling, "Illuminating the South China Seas Dark Fishing Fleets," Center for Strategic and International Studies, January 9, 2019, available at <https://ocean.csis.org/spotlights/illuminating-the-south-china-seas-dark-fishing-fleets/>.

[9] "Imposition of Chemical and Biological Weapons Control and Warfare Elimination Act Sanctions on Russia," press statement, Department of State, August 8, 2018, available at <www.state.gov/imposition-of-chemical-and-biological-weapons-control-and-warfare-elimination-act-sanctions-on-russia/>.

[10] "Novichok Nerve Agent Use in Salisbury: UK Government Response, March to April 2018," Government of the United Kingdom, April 18, 2018, available at <www.gov.uk/government/news/novichok-nerve-agent-use-in-salisbury-uk-government-response>.

[11] Their joint efforts, however, failed to carry votes on investigations into the use of chemical weapons in the Salisbury case or regarding the conflict in Syria; unlike the United Nations (UN) Security Council, the major powers do not have special veto powers separating them from other state parties to the Chemical Weapons Convention.

[12] Sergei Khazov-Cassia and Robert Coalson, "Russian Mercenaries: Vagner Commanders Describe Life Within the 'Meat Grinder,'" Radio Free Europe/Radio Liberty, March 14, 2018, available at <www.rferl.org/a/russian-mercenaries-vagner-commanders-syria/29100402.html>.

[13] *2017 Report on Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments* (Washington, DC: Department of State, 2017), available at <www.state.gov/2017-report-on-adherence-to-and-compliance-with-arms-control-nonproliferation-and-disarmament-agreements-and-commitments/#Missile4>.

[14] Fatima Bhojani, "How ISIS Makes IEDs: The Supply Chain of Terrorism," *Foreign Affairs*, March 2, 2016, available at <www.foreignaffairs.com/articles/2016-03-02/how-isis-makes-ieds>.

[15] "Statement by Ambassador Haley on Reports of Russian Violations of UN Security Council Resolutions," U.S. Mission to the United Nations, August 3, 2018, available at <https://usun.usmission.gov/statement-by-ambassador-haley-on-reports-of-russian-violations-of-un-security-council-resolutions/>; "U.S. Accuses Russia of Altering UN Report on North Korea Sanctions," Radio Free Europe/Radio Liberty, September 14, 2018, available at <www.rferl.org/a/u-s-accuses-russia-of-altering-un-report-on-north-korea-sanctions/29489277.html>.

[16] Lolita C. Baldor, "U.S. Defense Chief Sends Message to China with Photos Showing North Korea Sanctions Go Unenforced," Associated Press, June 11, 2019, available at <www.militarytimes.com/news/pentagon-congress/2019/06/11/acting-us-defense-chief-shared-photos-with-chinese-counterpart-that-show-north-korea-sanctions-go-unenforced/>.

[17] "Japan Says Fighter Jets Scramble after Russian Military Aircraft Violate Airspace," Radio Free Europe/Radio Liberty, June 21, 2019, available at <www.rferl.org/a/japan-says-fighter-jets-scramble-after-russian-military-aircraft-violate-airspace/30011921.html>; "Statement by General Terrence J. O'Shaughnessy," Senate Armed Services Committee (SASC), February 26, 2019, available at <www.armed-services.senate.gov/imo/media/doc/OShaughnessy_02-26-19.pdf>.

[18] SASC, "Statement by General Terrence J. O'Shaughnessy."

[19] Joint Publication 3-25, *Countering Threat Networks* (Washington, DC: The Joint Staff, December 21, 2016), viii, available at <www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_25.pdf>.

[20] David Richard Doran, "Outmatched: Shortfalls in Countering Threat Networks," *Joint Force Quarterly* 89 (2nd Quarter 2018), 28, available at <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1491501/outmatched-shortfalls-in-countering-threat-networks/>.

[21] "Department of Defense Press Briefing by Admiral Kurt Tidd," video, 31:01, U.S. Southern Command, March 6, 2018, available at <www.southcom.mil/Media/Speeches-Transcripts/Article/1458781/department-of-defense-press-briefing-by-admiral-kurt-tidd/>.

[22] Doran, "Outmatched," 30.

[23] Clay Wilson, *Improvised Explosive Devices (IEDs) in Iraq: Effects and Countermeasures*, RS22330 (Washington, DC: Congressional Research Service, February 10, 2006), available at <www.hsdl.org/?view&did=715089>.

[24] "U.S. Security Cooperation with Jordan," fact sheet, Department of State, May 21, 2019, available at <www.state.gov/u-s-security-cooperation-with-jordan/>.