Everything Old is New Again:

Russian, Chinese, Iranian and North Korean Use of Proxies Against the United States

By Lieutenant Colonel Christopher J. Heatherly (United States Army Europe G2)

And

Second Lieutenant Ian Melendez (Washington State University Army ROTC)

What role do unofficial transnational and criminal organizations play in the global adversarial competition among nations occurring today? How specifically do Russia, China, Iran, North Korea or other specifically named adversary employ unofficial transnational or criminal organizations in its strategic efforts to undermine the United States or its allies?

Introduction

"What has been will be again, what has been done will be done again; there is nothing new under the sun." - Ecclesiastes 1:9

On February 27th, 2014, a group of unidentified men entered the Ukrainian city of Simferopol on the Crimean Peninsula, seized several government buildings and raised the Russian flag.[1] Simultaneously, additional armed groups, including police officers, local citizens and the Russia based Night Wolves Motorcycle Club setup checkpoints on the roads to Sevastopol.[2] Shortly afterwards, Russian military units crossed into the Ukraine to illegally annex the entire Crimean Peninsula and the Donbass. The soldiers wore Russian uniforms, albeit devoid of insignia or rank, and were armed with Russian military equipment. Russian government entities and aligned media outlets immediately began a disinformation campaign denying involvement in the operation.[3] Russian President Vladimir Putin took part in the disinformation efforts claiming the soldiers were Ukrainian locals wearing surplus Russian uniforms.[4] As the Crimean crisis deepened, Ukraine's ability to coordinate a response suffered from cyber attacks against its cell phone networks, news websites and social media platforms. These attacks were allegedly carried out by Russian criminal hackers acting under Moscow's orders.[5] Moscow might have successfully conducted the operation independently but the use of the Russian ethnic diaspora as well as cyber, criminal, paramilitary, information and diplomatic proxies provided two critical advantages before, during and after the invasion. Their inclusion allowed Russia to rapidly seize and retain its strategic objectives in the Crimea while also affording deniability on the local, regional and world stages.

Russia's 2014 invasion of the Ukraine aptly demonstrated the effectiveness of proxies; however, their use was not unique. Nation states have employed official and unofficial proxies throughout recorded history from antiquity to the current era. For centuries, European aristocracy used their travel and international family ties to disguise backchannel diplomatic efforts. Blue blooded royalty were not the only unofficial entities participating in global affairs, criminal organizations had their part to play as well.[6] During WWII, the United States worked with Irish, Italian and Jewish criminal organizations to protect vital American seaports and assist with the liberation of Sicily in 1943.[7] American President Franklin D. Roosevelt created a network of unofficial intelligence agents to augment the nascent Office of Strategic Services and military intelligence bodies in that same conflict.[8] Nor are proxies limited to criminal or transnational entities; this paper opens the aperture to include examples from across the entire diplomatic, information, military and economic spectrum (DIME) to offer a more robust analysis.

For the moment, the US possesses capable instruments of national power but is rapidly losing its competitive edge given the absence of a coherent grand strategic plan. Proxies provide numerous tangible benefits to the user, not the least of which is deniability in the information domain. They further afford access to resources in three broad categories of time, talent and treasure that may be unavailable directly to the sponsoring nation state itself.

The United States' primary state competitors, namely Russia and China as well as regional actors Iran and North Korea, utilize proxies operating independently or in concert with their official instruments of national power. Russian military forces frequently work in partnership with paramilitary, criminal and cyber entities. As part of the 2017 National

Intelligence Law, Chinese companies are now legally required to work with Beijing in the conduct of intelligence operations.[9] Iran exercises regional influence via radical Islamic terrorist organizations such as Hezbollah and Hamas to counter American efforts in the Middle East, often acting indirectly against Israel to draw US resources away from other, arguably more vital, problem sets. The hermit state of North Korea uses front companies to smuggle illegally traded weapons to generate funding streams bypassing economic sanctions. Such ventures outside legitimate commerce exchange and regional or international agreements are more difficult for the United States and her allies to identify, track and counter. Clearly, America's competitors employ proxies across the DIME construct leading to a key question: What will the United States do to account for proxies in pursuing its own national interests?

Analysis

China

China's use of proxies is a well-known and well documented threat to the United States. Beijing is widely believed to use cyber actors to hack into government, commercial and military networks to conduct intellectual property theft to advance its own national capabilities or perform espionage to understand its opponents and exploit weaknesses. A 2013 Reuters news story alleged Chinese hackers stole F-35 plans from Boeing to build the People's Liberation Army Air Force advanced generation J-20 and J-31 stealth fighters.[10] China's cyber capability provides offensive and deniable, options threatening power grids, satellites, and hydroelectric dams. In 2014 Admiral Mike Rogers, then head of US Cyber Command, testified China and "one or two" other countries would be capable of mounting a cyberattack that could shut down the power grid."[11] China's Huawei Technologies Company remains in current news headlines as it seeks to expand its 5G network into the West – a move rightly deemed a threat by numerous government leaders and national security experts. Chinese law requires its companies to work with the government on intelligence matters, despite public claims to the contrary.[12] Recognizing the danger of Huawei's planned network expansion, US President Donald Trump signed an executive order preventing Huawei from selling its products in the United States and doing business with American companies.[13]

China's business firms are another set of proxies readily employed on a global level. China holds $1.12 trillion in US debt which could be used directly or indirectly against the United States.[14] Similarly, China offers large cash loans to developing nations but requires key infrastructure, such as ports, or natural resources, as collateral. China simply waits for the borrowing nation to default on the loan and then takes ownership thereby providing it real property and long-term influence. As of this writing, Kenya is in danger of losing its primary port of Mombasa after failing to repay a $2.3 billion loan back to Beijing.[15] China further employs economic organizations in the purchase of port facilities across Europe and Asia, the use of which might be denied to US commercial or military movements in the future.[16]

The vast Chinese diaspora, estimated at over 50 million people, is another proxy venue for Beijing's foreign policy program.[17] Even a casual Internet search quickly reveals numerous examples of Chinese citizens, ostensibly working or living overseas, caught spying – and far too often only after causing serious damage to the American economy or US national security. While the actual number of Chinese citizens actively spying is unknown, a 2016 FBI report indicated a 53% rise in economic espionage alone, predominately from China.[18] A 2019 US World Wide Threat Assessment characterized the threat of Chinese spying in plain language stating, "We assess that China's intelligence services will exploit the openness of American society, especially academia and the scientific community, using a variety of means."[19]

Russia

Like it's Communist neighbor, Russia regularly employs private and state-owned business proxies to spread its influence. Russia is Europe's largest supplier of natural gas and frequently threatens to reduce shipments during winter, withhold them altogether or raise prices to exert pressure on Western governments to "to the line" on the international stage.[20]

The Russian military effectively incorporated external entities into its operations including a wide variety of auxiliary and paramilitary formations from Russian ethnic enclaves within its former spheres of influence. Moscow actively recruits within fight clubs, cyber criminals and gangs to spread its influence across Europe and the United States.[21] Similarly, Russia makes use of private military companies, such as the Vagner Group – reportedly owned by Vladimir Putin ally Yevgeny Prigozhin - in far flung operations ranging from Syria to the Central African Republic.[22]

Russia's information operations platform is highly effective at spreading disinformation around the globe. Unlike the United States, which too frequently separates its warfighting functions in staff stovepipes, Russian Military Doctrine defines information warfare as a "holistic concept that includes computer network operations, electronic warfare, psychological operations, and information operations."[23] As such, Russia sees the operations as a strategic level capability with mutually supporting elements aimed at achieving the same goals. Whether through state and privately owned news sources, social media or so-called "fake news" Moscow has mastered the ability to gain and retain the initiative in the information domain – no small wonder given Russia outspends the US in foreign information operations ($400-500M vs. $20M).[24] Religion plays a role in the information domain as well given the Russian Orthodox Church has a large international congregation with adherents spread across the Baltics, Balkans and Caucasus regions.[25] Beginning with Putin's return to power in 2012, Moscow has made use of the Orthodox Church to counter the West and defend Russian territorial aggression.[26]

Islamic Republic of Iran

Iran has been a threat to the United States since the overthrow of the Shah in 1979, ushering in an era of theocratic dictatorial rule under Ayatollah Khomeini. Iran's religious leadership stands firmly against the United States and her allies while calling for Israel's destruction. For decades, Iran has employed terrorist organizations, including Hamas and Hezbollah, to advance its influence in the Levant. Both terror groups are political movements with militant arms and effective information operations dedicated to radical Islamic fundamentalism with the stated goal of ending the Israeli state. Since 2003, Iran has provided support to Shia militia groups in Iraq fighting against Baghdad and Washington.[27] US estimates suggest Iran donates billions of dollars to terrorist groups including the Assad regime ($15B+), Hezbollah ($700-800M), Shia militia groups in Iraq ($200M) as well as Hamas and Palestinian Islamic Jihad ($100M).[28] These funds are used for recruitment, training, political lobbying, information operations and military equipment purchases.

North Korea

The Democratic People's Republic of Korea (DPRK), more commonly known as North Korea, is a dictatorial hermit kingdom that emerged after the Korean War ceasefire in 1953. North Korea's abysmal human rights record, approach to foreign relations and philosophy of self-reliance, or *juche*, has largely cut off the country from accepted interstate engagement. As with other nation states, North Korea has also employed proxies to achieve its objectives. The DPRK has a long history of planning and conducting terrorist attacks against South Korean and US targets on the Korean peninsula.[29] These actions, combined with its external support to designated terrorist organizations, led the United States to declare North Korea a state sponsor of terrorism in 1988 and, following its removal in 2008, again in 2017.[30] US President Donald Trump and then Secretary of State Rex Tillerson cited several reasons this designation including North Korea's "unlawful nuclear and ballistic missile development, dangerous support for international terrorism and other malicious activities."[31]

North Korea bypasses international sanctions, designed to curb its further nuclear weapons aspirations, using front companies to conduct illegal arms sales to Iran and Syria. These sales provide Pyongyang with much needed hard currency while creating additional foreign policy changes for the United States and her allies.[32] North Korea has long understood how to use duplicity in its arms sales by employing a myriad number of overseas companies and numerous, albeit smaller, financial transactions beneath thresholds designed to identify such transfers.[33] Perhaps more alarming is Pyongyang's likely use of more difficult to trace cryptocurrency through its increasing use of third party Internet services.[34]

North Korea itself frequently serves as both a Russian and Chinese proxy as a means to distract the United States from their own competing actions. Providing North Korea with, say illegal petroleum sales or technology transfers, allows Pyongyang to partially bypass sanctions designed to curb its actions or outright threats against key US allies such as South Korea and Japan. Indeed, North Korean dictator Kim Jong-un has demonstrated a masterful ability to maintain American attention through a combination of carrot and stick approaches thereby forcing the US to focus its limited resources on the Korean peninsula vice Europe or the Middle East.[35]

Recommendations

Knowing Russia and other competitor nations employ proxies is not new information. Understanding *how and why* Russia, China, Iran or North Korea utilize them, however, provides valuable insight for the United States to develop appropriate offensive and defensive measures. A key question to consider is the part the emerging domains cyber and space play in international affairs the doctrine of which is still being developed in real time. A complete, nuanced answer to this question is beyond the scope of the paper; however, both domains must be addressed in any proffered solution.

One fact is certain as we look to the future: competitor proxies will continue to operate against US interests at the strategic, operational and tactical levels. For the United States to retain, arguably regain, its leading role on the international stage and maintain its advantage over competitor nations it must take two critical steps. First, it is imperative the US develop a realistic, long term - *read multigenerational* - strategic plan akin to George Kennan's Long Telegram of 1947. That prescient document successfully guided US international policy from the 1940's to the end of the Cold War. Since the fall of the USSR, however, America has too long relied upon "grand strategy du jour" creating much uncertainty amongst our citizens, our allies and our competitors. Bluntly restated, America is long overdue for a lasting strategy untainted by foreign lobbyists, pithy sound bites, opinion polls and partisan politics. The National Security Strategy and the supporting National Defense and National Military Strategies are not fully nested with the rest of the United States Government's other services such as the Department of State leading to frequently disjointed and occasionally contradictory US policy making.

Second, the United States must end its virtually exclusive reliance upon the military instrument of national power, often without a viable exit plan, and instead utilize a new approach incorporating the entire DIME model as well as the rest of US society writ large. Ideally, the US will generate a *whole of nation* approach bringing the expertise of the American people into the fight. This will necessitate the US government clearly demonstrate the shared risks of inaction and articulate the collective benefits of national cooperation. While this recommendation may seem unfeasible given the highly charged state of American domestic politics, the United States successfully employed a whole of nation approach during World War II and on a smaller scale through the post-WWII reconstruction of Europe and Japan. This policy will require the US government to recognize the severe threat posed by its competitors, find common policy ground to act and, most critically, restore the declining trust of the American people first lost during the Vietnam War.

While this paper advocates for greater US integration with international organizations and allies, this is not without challenge. International organizations, such as the UN or NATO, are notoriously slow to act in their decision-making cycles and are more easily influenced, legally or illegally, by US competitors. The confederated structure of the UN gives it little authority outside of the UNSC and NATO also sees the US giving disproportionately more in financial contributions than its allies based on GDP per capita. Their resolutions frequently require compromise thereby reducing the potential impact of their actions against US competitors. While the Unites States is capable of independent action it will be more effective when working by, with and through allies, partners and international organizations. No less a statesman than Winston Churchill recognized this truism stating, "There is only one thing worse than fighting with allies, and that is fighting without them."

Conclusion

America, its allies and its adversaries will continue to employ proxies across the DIME range on the global stage. The US must create a lasting, realistic, fully understood grand strategic plan understood and supported by the American people to defend its vital national interests. This document must be flexible enough to account for a rapidly changing strategic environment while simultaneously providing continued assurance to our citizens and allies. Nor can Washington rely exclusively on the military to retain its competitive edge or to achieve its desired national objectives. Remaining competitive in the brave new world of the 21st century demands a new approach beyond DIME and even beyond whole of government, instead requiring a whole of nation approach to succeed.

Notes

[1] BBC, “Ukraine: Gunmen seize Crimea government buildings,” 27 February 2014, accessed 26 January 2019, https://www.bbc.com/news/world-europe-26364891.

[2] The Guardian, “Ukraine: Night Wolves and unidentified military men seize key Crimea sites,” 28 February 2014, accessed 26 January 2019, https://www.theguardian.com/world/2014/feb/28/ukraine-night-wolves-military-seize-crimea.

[3] Euromaiden Press, “Little green men: the annexation of Crimea as an emblem of pro-Kremlin disinformation.” 23 March 2018, accessed 26 January 2019, http://euromaidanpress.com/2018/03/23/little-green-men-the-annexation-of-crimea-as-an-emblem-of-pro-kremlin-disinformation/.

[4] Vitaly Sevchenko, BBC, “”Little green men" or "Russian invaders"?,” 11 March 2014, accessed 26 January 2019, https://www.bbc.com/news/world-europe-26532154.

[5] Dave Lee, BBC, “Russia and Ukraine in ‘cyber stand-off’,” 05 March 2014, accessed 26 January 2019, https://www.bbc.com/news/technology-26447200.

[6] Christopher J. Heatherly, Military Review, “Go-Betweens for Hitler” (book review), 15 June 2018, accessed 27 January 2019, https://www.armyupress.army.mil/Journals/Military-Review/MR-Book-Reviews/Jun-2018/Book-Review-007/.

[7] Warfare History Network, “Project Underworld: The U.S. Navy’s Secret Pact with the Mafia,” 13 December 2018, accessed 26 January 2019, https://warfarehistorynetwork.com/daily/wwii/project-underworld-the-u-s-navys-secret-pact-with-the-mafia/.

[8] Joseph E. Persico, CIA, “Roosevelt's Secret War: FDR and World War II Espionage,” last updated 27 June 2008, accessed 27 January 2019, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no2/article07.html.

[9] Quartz, “What you need to know about China’s intelligence law that takes effect today,” 28 June 2017, accessed 27 January 2019, https://qz.com/1016531/what-you-need-to-know-about-chinas-intelligence-law-that-takes-effect-today/.

[10] David Alexander, Reuters, “Theft of F-35 design data is helping U.S. adversaries -Pentagon,” 19 June 2013, accessed 23 June 2019, https://www.reuters.com/article/usa-fighter-hacking/theft-of-f-35-design-data-is-helping-u-s-adversaries-pentagon-idUSL2N0EV0T320130619.

[11] Adam Segal, Council on Foreign Relations, “China and the Power Grid: Hacking and Getting Hacked,” 03 December 2014, accessed 23 June 2019, https://www.cfr.org/blog/china-and-power-grid-hacking-and-getting-hacked.

[12] Yuan Yang, Financial Times, “Is Huawei compelled by Chinese law to help with espionage?”, 05 March 2019, accessed 23 June 2019, https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0.

[13] Billy House and Rosalind Mathieson, “Comey Says Threat from Huawei is Something He and Trump Agree On,” Bloomberg, 21 June 2019, accessed 23 June 2019, https://www.bloomberg.com/news/articles/2019-06-21/comey-says-threat-from-huawei-is-something-he-and-trump-agree-on.

[14] Jeff Cox, CNBC, “China has cut its holdings of US debt to the lowest level in two years amid trade tensions,” accessed 16 May 2019, 23 June 2019, https://www.cnbc.com/2019/05/16/china-has-cut-its-holdings-of-us-debt-to-the-lowest-level-in-two-years.html.

[15] The Maritime Executive, “Report: Kenya Risks Losing Port of Mombasa to China,” 20 December 2018, accessed 27 January 2019, https://www.maritime-executive.com/article/kenya-risks-losing-port-of-mombasa-to-china.

[16] Keith Johnson, Foreign Policy, “Why is China Buying Up Europe’s Ports?,” 02 February 2018, accessed 25 June 2019, https://foreignpolicy.com/2018/02/02/why-is-china-buying-up-europes-ports/.

[17] Statista, “Number of Chinese people living overseas as of 2017, by continent,” last edited 04 February 2019, accessed 24 June 2019, https://www.statista.com/statistics/632850/chinese-nationals-number-overseas-by-continent/.

[18] John R. Schindler, Observer, “”The Unpleasant Truth About Chinese Espionage,” 22 April 2016, accessed 23 June 2019, https://observer.com/2016/04/the-unpleasant-truth-about-chinese-espionage/.

[19] Zachary Cohen and Alex Marquardt, CNN, “US intelligence warns China is using student spies to steal secrets,” 02 February 2019, accessed 24 June 2019, https://edition.cnn.com/2019/02/01/politics/us-intelligence-chinese-student-espionage/index.html.

[20] Nastassia Astrasheuskaya, Foreign Times, “Russia defies pipeline threats over gas for Europe,” 18 June 2019, accessed 24 June 2019, https://www.ft.com/content/1f6ac3d6-861f-11e9-97ea-05ac2431f453.

[21] Michael Carpenter, The Atlantic, “Russia Is Co-opting Angry Young Men,” 29 August 2018, accessed 25 June 2019, https://www.theatlantic.com/ideas/archive/2018/08/russia-is-co-opting-angry-young-men/568741/.

[23] Carl Schreck, Radio Free Europe, “What Are Russian Military Contractors Doing In The Central African Republic?”, 01 August 2018, accessed 25 June 2019, https://www.rferl.org/a/explainer-what-russian-military-contractors-are-doing-in-central-african-republic/29405290.html.

[24] Global Security Review, "Analyzing Russian Information Warfare and Influence Operations," 01 July 2019, accessed 26 June 2019, https://globalsecurityreview.com/cold-war-2-0-russian-information-warfare/.

[25] Paul Szoldra, Task and Purpose, "Military Leaders Are Starting To Freak Out Over Russia's Information Warfare Dominance," 09 October 2018, accessed 26 June 2019, https://taskandpurpose.com/russia-information-war.

[26] Pew Research Center, "Religious Belief and National Belonging in Central and Eastern Europe," 10 May 2017, accessed 26 June 2019, https://www.pewforum.org/2017/05/10/religious-belief-and-national-belonging-in-central-and-eastern-europe/.

[27] Alexis Mrachek and Shane McCrum, "How Putin Uses Russian Orthodoxy to Grow His Empire," 22 February 2019, accessed 26 June 2019, https://www.heritage.org/europe/commentary/how-putin-uses-russian-orthodoxy-grow-his-empire.

[28] Geneive Abdo, National Interest, "Iraq's Intra-Shia Struggle Over Iranian Influence," 18 December 2018, accessed 24 June 2019, https://nationalinterest.org/feature/iraqs-intra-shia-struggle-over-iranian-influence-39057.

[29] David Adesnik, Foundation for Defense of Democracies, "Iran Spends $16 Billion Annually to Support Terrorists and Rogue Regimes," 10 January 2018, accessed 23 June 2019, https://www.fdd.org/analysis/2018/01/10/iran-spends-16-billion-annually-to-support-terrorists-and-rogue-regimes/.

[30] Krishnadev Calamur, The Atlantic, "North Korea's Terrorism Designation Isn't Entirely About Terrorism," 20 November 2017, accessed 23 June 2019, https://www.theatlantic.com/international/archive/2017/11/north-korea-state-sponsor-terrorism/546386/.

[31] Adam Taylor, The Washington Post, "North Korea's on-again-off-again status as a state sponsor of terrorism," 20 November 2017, accessed 23 June 2019, https://www.washingtonpost.com/news/worldviews/wp/2017/11/20/north-koreas-on-again-off-again-status-as-a-state-sponsor-of-terrorism/?noredirect=on&utm_term=.8cd530c01836.

[32] Dan Merica, Jeremy Diamond and Zachary Cohen, CNN, "Trump names North Korea a state sponsor of terrorism," 21 November 2017, accessed 23 June 2019, https://edition.cnn.com/2017/11/20/politics/president-donald-trump-north-korea-terrorism/index.html.

[33] Bruce E. Bechtol, Jr., Foreign Affairs, "North Korea's Illegal Weapons Trade," 06 June 2018, accessed 23 June 2019, https://www.foreignaffairs.com/articles/north-korea/2018-06-06/north-koreas-illegal-weapons-trade.

[34] Kate Fazzini, CNBC, "Complex web of international banks, shell companies, helps North Korea gain access to funds, WSJ reports," 29 December 2019, accessed 23 June 2019, https://www.cnbc.com/2018/12/29/north-korea-skirts-sanctions-through-web-of-banks-companies-wsj.html.

[35] Recorded Future, "Shifting Patterns in Internet Use Reveal Adaptable and Innovative North Korean Ruling Elite," 25 October 2018, accessed 23 June 2019, https://www.recordedfuture.com/north-korea-internet-usage/.

[36] Robert Einhorn, Brookings, "Let's get realistic on North Korea and Iran," 05 October 2018, accessed 23 June 2019, https://www.brookings.edu/blog/order-from-chaos/2018/10/05/lets-get-realistic-on-north-korea-and-iran/.