The “Sick Man of Eurasia”: Quarantining the Russian Federation in the 21st Century ...............8
Douglas A. Livermore

The Russian Federation in the early 21st century is only a weak aspirant to the mantle of the former Soviet Union, which itself was never truly a geopolitical equal of the United States. The Russian Federation today is “The Sick Man of Eurasia” and nurses its delusions of bygone imperial grandeur despite its many weaknesses and crumbling prospects. Moscow is now diplomatically isolated from the post-Soviet world order, ideologically bereft of a viable vision with which to compete on the global stage, overwhelmingly reliant on a conventionally weak military, and facing an increasingly grim economic outlook. Demographic shifts are also changing the ethnic composition of Russia, which will have significant influence on the future direction of the Federation. Faced with such a weak global “competitor,” the best path forward for the United States and its allies is to pursue an updated “containment” or “quarantine” strategy, similar to that which succeeded in defeating the Soviet Union’s Cold War ambitions. This quarantine approach would minimize the potential for catastrophic state-on-state war with Russia, leverage Russia’s own internal weaknesses over the long term to mitigate its disruptive global activities, and increase the prospects of an eventual Russian transition to a more peaceful, responsible, and democratic form of representative government prepared to integrate into the existing world order.

US Assistance to Syrian Kurdish Forces ....................................................................................22
Rebecca Lucas

US Special Forces support for Syrian Kurdish forces fighting ISIS, most prominently the People’s Protection Units (YPG), has focused on military support such as train and equip missions. However, the YPG’s increasing territorial control indicates that in order to ensure long-term stability in Syria, the United States needs to assist with building the institutions necessary for good governance. Historical examples indicate that, even with this support, the United States cannot control its partners enough to ensure that they do not act in ways that perpetuate instability and popular dissent.
Domestic Politics, Military Reforms, and Threat Perceptions: Three Factors Influencing Russian Decision-Making in its Near Abroad

Nicholas Fedyk

The troubling escalation in Russian-American tensions today partly stems from Russian meddling in Ukraine. Of all the countries that make up Russia's near abroad, Ukraine is the most populous and prosperous, and its positioning between Europe and Russia has made it a flashpoint in big power politics in recent years. This paper explores why exactly Russia is destabilizing Ukraine by comparing President Putin's different responses to two revolutions in post-Soviet Ukraine—the 2004 Orange Revolution and the 2013–2014 Euromaidan. After establishing that the revolutions are sufficiently similar to merit comparison, I will evaluate three potential factors that influenced Putin's response:

1. The transition of Putin's inner circle of advisers from liberal, Western-oriented economists to security-community colleagues more skeptical and hostile towards the West.
2. Military reforms that significantly improved the performance of the armed forces.
3. Escalating threat perceptions associated with Ukraine and its Western allies.

I conclude that in 2014 Putin was more willing (due to Russia's domestic politics), more capable (due to Russia's military reforms), and more threatened (due to Russia's geopolitical situation) to utilize military force against Ukraine. At a time when Russia has become a major national security priority, this bears several lessons for countering future Russian adventurism.

A Commitment to Peace or Just Good Enough?: Analyzing the Tuareg Uprisings in Niger (1990–2009)

Emily Gilbert

Despite their treatment as two distinct rebellions, the Nigerien Tuareg insurgencies were one phenomenon that witnessed multiple swells of violence. The Nigerien government's initial response was an attempt at an authoritarian counter-insurgency campaign. The government, however, had neither the institutional capacity nor the means to sustain such an operation. Prolonged fighting both weakened the state's financial resources and undermined the quality of its armed forces. The state failed equally in its initial attempts at a negotiated settlement, allowing conflict to break out once again in 2007. Ultimately, despite the feebleness in the state's responses, the insurgency ended not due to government efforts, but due to critical weaknesses in the insurgent groups themselves.
The Role of the Security Services in Russian Foreign Adventurism and Its Consequences for US Policy

Nicholas McCarty

Russian intelligence services have garnered a great deal of press attention in the last year over cyber warfare, hacking, and their influence on Western democracy. Missing from this conversation (in the West at least) is the influence of the security services on Russia itself. As Vladimir Putin and Russia have become increasingly isolated from the international community, Russia’s foreign policy has become dominated by the so-called siloviki, ex-security service members who hope to steer the state toward their interests. Greater awareness of the history and role of the state security services in Russian society is needed if US policymakers are to respond correctly to future crises.

An Unorthodox Call to Arms: The Humanitarian Case for Military Intervention in the DPRK

Bryant King

In the landmark 2014 Report of the Commission of Inquiry on Human Rights in the Democratic People’s Republic of Korea (DPRK), the United Nations claims that the DPRK is presiding over “systematic, widespread, and gross human rights violations” against its citizenry, whose “gravity, scale, and nature reveal a state that does not have any parallel in the contemporary world.” Consequently, it is appropriate for the United States and its allies to consider whether military intervention might be justified to address this situation, based on the Responsibility to Protect (R2P) framework developed by the International Commission on Intervention and State Sovereignty (ICISS) and the UN’s 2005 World Summit Outcome Document. Because preventive and non-military reactive measures implemented against the DPRK have not ameliorated the state’s human rights situation, the United States and its allies should view military intervention as a viable and legitimate course of action. However, the United States and its allies must recognize the ethical and political challenges they would face in the period leading up to and during the execution of a military intervention, and be willing to support long-running and extensive post-intervention state-building operations lead by the United Nations. While conducting a military intervention might seem a counterintuitive measure to address the DPRK’s human rights crisis, recent history proves that it might represent the only course of action.
Lessons Learned from the Russian Active Measures Campaign in the 2016 United States Presidential Elections: A Crossroads of Success and Failure

Susanne Boss

Over the past year, allegations have solidified into judgments surrounding Russian involvement in targeting multiple facets of the US 2016 Presidential Election. Known as active measures, Russian actions strategically blended the use of covert intelligence operations with overt activity in three method areas: Malicious Cyber Activity, Disinformation, and Possible Collusion between Russia and Trump Campaign officials. Examples of these method areas range from the exposure of more than 126 million users on Facebook to posts created and disseminated by Russian operatives, to the Russian-linked hacking and leaking of thousands of emails associated with the Hillary Clinton Campaign and the Democratic National Committee. This article examines the Russian active measures targeting of the US 2016 Presidential Election as a case study of both successful Russian covert action and failed American counterintelligence. As Russia will certainly apply lessons learned from this campaign to future influence efforts against the United States and other democracies, it is critical for policy makers to identify and apply lessons from this experience to better prepare for and counter future active measures operations.

Roles and Missions of the Armed Forces and Civilian Control Mechanisms in Colombia: 1991-2016

Carlos F. Castillo

As the recently signed peace agreement between the government of Colombia and the Fuerzas Armadas Revolucionarias de Colombia (FARC) insurgency moves forward to the implementation phase, revisiting the role of the armed forces, as well as civilian control mechanisms, is needed for civil–military relations to adapt to the new transitional strategic environment—especially, given the ongoing political and institutional changes that could result in additional stress between civilian authorities and the military. In this article, I compare the recent dynamics in civil–military relations in theory and practice, to discuss, assess, and inform decision-makers about the most prevalent challenges concerning the relationship between civilian authorities and the officer corps in the country. Furthermore, I argue that the ruling elites in Colombia have instrumentally used the armed forces through institutional and ideological control mechanisms, neglecting broad national security concerns and limiting the roles and missions of the different armed services. In this way, the government of Colombia has exercised a form of subjective control by matching their private interests with the martial values of the officer corps, and enabling the armed forces to effectively shape domestic politics.
The Drivers of Iranian Cyber Strategy: From Stuxnet to the Present ................................................................. 129

Jack Rock Lucas

Despite being a relatively young cyber power, Iran’s execution of several prominent cyber-attacks demonstrate that Tehran is willing and able to operate in the cyber domain to achieve its strategic objectives. This article proposes that, since Iran began investing in cyber capabilities in reaction to the 2010 discovery of the Stuxnet attack, it has sought to use the cyber domain to maintain control of its population through extensive monitoring, exert influence on its neighbors through proxy organizations, and deter its technologically advanced adversaries through the threat of costly cyber-attacks on critical infrastructure. Iranian cyber strategy is investigated by identifying three phases of development for the country’s cyber capabilities: the creation of formal cyber organizations, the demonstration of ‘loud’ retaliatory capabilities, and the ‘quiet’ collection of critical vulnerabilities for sophisticated attacks. Lastly, this article speculates as to what factors will make Tehran more or less likely to reactively execute cyber-attacks on critical infrastructure in the future.

“Then Kill the Pagans Wherever You Find Them”: The Emerging Trend of Islamic State Networks Targeting Christians in Egypt ........................................................................................................ 136

Sarah Gilkes

Since the rise of the Islamic State (IS) and the organization’s declaration of a caliphate in June 2014, much scholarship has been devoted to examining the group’s evolution, ideology, and expansion. Little attention, however, has been paid to the development and mobilization of IS’s affiliate in Egypt, Wilayat Sinai, and other IS-related networks across Egypt. This article seeks to fill this gap through a quantitative study of terrorist attacks attributed to and/or claimed by Egyptian IS-related entities and their predecessors, specifically Ansar Bayt al-Maqdis (ABM), between January 1, 2011, and June 30, 2017. In particular, this article focuses on the recent shift of IS strategy within Egypt embracing the targeting of Coptic Christians, the largest Christian community in the Middle East. Comprehensive examination of all ABM and IS-related terrorist attacks in Egypt during this period reveals that while attacks targeting Christians began in early 2014, only in the first six months of 2017 did IS-related networks—both in the Sinai and across mainland Egypt—begin to systematically target Copts. Analysis of official IS propaganda suggests that militants hope attacks will aggravate existing tensions between the Coptic minority and Muslim majority in Egypt, thereby sparking a larger civil and political conflict and enabling IS-related networks of militants to act as the defenders of the Sunni Muslim community.
Individual Choice, National Consciousness: Cyber Hygiene

Christen Soden

Individuals must practice cyber hygiene, not only for their personal protection but for the greater national security. Malicious actors can use individual lapses in cyber hygiene to access restricted networks and weaponize devices, exposing state secrets and disabling critical infrastructure. However, cyber hygiene presents a collective action problem and requires a government campaign or incentive structure to mobilize compliance. Academics and practitioners have looked to the public health model for answers. However, the public health model has several shortcomings for application to cyber, including the need for a new federal regulatory authority, enforcement of individual compliance, the importance of mission-oriented non-governmental and quasi-governmental organizations, and the stronger tie to self-interest. This paper suggests an alternative model for consideration: the Federal Civil Defense Administration (FCDA), and the post-World War II devolution of civilian defense to the state and local levels. This structure depended less upon regulations and compliance enforcement, and more upon local civilian defense units to provide functional adaptability and local surge capacity.
The “Sick Man of Eurasia”: Quarantining the Russian Federation in the 21st Century

Douglas A. Livermore

The Russian Federation in the early 21st century is only a weak aspirant to the mantle of the former Soviet Union, which itself was never truly a geopolitical equal of the United States. The Russian Federation today is “The Sick Man of Eurasia” and nurses its delusions of bygone imperial grandeur despite its many weaknesses and crumbling prospects. Moscow is now diplomatically isolated from the post-Soviet world order, ideologically bereft of a viable vision with which to compete on the global stage, overwhelmingly reliant on a conventionally weak military, and facing an increasingly grim economic outlook. Demographic shifts are also changing the ethnic composition of Russia, which will have significant influence on the future direction of the Federation. Faced with such a weak global “competitor,” the best path forward for the United States and its allies is to pursue an updated “containment” or “quarantine” strategy, similar to that which succeeded in defeating the Soviet Union’s Cold War ambitions. This quarantine approach would minimize the potential for catastrophic state–on–state war with Russia, leverage Russia’s own internal weaknesses over the long term to mitigate its disruptive global activities, and increase the prospects of an eventual Russian transition to a more peaceful, responsible, and democratic form of representative government prepared to integrate into the existing world order.

Diagnosing the Patient: Placing the Threat in Context

Russian President Vladimir Putin does not want to resurrect the defunct Union of Soviet Socialist Republics (USSR), of which Russia was the principal political, ideological, military, and economic component. What he does want is for Russia to regain a measure of the international standing and influence that the USSR enjoyed as a co–equal to the United States within the bipolar global system of the Cold War. This vision appeals to many Russians who feel betrayed by unrealized (and often assumed) Western promises in the post–Soviet era, and Putin encourages this sentiment as a means of maintaining his personal autocracy from the Kremlin.¹ Russians are seemingly unable to accept that they will never be able to recapture the “imperial

glory” of Soviet yesteryears. Russia continues to cling to the trappings of its previous grandeur and attempts to assert itself on the global stage, despite increasingly bleak prospects.

The systemic obstacles that separate Russia from its goal of resurrected international relevance are more numerous and significant than those that faced, and ultimately frustrated, the Soviet Union’s global ambitions. Russia today is more diplomatically isolated than the Soviet Union ever was. It does not embrace any definable ideology with which to compete with the United States and its allies. Russia primarily advances its foreign policy using a weakened military that still uses largely Soviet-era equipment. Both Russia’s revitalization and Putin’s personal patronage systems rely upon a hydrocarbon-based economy that continues to falter in the contracting global energy market. As if these were not enough hurdles, Russia at the beginning of the 21st century is facing daunting demographic challenges due to depressed life expectancy and ethnic Russian reproductive rates at the same time that migratory influx is placing ever-increasing strain on the already tenuous internal dynamics of the Federation.

Diplomatically, Russia under Putin has reached near-pariah state status due to its ongoing destabilizing activities around the globe. While it still holds its traditional seat on the United Nations Security Council, Russia’s influence abroad has continued to wane as global opinion coalesces into general opposition. The circle of diplomatic allies on which Russia can rely has shrunk considerably since the days of the USSR and Warsaw Pact, and this circle is largely comprised of a “rogue's gallery” of similarly isolated states or sub-state actors. Among its international allies, Russia can count only Ukrainian separatists, Belarussian dictators, authoritarian Libyan warlords, and Syrian tyrants. Among this motley crew of international misfits, the most pervasive characteristic is utter reliance on Russian support to maintain their tenuous holds on power. To a lesser extent, Russia occasionally finds its interests aligned with the brutal Iranian regime, the oppressive Chinese government, and North Korea’s police state. Russia’s diplomatic relations are heavily influenced by Putin’s single-minded focus on realpolitik, which places Russia in a constant state of competition, and only occasionally distrustful cooperation, with these few other states that are willing to maintain any meaningful relations with the Kremlin.

---


Russia’s diplomatic weakness has been most evident since the Kremlin’s intervention in Ukraine starting in 2014. The lightning-fast occupation and annexation in March 2014 of the Crimean Peninsula was quickly followed by escalatory support to ethnic Russian separatists in the country’s east. These same Russian-backed rebels shot down a civilian airliner in July that same year, killing all 298 people aboard. This atrocity resulted in near-universal condemnation of the Kremlin, which had supplied the missile systems and training that the separatists used in the downing of the civilian aircraft.\(^5\) Sanctions levied against Russia by the international community for its Ukrainian intervention continue to severely limit Russian diplomatic options. Similarly, Russian support to Syrian dictator Bashar al-Assad, who has killed hundreds of thousands of his own citizens, has further damaged Russian diplomatic credibility abroad.\(^6\) In recent months, the Kremlin’s support to Libyan warlord Khalifa Haftar, whose forces have often clashed violently with the internationally recognized Libyan Government of National Accord, have put Moscow at odds with most of the major world governments and international bodies.\(^7\)

Ideologically, Russia lacks a viable alternative worldview with which to compete with the United States and the existing liberal world order. During the Cold War, the Soviet Union ostensibly sought to “liberate” the world from the evils of capitalism and usher in a glorious global communist utopia. However, Russia under Putin does not have such a grandiose, unifying vision around which to rally and pursue a coherent strategy. Rather, his Hobbesian perspective drives all of Putin’s interaction with the wider world—he sees international relations as a zero-sum game of constant competition for survival.\(^8\) Putin’s perspective of a global arrangement of constant competition is not without merit, though his previously discussed destabilizing activities are largely to blame for the general alignment of international opposition against his regime. Putin’s ideology is purely about maintaining his own autocratic hold on power, which does face


some level of domestic opposition that he seeks to quell through military adventurism (which is generally popular with ethnic Russians⁹) and heightening internal oppression.¹⁰

Putin views domestic opposition as the main threat to the survival of his regime, followed by unified international hostility to his rule because of the international community’s ability to potentially support his domestic opposition.¹¹ Therefore, it is unsurprising that Putin directs much of his destabilizing efforts abroad toward undermining international organizations that oppose his activities and might potentially seek his ouster. However, Russia’s destabilizing activities abroad are waning in their efficacy and are even starting to have counterproductive effects. The Russian government’s interference in the 2016 US presidential elections saw the strategic impact that information influence and cyber offensive activities can have on swaying national-level policy.¹²

In both the US election and elsewhere, Kremlin-directed influence operations seek to undermine public confidence in democratic governance, international alliances, and the overarching liberal world order. Putin has decided that Russia cannot regain its prior influence in the existing system, which drives his desire to return the world to a state of Hobbesian state-on-state competition. However, subsequent efforts by the Russian government to influence national elections and undermine international order in the United Kingdom, France, and Germany have seen increased recognition and comprehensive strategies to minimize the Kremlin’s ability to interfere.¹³ These influence operations have further backfired against Putin, as even President Donald Trump, an alleged ally, has been unable to successfully “reset” relations between the United States and Russia due to ongoing investigations into suspected collusion between Moscow and the Trump administration.¹⁴ Meanwhile, growing condemnation of the Kremlin’s

interference in the domestic politics of other countries is contributing further to Russia’s international isolation.

Militarily, Russia lags even further behind the United States and its allies in conventional warfare capabilities than the Soviet Union ever did at any point during the Cold War. Over the last several years, the Kremlin has undertaken a highly publicized but largely ineffective military modernization program to try to close this capability gap.¹⁵ Today’s Russian military is not nearly as dilapidated and obsolete as that which floundered during the early 2000s, though it still lacks a comparably capable expeditionary force or true technological parity with the United States.¹⁶ Much like during the Cold War, this conventional inferiority has caused the Russian military to acknowledge this disparity by shifting developmental priorities to emphasize asymmetric deterrence, influence, and cyber warfare capabilities.¹⁷ The Kremlin’s focus on strategic nuclear deterrence as a counterbalance to superior Western conventional military capability betrays this reality. In 2002, Russian doctrine officially dropped its prior “no first use” policy for nuclear weapon release, authorizing such an employment “in response to a large-scale conventional aggression.”¹⁸ Recent Russian wargames have even simulated strategic nuclear weapon release to defeat simulated threat forces.¹⁹ The design of this wargame betrays the weakness and inferiority vis-à-vis the West that Moscow recognizes in its own conventional forces.

Moreover, recent Russian expeditionary activities in Ukraine and Syria have highlighted the significant shortcomings of the Russian military. In late 2016, the Russian Navy’s single operational aircraft carrier (a Soviet-era holdover termed an “aircraft cruiser” to sidestep treaty restrictions on transiting the Turkish Straits of Bosporus) staggered through the English Channel accompanied by its own repair tugboat while en route to the eastern Mediterranean.²⁰ By comparison, the United States Navy maintains a fleet of 10 aircraft carriers and regularly


considers options to expand its fleet even further.\textsuperscript{21} Despite Ukraine being an immediate Russian neighbor and fielding a severely weakened military only a fraction of the Russian Army’s size, the Ukrainians have inflicted horrific losses on the Russians and their proxies.\textsuperscript{22} Effusive Russian media reporting has highlighted the overwhelming success enjoyed by Russian forces supporting Syrian dictator Bashar al-Assad against his own people. However, Russian military success in Syria is predicated primarily on the Russian Air Force, which is generally considered woefully obsolete by Western standards, and most experts believe would be incapable of operating against a superior adversary such as the United States.\textsuperscript{23} The Russian Air Force’s first planned fifth-generation fighter aircraft, the Sukhoi T-50, has struggled pitifully to reach even initial production levels.\textsuperscript{24} By comparison, the United States’ second fifth-generation fighter, the F-35 Lightning II, is already reaching operational status.\textsuperscript{25} Also rather embarrassingly, an early-production T-14 Armata main battle tank, the crown jewel of Russian modernization, broke down in the middle of Red Square during a rehearsal for a 2015 Russian military parade.\textsuperscript{26} Subsequent reports have also questioned the capabilities and cost of the Armata in comparison to even current generation Russian tanks.\textsuperscript{27} Recognizing the stark inferiority of their conventional forces, Moscow has desperately sought to level the playing field by deploying nuclear-capable ballistic missiles banned by the Intermediate-range Nuclear Forces (INF) treaty.\textsuperscript{28} For all if its bluster, the Russian military is currently a paper tiger incapable of offensively challenging the West in a conventional conflict.


Economically, Russia faces perhaps its greatest challenges, as revenue flow directly underpins Putin’s patronage system and other national revitalization efforts. The Russian economy predominately relies upon hydrocarbon extraction, refining, and export, particularly to European markets. Since 2014, the triple effects of hydrocarbon energy market contraction, energy diversification, and sanctions-related pressure have all driven Russian economic prospects into dire straits. The Russian economy is the entire basis of Putin’s patronage system, which is the carefully calibrated tool of corruption that he leans heavily upon to maintain the support of key Russian oligarchs and government officials. Increasingly, domestic discontent with pervasive corruption throughout the Russian government’s systems has caused Putin to make a half-hearted show of cracking down on the problem. However, Putin often exploits such required demonstrations to eliminate problematic associates and send clear messages to his remaining supporters. As these trends continue to accelerate, it is unclear how much longer Putin will be able to maintain his personal network of patronage or even continue funding other critical initiatives like military modernization.

A combination of natural market forces and intentional price manipulation has largely driven hydrocarbon market contraction. This contraction, particularly as the price per barrel of crude oil plummeted below $70 following the Organization of Petroleum Exporting Countries’ (OPEC) decision to maintain production levels in late 2014, severely impacted Russian revenue. Exploitation of new oil reserves as well as the driving down of oil prices by US allies in OPEC placed significant economic burden on Russia. Similarly, diversification of energy markets has reduced demand for Russian hydrocarbons. The “Green Energy” movement will continue to undermine Russia’s long-term economic potential as Western Europe transitions to alternative energy sources. In fact, the French government recently announced plans to end the sale of gas and diesel vehicles by 2040. Finally, pervasive economic sanctions on key Russian oligarchs and financial institutions continue to damage severely the overall Russian economy. For example, sanction restrictions that prevent Russian oil companies from borrowing investment

---

funds from Western banks for longer than 30 days have had a growing negative impact on Russian economic forecasts.\textsuperscript{33}

Demographically, the most ambiguous challenge that Russia faces in the modern era is the potential impact of ethnic shifts within the Federation. Alarmingly shortened life expectancy among ethnic Russians, accelerating immigration from largely Muslim Central Asian republics, and increased reliance on East Asian migrant workers may soon change what it means to “be” Russian. Given the importance that Russian ethnic identity has on the Kremlin’s ambitions for resurgence, the impact of an ethnic shift may be fundamental. Putin domestically touts his military adventurism, particularly in Ukraine and Eastern Europe, as necessary crusades to defend ethnic Russians outside its borders from genocidal and cultural threats.\textsuperscript{34} As ethnic Russians become less of a percentage of the overall Russian population, this means of securing domestic support will become less and less effective for Putin.

Several recent studies have shown a marked downturn in the life expectancy of ethnic Russians, particularly among males. Increased alcoholism, depression, resultant suicides, and a host of other factors all contribute to this trend.\textsuperscript{35} At the same time, increased immigration from majority Muslim Central Asian republics has threatened to displace ethnic Russians as the majority population in several areas of the Federation.\textsuperscript{36} This dearth of able-bodied ethnic Russian males has resulted in increased reliance on Eastern Asian manual labor in the Russian Far East.\textsuperscript{37} These factors have all contributed to projections that predict ethnic Russians becoming a minority in several key areas of the Russian Federation by the mid-21st century.\textsuperscript{38} Given that much of Putin’s current domestic popularity and the survivability of his regime is specifically tied to the strength of Russian nationalism, this trend will certainly give him reason

\begin{footnotes}


\end{footnotes}
for concern.39 The challenges and opportunities posed by this demographic shift are unclear, but the ethnic Russian yearning for a resurgent Russian Empire will likely wane as ethnic diversification increases.

Treating the Patient: Quarantine and “Political Warfare”

In Section 1239 of the 2018 National Defense Authorization Act, the United States Congress directed the Department of Defense to lead the development and implementation of a comprehensive interagency strategy to counter the threat posed by the Russian Federation.40 The United States and its allies should address the challenges posed by Russia’s destabilizing activities and resurgent global ambitions with an updated version of the Cold War’s “containment” strategy. The containment strategy advocated for “political warfare” that leveraged all elements of national power to restrain and ultimately defeat the Soviet Union. Best described in a 1948 State Department memorandum by US Ambassador George Kennan, political warfare involved:

The employment of all the means at a nation’s command, short of war, to achieve its national objectives [...] They range from such overt actions as political alliances, economic measures, and ‘white’ propaganda to such covert operations as clandestine support of ‘friendly’ foreign elements, ‘black’ psychological warfare and even encouragement of underground resistance in hostile states.41

An updated containment, or “quarantine” strategy, should bring to bear all components of US national power to minimize Russian influence on global stability while allowing and encouraging Russia’s own internal dysfunction to bring about an eventual transition to a more peaceful, transparent, and representative government. It is important to specify that US policymakers must design this updated quarantine strategy with situational-dependent escalatory (and corresponding de-escalatory) measures intended to create increased negotiating space with Russia on terms that are more favorable to the United States and its allies.

Diplomatically, the United States should continue to isolate Moscow by highlighting its unacceptable destabilizing activities while expanding and fostering stronger ties with alliances and international organizations, such as the North Atlantic Treaty Organization and the European Union, which restrain Russian activities abroad. By clearly correlating Russia’s


destabilizing activities to its increased marginalization, the United States may influence Putin’s behavior away from his current path. While such diplomatic isolation will likely increase Russian support for Putin in the short term, the continued degradation of Russian prestige and international relevancy may ultimately sway his domestic base. Currently, Putin maintains a measure of domestic legitimacy through casting the Russian state as unfairly under siege, and clearly identifying Russia’s “bad” behavior as justification for continued isolation may eventually influence Russian policymaking.  

We have already seen such diplomatic efforts lead to noteworthy international progress.

The Russian interventions in both Ukraine and Syria have seen consistent and firm condemnation from the United States, a chorus that has grown in unity and strength across Europe, the Americas, and elsewhere. The strengthening of this widespread diplomatic opposition to Russia’s destabilizing activities will only exacerbate Moscow’s isolation and undermine its efforts to widen the Kremlin’s diplomatic sphere of influence. Growing Russian domestic frustration with Putin’s inability to deliver on his promises of a resurgent Russia will ultimately weaken his regime’s grip on power. The more successful that the United States and its allies are in clearly articulating the connection between Russia’s destabilizing activities and its imposed pariah status, the more opportunities there will be to use such isolation as a point of negotiation to promote a more positive relationship and convince Moscow to cease its unacceptable activities.

Ideologically, the United States and its allies must undertake an aggressive strategic messaging campaign designed to undermine Putin’s legitimacy as a leader, highlight the pervasive corruption and inefficiency in Moscow’s governmental systems, and extol the virtues of true representative democracy as an alternative to Putin’s autocratic regime. These ideological efforts should be directed both against the Russian “Near Abroad” along its Eastern European border as well as internal to the Federation. Russian influence operations conducted in bordering countries target chiefly ethnic Russians and local governments to incite instability and then paralyze local responses until Russia can achieve its strategic objectives.  

The Kremlin has applied this model repeatedly, beginning with Georgia in 2008, Crimea and Eastern Ukraine in

---


2014, and most recently against the Baltic republics. In seeking to reach those same populations, Western influence operations should incorporate supporting cyber activities that amplify the overall effects and achieve greater influence over Russian behavior both in the targeted border states and domestically within Russia itself.

Such ideological influence operations will also encourage and support increased domestic opposition to Putin’s disruptive policies. Internally, this increased political opposition potential can provide valuable Russian domestic allies for the United States to support in further undermining the Kremlin’s destabilizing activities. Russian government interference in the 2016 US elections clearly demonstrates the potential strategic impact of a well-coordinated and executed influence campaign against an adversary. Furthermore, recent changes in Russian military organization and domestic authorities demonstrate the extent to which the Kremlin is concerned about internal instability. Recent years have seen widespread assassinations, unjust imprisonment, and general oppression of domestic sources of opposition to Putin’s regime. With proper international recognition, support, and engagement, these sources of domestic opposition could become powerful tools to influence Putin’s behavior. Finally, ideological support to the Russian domestic opposition is a vital avenue to facilitate an eventual transition to a more transparent and representative Russian government. It is also important to note the potential moral hazard created in externally supporting domestic Russian opposition, given the lengths to which Putin has already demonstrated he will go to silence dissent to his continued rule. Internal opposition groups that receive support and engage constructively with the United States and its allies may face additional negative attention from Russian security services, suggesting that great deliberation, planning, and care be taken in pursuing such ideological operations.

Militarily, the United States should develop aggressive options for applying military pressure on Russia to regain the initiative in the escalation domain. Escalation dominance is a critical component of Russia’s “New Generation Warfare”, which Russian Chief of Staff Valery

Gerasimov first described in 2013 and is now in current Russian military doctrine. Under this concept, Russian military forces encourage and exploit instability in a targeted country before intervening to seize strategic objectives. After achieving their objectives, Russian military forces can then escalate, or demonstrate an intention to escalate, the level of violence to dissuade any reactive effort to turn back these advances. Currently, the US and NATO strategy for addressing such Russian destabilizing activity focuses predominately upon minimally reactive measures conducted only in allied-controlled territory. This overly defensive focus severely limits military options and essentially denies the United States and its allies an opportunity to achieve local escalation dominance against Russia.

To offer US policymakers with a wider range of options to counter Russian military aggression, the United States and its allies must pressure Russia militarily by providing additional levers of escalation by which to influence the Kremlin’s strategic calculus. Specifically, the United States should increase rotational military deployments, foreign military sales and the provision of lethal aid in Eastern Europe, expand security force assistance training, comprehensively support development of resilience and resistance potential in threatened states, and, where and when appropriate, support indigenous resistance against Russian military activity. The United States and its allies should immediately respond to continued Russian interference of Eastern Ukraine by providing lethal military aid and other military assistance in the form of intelligence, training, and strategic-level advisement. The Kremlin continues to deny its deep involvement in the conflict. Therefore, more aggressive military pressure will both increase the cost to Russia of the conflict (which the struggling Russian economy can ill-afford) and embolden domestic opposition to Putin’s continued adventurism abroad. Rotational deployments of US forces to Eastern Europe, increased training and integration with partners, and efforts to increase the resilience and resistance potential in states threatened by Russian aggression will have an immediate impact on Putin’s strategic calculus as he sees potential costs of further interference.

In the short term, Putin will likely pause his destabilizing activities as he reassesses the likelihood of achieving his immediate objectives without entering into an unwinnable escalatory spiral. The lack of external Russian expansion will, in the long term, cause discontent among Russian nationalists and embolden Putin’s domestic opponents.

Economically, increased sanctions that target a wider range of key Russian businesses, policymakers, and oligarchs (as well as their families and associates), will systemically undermine all the Kremlin’s global ambitions and destabilizing activities. Past sanctions imposed by the United States and its allies were too narrowly focused, allowing Putin and his cronies to hide their substantial (and often undeclared) wealth in overseas accounts or with family members and other associates. By expanding these sanctions the United States can further pressure the Kremlin’s decision-making processes. Particularly if sanctions start to directly affect the personal wealth of Putin and his closest associates, the potential for influencing Moscow to curtail its unacceptable behavior should increase exponentially. Escalatory sanctions will also create the potential to deescalate those same measures, providing valuable tools for moderating the Kremlin’s behavior and improving the negotiating strength of the United States and its allies in relation to Russia. Continued economic pressure on Russia will starve its already weakened state of the lifeblood that fuels all its ambitions: money. Without access to overseas investment, banking mechanisms, or consistent incoming revenue, Moscow will not be able to sustain its grandiose military modernization programs or conduct comprehensive influence operations abroad. Similarly, continued economic freefall will negatively affect the already eroding Russian quality of life, which will increase domestic opposition to Putin’s continued ineffective and corrupt rule. Constriction of critical revenue streams will also nullify Putin’s personal patronage system, the primary means by which he maintains the critical loyalty of his core supporters. Without this support, Putin will have to cease his destabilizing activities or face ruinous ouster. Economic pressure, while slow to build and realize its fullest impact, will undoubtedly have the most influence on the future direction of the Russian Federation.

---

Calming the Vulnerable Population: Inoculating Against Panic

Despite the alarm and fear-mongering that accompany much of the coverage of Russia’s aggressive and destabilizing activities in the Western media, the Russian Federation is an incredibly weak state and is deserving of the moniker “The Sick Man of Eurasia.” Russia’s significant diplomatic, ideological, military, economic, and demographic shortcomings all suggest that it is a state that will never pose a legitimate challenge to the United States, its allies, or the established liberal world order. For all of Putin’s bluster and ambition to restore Russia’s past “glory,” the Federation is more diplomatically isolated, ideologically bereft, militarily incapable, economically weak, and demographically mixed than at any point in recent history. For all the promises that Putin has made to the Russian people, it is unlikely that he will ever be able to deliver on them, and will lean on internal oppression to quell rising opposition to his corrupt rule. Given these circumstances, the United States and its allies should implement an updated “quarantine” strategy to minimize Russia’s negative influence. Ideally, this approach will encourage a peaceful Russian transition to a more transparent, responsible, and democratic form of representative government by containing Russia’s destabilizing behavior until the Federation’s own internal weaknesses overwhelm the Putin regime.

About the Author

Doug Livermore works in the Office of the Under Secretary of Defense (Intelligence) as an operational advisor as well as serving as a Special Forces officer with Special Operations Detachment – NATO in the Maryland Army National Guard. In addition to multiple combat deployments to both Iraq and Afghanistan, Doug led special operations elements during sensitive contingency operations across Africa. He is a West Point graduate currently pursuing his master’s degree full time through Georgetown University’s Security Studies Program. The views expressed in this article do not represent the positions of the Department of Defense or any other part of the U.S. government.
US Assistance to Syrian Kurdish Forces

Rebecca Lucas

US Special Forces support for Syrian Kurdish forces fighting ISIS, most prominently the People’s Protection Units (YPG), has focused on military support such as train and equip missions. However, the YPG’s increasing territorial control indicates that in order to ensure long-term stability in Syria, the United States needs to assist with building the institutions necessary for good governance. Historical examples indicate that, even with this support, the United States cannot control its partners enough to ensure that they do not act in ways that perpetuate instability and popular dissent.

Though the United States does not want to make long-term commitments in Syria, support for governance and nation building may be necessary to achieve long-term stability within Syria. To combat the Islamic State (ISIS), the US military is training and equipping multiple local groups, including a Syrian Kurdish group known primarily by their acronym, the YPG.1 The YPG has consistently made headlines a variety of reasons, including its secular ideology, the efficacy of its fighting forces, and the novelty of its all-female units. Despite extensive media coverage of US assistance to the YPG, US officials describe the relationship as “temporary” or provide non-committal answers about the depth of the relationship. 2 Unfortunately, YPG actions will continue to impact US policy in the region long after Special Operations Forces (SOF) have left Syria, particularly now that the United States is openly providing equipment to the YPG. If the United States’ desired end state in Syria is anything more complex than the immediate elimination of ISIS, American policymakers must accept the need for a more multi-faceted relationship with the YPG to ensure that it avoids perpetuating the Syrian civil war and continues to further regional stability. This article will discuss SOF assistance and US policy towards the YPG before focusing on problems of governance raised by the YPG’s recent and rapid expansion of territorial control. Finally, it will briefly offer policy recommendations.

1 “YPG” is the acronym for the group’s Kurdish name, Yekîneyên Parastina Gel. The English translation, “People’s Protection Units” is less frequently used, and never used as an acronym.
SOF Assistance

“Train and equip” programs, including the assistance the US currently provides to the YPG, are one of the critical capabilities of US Special Operations Forces (SOF): the ability to indirectly conduct operations against adversaries around the world by forming partnerships with a variety of local actors. Bolstering the capabilities of organizations whose interests align with US national security objectives can be a resource-efficient and sustainable means of addressing US adversaries. Support to non-state actors, such as the YPG, is considered Unconventional Warfare (UW). UW is a key component of SOF capabilities used to indirectly influence operational environments and pressure various state and non-state actors.

Given the increases in the YPG’s increasing territorial control and governmental institutions, however, UW support to the group bears a greater resemblance to Foreign Internal Defense (FID), as the YPG is the governing authority in much of Syrian territory. FID refers to activities in support of a state’s internal defense that enable it to address causes of instability and “protect against subversion, lawlessness, insurgency, terrorism, and other threats to their security, stability, and legitimacy.” Like UW, FID is a key component of SOF capabilities against various state and non-state actors; however, it also includes any support necessary to maintain internal stability. UW and FID support both span the spectrum of armed conflict and can include counterinsurgency (COIN). While typically focused on military activities, FID and UW can also include other non-military sources of support, such as economic, political, and intelligence assistance.

US Assistance to the YPG

The YPG is a Syrian Kurdish militia that, through its political wing, the PYD, controls a region of Syria that has been de facto autonomous since 2011. The YPG has become a valuable US partner in Syria, as it is one of the foremost forces on the ground in the campaign against ISIS. This partnership is complicated, however, by the general consensus that the YPG is the

---

3 Public Law Title 10 Section 167, United States Special Operations Command.
4 The political wing of YPG, Partiya Yekitiya Demokrat (PYD) or “Democratic Union Party”, is technically the governing authority in the territory they hold. However, given that the two organizations are closely intertwined, for simplicity’s sake I will refer to both as the “YPG” throughout this article.
5 Special Operations JP 3-05, Joint Publication (April 18, 2011), p. II-8. JP 3-05 states, “UW activities are conducted in support of a resistance or insurgency in a denied area…where the governing authority has the capacity to deny overt freedom of action” (JP 3-05 II-8).
6 Ibid, II-11.
7 Ibid, II-10.
8 Ibid, II-12.
9 Ibid, II-11.
Syrian affiliate of the Kurdistan Workers’ Party, better known by their Kurdish acronym PKK (Partiye Karkeren Kurdistan). The PKK engages in an insurgency against the Turkish government and both the US and the European Union consider it a terrorist organization. Due to this affiliation, the Obama administration proceeded very carefully with YPG train and equip programs, and started by partnering with the YPG for specific operations, including targeting air strikes.\textsuperscript{10} The YPG made it easier for the administration to provide support by joining a small number of non-Kurdish groups to form the Syrian Democratic Forces (SDF) in October 2015. The SDF became the beneficiary of wide-ranging US military support, although US officials clarified that weapons were only provided to non-Kurdish elements within the SDF due to YPG ties to the PKK.\textsuperscript{11} Opponents of the YPG, led by the Turkish government, criticized the SDF as merely a rebranding of the existing group, as Kurds constituted the majority of SDF forces and YPG commanders maintained leading roles.\textsuperscript{12} In addition to material support, US SOF have been co-located with SDF forces since late 2015, providing training and—at times—heavy artillery support.\textsuperscript{13} Over that period, the YPG continued to insist that, while they adhered to certain components of PKK ideology, they were an independent group, albeit one with some shared aspects of ideology.\textsuperscript{14} Despite vociferous Turkish objections and the legal quagmire of supporting a group that was debatably part of a designated terrorist organization, the Obama administration committed a large number of resources to working with the YPG by the end of 2016.

As part of the Trump administration’s more aggressive approach to ISIS, the Pentagon announced in May that US forces were now authorized by President Trump to directly equip Kurdish elements of the SDF.\textsuperscript{15} As a nod to Turkish objections, the Pentagon clarified that the flow of US arms would be linked to specific operations and would be carefully monitored to prevent weapons from being diverted to the PKK.\textsuperscript{16} Other officials have stated that the United States intends to restrict the use of weapons to specific battlefield missions and require that they

\textsuperscript{11} Ibid.
\textsuperscript{12} Ibid.
\textsuperscript{13} Ibid., 14.
\textsuperscript{15} Humud, Blanchard, and Nikitin, “Armed Conflict in Syria,” p. 14.
be then returned to US control.\textsuperscript{17} Further, officials have stated that the supply of weapons will be cut off if evidence emerges that the YPG is diverting weapons for use outside of the designated operations.\textsuperscript{18} Not surprisingly, this has not mollified Turkey, who believes that the YPG still answers to the PKK commanders in Qandil, Iraq. Whether or not Turkey’s concerns are justified, President Trump’s decision to explicitly engage with Kurdish groups within the SDF has further tied the United States to YPG actions. Such a tie has the potential to create multiple unintended consequences and ramifications for the United States, as has happened in past “train and equip” operations.\textsuperscript{19}

**Influencing Partner Behavior**

One of the chief causes of unintended consequences in “train and equip” operations is the unforeseen actions of US partners. Though UW and FID are effective and efficient ways for US SOF to support policy objectives, local partners are ultimately independent actors. Therefore, UW and other means of indirect support also entail the sacrifice of some measure of command and control (C2) over the forces in the field. Strengthening actors over whom the United States does not have complete C2 can have a number of unforeseen consequences. It is therefore important to understand the interests and objectives of those with whom the United States partners and ensure that they match or at least complement US interests and objectives. The historic record shows that divergent interests can prove challenging when dealing with local partners.\textsuperscript{20} These interests may lead states to act in ways that do not contribute to, or even work against, US strategic interests. If US support has been overt, this is particularly problematic, as the United States will be linked to any policies the actor pursues, whether or not it agrees with them. Differing and diverging interests between the United States and partners such as the YPG are an important consideration in the provision of FID and UW support.

When divergent interests occur, the United States can use incentives or pressures to affect partners’ behavior; however, US policymakers frequently overestimate the amount of leverage that they have over a potential partner and therefore overlook potential points of friction. For example, influence over partners in such circumstances often stems from the money, equipment,


and training that US SOF can provide; however, once partners have the equipment and training in hand, it can be difficult to take it away. This leaves the United States in a conundrum: as the amount the United States invests in a partner increases, and therefore the more closely that partner’s actions reflect on the United States, its leverage over that partner often faces a corresponding decrease. Further, policymakers may be reluctant to withhold support from critical US allies for fear of allowing instability to return or an adversary to gain the advantage. Finally, when the United States eventually withdraws some or all of its support, it loses the bulk of its influence over partner actions or overall outcomes. The United States faces difficulties exercising and enforcing C2 over its partners, particularly when their interests diverge.

For example, throughout the 1980s, the United States provided FID support to the Government of El Salvador as it fought a civil war against the leftist Farabundo Martí National Liberation Front (FMLN). Both the Carter and Reagan administrations saw this support as the only way to prevent a communist takeover in Central America. While US support to El Salvador is often seen as a success story, the behavior of the Salvadoran regime during this period, particularly the Armed Forces of El Salvador (FAES), undermined US tactical and strategic aims, as well as Salvadoran stability. Despite US encouragement to pursue a “hearts and minds” focus, FAES committed widespread human rights abuses. Such abuses undermined the government’s legitimacy, causing large portions of the population to openly support FMLN. As the Salvadoran example demonstrates, the lack of C2 over local state and non-state actors is a critical component of UW, and therefore requires attention from policymakers.

The YPG’s lack of governing experience and official institutions makes this concern particularly acute. The US encounter with these issues in El Salvador, a country with an existing government and established institutions, points to the difficulty of successful resolution. The YPG is currently in the process of building and expanding its systems of governance, making command lines more fluid and centralized. This makes exercising C2 and mitigating problems that arise even more difficult.

**Beyond the Battlefield: The YPG and Governance**

Equally as pressing as C2, however, is the challenge of good governance in the territory the YPG has so rapidly acquired with US assistance. The YPG, which previously had no governing experience, has achieved considerable territorial gains since the outbreak of the Syrian

---


Civil War. After initially taking control of a primarily Kurdish area in northern Syria soon after war broke out in 2011, the YPG expanded its holdings at an increasing pace, particularly over the past two years. The YPG now controls a contiguous belt of territory along the Turkish-Syrian border over which they declared a federal system of governance in 2015.\textsuperscript{23} Even if their territorial control is only temporary, they will need to maintain good governance in the interim before working with the central government, presumably in Damascus, to facilitate a long-term solution. This territory includes an unprecedented number of non-Kurdish communities over which the YPG now has control.\textsuperscript{24} A history of ethnic tensions and resentment between Kurds and Arabs in the region, as well as the perception of ISIS as a Sunni Arab organization, create ample opportunity for conflict.\textsuperscript{25} While the United States is understandably leery about the prospect of providing nation building assistance, particularly in the Middle East, it is necessary in order to consolidate the progress made against ISIS and other extremist groups.

YPG governance is primarily based on the leftist ideology of democratic confederalism, a federal system that emphasizes limited central authority and localized decision-making.\textsuperscript{26} The group stresses an emphasis on gender and class equality, democracy, and human rights.\textsuperscript{27} However, though its governing ideology may look good in theory, putting any ideology into practice is difficult even assuming the best intentions. If the ideology is merely window dressing to make an authoritarian system more appealing to Western allies, as some opponents claim, the situation is even worse. Even if the YPG has the best of intentions, democratic confederalism is not without its problems. The ideology is the creation of Abdullah Ocalan, the leader of the PKK who, prior to his arrest in 1999, implemented an autocratic system of leadership over the group.\textsuperscript{28} While Ocalan’s stated ideology may include respect for human rights, it actually adheres to an authoritarian command structure that has placed human rights goals far behind military goals. Between the difficulty of establishing any form of government in occupied Syria and the lack of good models for democratic governance, US nation-building support is essential to consolidate the YPG’s territorial control without a turn to oppressive tactics.

\textsuperscript{26} Kajjo, “Writings of Obscure American Leftist Drive Kurdish Forces in Syria.”
\textsuperscript{28} Bradley and Parkinson, “America’s Marxist Allies Against ISIS: A Personal War.”
Also of concern is the cult of personality surrounding Ocalan. YPG-controlled areas such as Rojava revere Ocalan and opponents of the YPG perceive a level of devotion that leaves little room for disagreement or dissent. A 2017 Washington Post article described a requirement that new recruits learn Ocalan’s ideology before being deployed; this applied to Arab as well as Turkish recruits. Anecdotes from a 2015 New York Times article described a YPG fighter calling in American air strikes from a phone with an Ocalan screen saver, and saying Ocalan’s face was also a common sight in YPG headquarters and pinned to fighters’ uniforms. Despite remaining in prison, the reverence for Ocalan belies claims of a YPG system aspiring to egalitarianism, instead recalling centralized systems that are not tolerant of dissent. The PKK’s leadership, for example, still consists of many of the same men who founded the group with Ocalan in 1979. This is a concern both given Ocalan’s history of authoritarian leadership over the PKK and the YPG’s future relations with other countries in the region, as this article discusses below.

Given this precedent of authoritarian rule, the YPG needs to design institutions to ensure that power rests with individuals accountable to the public rather than military leaders. Despite not wanting to be involved in such decisions, US assistance is already affecting power structures within the YPG. In providing training and equipment, US SOF are primarily engaging with military commanders, and thereby strengthening their influence in relation to civilian commanders. Western observers have alleged that, despite the presence of elected officials, military commanders retain most of the power. While to some extent this is the consequence of the importance of the military in day-to-day life in conflict-ridden Syria, the US disinclination to engage with, much less provide resources or training to, civilian leadership exacerbates this trend. Of further concern is the claim that many of these military commanders gained their battlefield experience fighting with the PKK in the 1990s under Ocalan’s top-down leadership; therefore, they have no experience with democratic or civilian governance. Regardless of US desire to

---


33 Sly, “US military aid is fueling big ambitions for Syria’s leftist Kurdish militia.”

34 Ibid, 15.
involve itself in questions of governance, the effects of US aid are already shaping power dynamics within the YPG.

Causes for Concern: YPG Performance to Date

Human Rights Watch and Amnesty International are among those who allege that the YPG already has a poor history of democratic, civilian leadership. In 2014, Human Rights Watch voiced concerns about violence against unarmed protestors, the use of child soldiers as young as thirteen, and abuses by police.\(^35\) In the same year, Amnesty International accused the group of destroying entire villages due to suspicions that they harbored ISIS fighters.\(^36\) While there were Kurdish villages that fell victim to such treatment, Amnesty alleged that the YPG disproportionately targeted Arab and Turkmen villages with—what the human rights watchdog termed—"war crimes."\(^37\) The YPG disputes the accusations, stating that any displacements that occurred were necessary for villagers’ security and pointing out that they fully cooperated with the investigations.\(^38\) Further, they responded to the Human Rights Watch report by passing a law that prohibited enlistment by anyone under 18. However, allegations of misconduct—particularly against political dissidents—continue.

In addition to highlighting the need to provide political and social aid to the YPG, the Human Rights Watch report also demonstrates that an American push for improved governance is not a quixotic endeavor, particularly if the YPG is really committed to democratic values. Condemnation from an international human rights organization with no enforcement power led the group to at least overtly curtail its use of children as soldiers against ISIS. Even if the incentive for reform is public image preservation rather than genuine ideology, such changes have value and require minimal effort on the part of the US government or non-governmental partners.

The YPG and Regional Disputes

In addition to US concerns about supporting good governance within YPG territory, there are also concerns about the YPG’s relationships with the countries surrounding it. Exploring the many fraught relationships in the region and potential points of friction is beyond the scope of this paper; however, it remains an important point to address, particularly given the

\(^{36}\) Enzinna, “A Dream of Secular Utopia in ISIS’ Backyard.”
\(^{38}\) Enzinna, “A Dream of Secular Utopia in ISIS’ Backyard.”
introduction of overt US weaponry. Any idea that the YPG will simply give these weapons back after completing a limited operation is at best foolish, and at worst intentionally deceptive. Furthermore, the idea that the US military can accurately track all potentially lethal military equipment that it provides to the YPG and will have the manpower to recover it if it is lost or diverted, also strains credulity. Should individuals go on to use US-provided weaponry in an attack on the Kurdistan Regional Government or Turkey—both important US partners engaged in conflict with the PKK—the consequences could be disastrous. Therefore, the United States must consider realistic ways to mitigate this risk such as encouraging the YPG to further distance itself from the PKK. The full set of such options falls beyond the scope of this article, which is primarily focused on the importance of YPG governance; however, non-inflammatory foreign relations are an important aspect of responsible governing behavior. US policy must account for this area of governance as well.

US Goals

In order to achieve lasting success in Syria, the United States must first determine its desired and sustainable end state, particularly as it concerns essential partners—such as the YPG and Turkey—and adjust its levels and types of partner support accordingly. Any goal beyond the immediate and narrow military defeat of ISIS will require the YPG to develop the capacity for good governance, even if only in the short-term, and will require the United States to create a plan to support the YPG’s establishment of the infrastructure and institutions it requires to govern effectively. Further, the United States must cultivate additional alliances in the region in order to maintain leverage over the YPG and thereby ensure its other actions have an effect.

In light of the apparent challenges, US policy must reflect a comprehensive plan that goes beyond enhancing the YPG’s military capacity. SOF must coordinate their activities with also interagency and international partners to help the YPG bolster its capacity for local governance and develop the institutions that enable it to do so. Efforts to encourage sustainable development will also contribute to stability in this proto-state. Whether these efforts ultimately result in an independent state or simply enable the YPG to govern this population until such a time as central authority is reasserted in Syria, they should be treated as a critical component of SOF activities. This becomes especially important in light of the increasing number of Sunni Arab communities falling under YPG control, since many experts argue that the disenfranchisement of these communities under previous governments greatly contributed to the rise of ISIS.39 As US

investment in stability operations or reconstruction efforts have thus far been limited, a shift in thinking will be necessary to adopt this change in policy.

In addition to planning its relationship with the YPG, the United States must also reach out to other regional actors to create a network of alliances and maintain leverage over the YPG. The US ability to influence YPG behavior is primarily contingent on its ability to withdraw military support. If the YPG is the only effective US partner in the fight against ISIS, the US cannot credibly threaten to withdraw any degree of support for fear of emboldening and empowering ISIS. To return to the Salvadoran example, many experts believe that the inability of the United States to rein in Salvadoran human rights abuse was due, in part, to the importance US policy placed on preventing the spread of communism in Central America. Assistant Secretary of State James Cheek later observed that US leverage in El Salvador depended on promises of future military aid, which the United States was never entirely prepared to withdraw for fear that the Salvadoran government would fall. US officials rationalized that preventing an insurgent victory had to take priority over concerns regarding human rights. Knowledge of such beliefs would have diminished incentives for the Salvadoran government or FAES to heed US warnings or advice. Similarly, a lack of viable alternatives would severely diminish the US ability to influence YPG behavior should its interests, and those of the YPG, diverge. Though the United States has found a reliable and valuable ally in the YPG, it must continue to diversify its partners in the fight against ISIS in order to retain any degree of control over the YPG.

US policymakers have been successful in creating a military partnership with the YPG in the fight against ISIS. However, they have not yet taken steps necessary to execute a desirable end state in Syria. In order to maintain stability in Syria and prevent further humanitarian strife, the United States must broaden the scope of its involvement with the YPG to include interagency support for good governance, institution building, and capacity building beyond simply military skills. While “nation-building” is an understandably fraught term for the US military, it is an important component of the support SOF is capable of providing. In this case, the United States must ensure that the YPG is able to govern the territory it has gained without creating further instability or sectarian division. To all appearances, the YPG is a capable ally who has every intention of building their own nation with or without US support. The United

States must therefore pursue a whole-of-government approach to its cooperation with the YPG to execute a desired end state in Syria.

About the Author

Rebecca Lucas is pursuing a master's degree in Georgetown University's Security Studies Program with a concentration in terrorism and substate violence. In addition to her coursework, Rebecca is a Senior Consultant at Booz Allen Hamilton supporting various Department of Defense clients. She graduated from Wellesley College cum laude with departmental honors in her major, Political Science, and a minor in religion.
Domestic Politics, Military Reforms, and Threat Perceptions: Three Factors Influencing Russian Decision-Making in its Near Abroad

Nicholas Fedyk

The troubling escalation in Russian-American tensions today partly stems from Russian meddling in Ukraine. Of all the countries that make up Russia’s near abroad, Ukraine is the most populous and prosperous, and its positioning between Europe and Russia has made it a flashpoint in big power politics in recent years. This article explores why exactly Russia is destabilizing Ukraine by comparing President Putin’s different responses to two revolutions in post-Soviet Ukraine—the 2004 Orange Revolution and the 2013–2014 Euromaidan. After establishing that the revolutions are sufficiently similar to merit comparison, I will evaluate three potential factors that influenced Putin’s response:

1. The transition of Putin’s inner circle of advisers from liberal, Western-oriented economists to security-community colleagues more skeptical and hostile towards the West.
2. Military reforms that significantly improved the performance of the armed forces.
3. Escalating threat perceptions associated with Ukraine and its Western allies.

I conclude that in 2014 Putin was more willing (due to Russia’s domestic politics), more capable (due to Russia’s military reforms), and more threatened (due to Russia’s geopolitical situation) to utilize military force against Ukraine. At a time when Russia has become a major national security priority, this bears several lessons for countering future Russian adventurism.

HISTORICAL CONTEXT

Orange Revolution

Let us begin by examining the Ukrainian revolutions in greater detail. First is the Orange Revolution. In the 2004 president election, Viktor Yushchenko’s Our Ukraine party (Nasha Ukraina) squared off against Viktor Yanukovych’s Party of Regions (Partiya Reioniv). The parties represented different polarities of the electorate. Yushchenko was the liberal, European-leaning reformer who promised to weaken oligarchic influence and draw closer toward NATO membership. Yanukovych was the eastern oligarch supported by “Euroskeptics” who promised stable, close ties with Russia. When final results showed Yanukovych winning by an inconclusive margin, Yushchenko’s supporters accused Yanukovych of fraud and filled Kiev’s Independence Square, waving the orange flags of Nasha Ukraina. The Supreme Court nullified the results, and sure enough, Yushchenko won the second run-off in December 2004.
Western support for the Orange Revolution was overwhelming. US Secretary of State Colin Powell, US Ambassador to Ukraine John Herbst, and their European partners applauded the peaceful and democratic transition of power. Government agencies contributed material support. For example, through the US Agency for International Development, National Endowment for Democracy, and the vast network of philanthropic charities led by George Soros, the US State Department allocated an estimated $65 million to support democratic institution-building in Ukraine.¹

Putin, however, had the opposite reaction and fiercely criticized what he deemed to be a chaotic and illegitimate coup. He clearly supported the Party of Regions, appearing publicly with Yanukovych before each election round. Russian political elites smeared Yushchenko, accusing him of ties with radical Nazi sympathizers and Polish nationalists who would incite violence and threaten Russian minorities in Ukraine.² Yet Putin’s response was limited to words, and never did he threaten forceful retaliation.³

**Euromaidan**

The 2014 Euromaidan Revolution is the second case study. Though defeated in 2004, Yanukovych remained the head of Partiya Reioniv and eventually won the 2010 presidential elections.⁴ During his first three years in office, Yanukovych established trade partnerships with both Russia and the European Union. He even drafted an “association agreement” with the latter in March 2012, which provided a framework for closer cooperation with the European Union and a pathway for liberal economic and judicial reforms. But after its drafting in 2012, Yanukovych stalled its final ratification, claiming he was seeking more favorable terms. He announced its official postponement in November 2013.

Just as in 2004, protestors gathered in Kiev’s Independence Square—this time demanding a renewal of the EU integration process. Unlike the Orange Revolution, Euromaidan turned violent. The Berkut riot police did not side with the protestors, as they did in 2004. Instead, they

---

3 Putin argued thus: “A rerun of the second round may also produce nothing... What happens then? Will there have to be a third, a fourth, a 25th round until one of the sides obtains the necessary result?” See Terence Neilan, “In Shift, Putin Says He Will Back Whomever Ukraine Elects,” accessed April 13, 2017, https://www.nytimes.com/2004/12/06/international/europe/in-shift-putin-says-he-will-back-whomever-ukraine.html.
4 This time, the results were uncontested; Yuschenko won a mere 5 percent of the first-round vote, and Yanukovych defeated opponent Yulia Tymoshenko by a final tally of 48.95 percent to 45.47 percent.
advanced on the Euromaidan, leading to bloody clashes in February 2014. The sheer number of protesters overwhelmed the police; using improvised weapons, they chased Yanukovych out of his presidential headquarters and overran the parliament building. Protest leaders Petro Poroshenko, Vitaly Klischko, Arseny Yatsenyuk, and Oleh Tyahnybok organized snap elections and installed a new government.

These chaotic events drew swift reactions from the international community. As in 2004, the United States and Europe applauded the revolution and played an active role in encouraging, shaping, and funding its leaders. Several congressmen, notably Senator John McCain, repeatedly visited Independence Square and praised the Ukrainians’ love for freedom and democracy. Ambassador to Ukraine Geoffrey Pyatt and Assistant Secretary of State Victoria Nuland hand-picked certain protest leaders during the transitional elections, all but guaranteeing their victory.5

Putin, meanwhile, decried the revolution as a violent and illegitimate coup—another destabilizing “color revolution” that threatened Russia’s sphere of interest. Perhaps motivated by this insecurity—which will be explored later in this article—he deployed teams of special operations troops to orchestrate a military takeover of Crimea.6 In February 2014, these “little green men” quietly took over the Crimean parliament building, the Ukrainian Navy’s headquarters in Sevastopol, and other strategic locations. Crimea was de facto annexed into the Russian Federation on March 16. That same month, Russian forces executed a second military operation in Donbas, aiding separatist insurgents with manpower, lethal and humanitarian aid, and military training. Shadow governments emerged in the cities of Donetsk and Luhansk, which remain to this day.

THREE FACTORS EXPLAINING RUSSIAN BEHAVIOR

What factors influenced Putin’s dramatically different responses to these two revolutions? This section develops and tests three possible—and ultimately plausible—explanations. Alternative explanations are evaluated at the end of this article.

6 Many of these “little green men” hailed from the Special Operations Command, a new clandestine unit formed in 2009 which reported directly to the Russian General Staff. They were aided by the 45th Spetsnaz Regiment and possibly the 810th Marines Brigade already based in Sevastopol, giving the intervention a local flavor. Their unmarked uniforms made it difficult to pinpoint their exact origin and allowed Putin to deny that they were Russian forces at all. See Anton Lavrov, “Russian Again: The Military Operation for Crimea,” in Brothers Armed: Military Aspects of the Crisis in Ukraine, ed. Colby Howard and Ruslan Pukhov (Minneapolis: East View Press, 2014), 157–86.
Factor 1: Changing Domestic Politics Increase Hostility Toward West

The first factor is changing domestic politics; that is, the economists, wonks, security personnel, and oligarchs who comprise Putin’s “inner circle” changed between 2004 and 2014 in a way that increased hostility toward the West. As scholar Marcin Kaczmarski argues, three major shifts have occurred over the past 17 years, adapted in the chart below. 7

Figure 1: Shifts in Putin’s Inner Circle

<table>
<thead>
<tr>
<th>Period</th>
<th>Years (Approx.)</th>
<th>Dominant Group within Inner Circle</th>
<th>Outlook</th>
</tr>
</thead>
<tbody>
<tr>
<td>Period 1</td>
<td>2000 - 2003</td>
<td>- Liberal economists like Anatoly Chubais and Alexei Kudrin&lt;br&gt;- Advisers carried over from Yeltsin administration</td>
<td>- Attempted economic liberalization&lt;br&gt;- Emulation of and partnership with Europe and United States</td>
</tr>
<tr>
<td>Period 2</td>
<td>2004 - 2011</td>
<td>- Economic elite who benefited from nationalization, like Igor Sechin</td>
<td>- Nationalization of domestic industries and protectionism&lt;br&gt;- Increasing competition with Western states</td>
</tr>
<tr>
<td>Period 3</td>
<td>2011 - Present</td>
<td>- Security colleagues from the KGB, like Sergei Ivanov</td>
<td>- Open hostility to Western states&lt;br&gt;- Discouraging international investments through “de-offshoreization”</td>
</tr>
</tbody>
</table>

The first period (2000-2003) began when Putin assumed the presidency in 2000 in a power vacuum. With little political capital, he relied on liberal economists like Anatoly Chubais and Alexei Kudrin (Putin’s former boss in the St. Petersburg mayor’s office) to consolidate his power. These individuals supported his dark horse presidential bid and turned the vote against his primary liberal competitor, Boris Nemtsov. As a veteran KGB officer based in St. Petersburg and East Germany, Putin came to Moscow as an outsider, and it is unlikely that he would have won the election without these endorsements. For this reason, liberals became especially influential during this first period.

As per his endorsers’ advice, Putin prioritized market economics as essential to restoring Russia’s regional and global power status. 8 Economic liberalism aimed to integrate Russia into the world economy, increase private entrepreneurship, and increase international demand for Russian goods, particularly in Western Europe. For example, consider the booming natural gas and oil markets of the early 2000s. By 2003, the relatively prosperous states in Western Europe

8 Putin’s first Open Letter to Voters in February 2000 heavily emphasizes these sentiments.
consumed some two-thirds of Russian gas exports. Compared to Russia’s clients in Ukraine, Georgia, and other former Soviet countries that were frequently late on their payments, Western Europe presented a far more attractive opportunity for economic expansion.

Liberal economics led to a radical new vision of liberal politics. Anatoly Chubais—who served as Putin’s chief campaign manager, deputy prime minister, and economic adviser—argued that Russia was the vanguard of a new “liberal empire.” As its near abroad (i.e., Belarus, Ukraine, Kazakhstan, and other former Soviet republics) experienced democratic and economic stagnation, Chubais argued that Russia ought to reassert its dominance for the purpose of building a liberal imperialism that was uniquely Russian:

The government must maintain an active stance concerning the expansion of Russian businesses outside the country. This concerns not only commerce, but also asset purchases, opening of new businesses and development. The Russian government should actively support freedom and democracy outside Russia.

Increasing wealth was a national security priority that ought not be “muddied by the baggage of geopolitical pretensions” that could disrupt relations with the West, Russia’s greatest ally for spreading democratic institutions and market economics. Moscow decision-makers pursued this agenda by advocating for a relatively risk-averse response to the Orange Revolution in 2004. Putin was not yet willing to jeopardize his profitable relations with the West.

The liberal elites’ optimism was tempered in the second period (2004-2011). In fact, the very term “liberal” is rather misleading; what Russia experienced in the early 2000s is better characterized as nationalization under the façade of liberalism. Starting around 2004, Putin established seven state corporations, hand-picked oligarchs to run each of them, and granted subsidies so that they could compete with international firms. This was ostensibly done in the name of “market economics.”

The resulting fusion of political and economic power created a new class of economic elite dependent on Putin. “Kremlin, Inc.” was the new catchphrase of the new inner circle. Putin distributed power in a variety of ways. Some acquired material resources and enjoyed their new positions as chairmen and CEOs of business and energy conglomerates, like Gennady Timchenko. Others acquired political capital and were adept at building networks within the

---

9 Bobo Lo, Vladimir Putin and the Evolution of Russian Foreign Policy (London: Royal Institute of International Affairs, 2003), 63.
11 Lo, Vladimir Putin and the Evolution of Russian Foreign Policy, 64.
12 These include Rostekhnologii (high-tech industrials, now named Rostec), Rosnano (nanotech), and Rosatom (nuclear energy).
Kremlin, like Igor Sechin. But some oligarchs lost favor with Putin, either because they underestimated his authority or publicly criticized his policies, like Boris Berezovsky and Mikhail Khodorkovsky. The Kremlin charged them and others with money laundering, paraded them in show trials, and merged their private companies with state-run corporations.\(^{13}\) Benefitting from the increasing consolidation of political and economic resources, Putin did not hesitate to use the state's repressive power during this period. The steady transition away from liberal ideals increased the gap between Russia and the West, increasing the likelihood of conflict over Ukraine after 2004.

This gap would increase during the third period (2011-present). First, the strength of some elites empowered by nationalization began to wane. Kaczmarski argues that, as they bargained over political influence, the so-called “winning coalition” became increasingly divided and torn apart. The long-lasting effects of the global economic crisis further splintered this coalition. Those with the closest ties to the Kremlin became even more powerful, since smaller corporations loaned large amounts of money from state corporations to remain solvent. For example, development bank VeshEkonomBank provided $25 billion to help private Russian companies refinance their loans post-2008; in return, it received a significant percentage of shares of those smaller companies—sometimes as high as 25 percent.\(^{14}\)

Perhaps reacting to this internal chaos—and fearing the growing, disproportionate power of a small group of companies—Putin began reaching out to close personal allies over traditional business leaders. Many hailed from the security community, especially Putin’s KGB colleagues. Contrary to the new economic elites in the prior period, Putin’s inner circle is now increasingly comprised of career bureaucrats with little business leadership experience, like Sergei Ivanov, Dmitri Medvedev, and Vladislav Surkov. These individuals possess a high degree of so-called political resources. They are well-connected networkers and managers within the Kremlin, and know how to make themselves indispensable.

Several global patterns catalyzed the narrowing and redefining of Putin’s inner circle: the destabilizing “color revolutions” in Ukraine, Georgia, and Kyrgyzstan inspired by Western supporters; US and European opposition to Russia’s 2008 invasion of Georgia and the threat of punitive sanctions; and the 2012 collapse of Cypriot banks (with some $20 billion Russian assets). These hostile actions inspired Putin to call for Russians to reinvest their money inside Russia—supporting national businesses, banks, and entrepreneurs while insuring Russia against

---

\(^{13}\) Two examples of such take-overs are Rosneft acquiring Yuganskneftegaz (Khordorkovsky's main asset) for $9 billion in 2004 and Gazprom’s acquiring Sibneft for $13 billion in 2005.

global shocks or sanctions. Putin even attacked Russian oligarchs and politicians with large foreign portfolios. He proposed that any government official “in charge of key decisions” should declare their foreign assets or give up their position. In 2013 the State Duma passed a law with these exact measures, prohibiting ownership of foreign bank accounts and requiring elites to report all foreign assets.

By the time the Euromaidan Revolution broke out, the insular nature of the inner circle brought unique foreign policy perspectives to bear on Putin that would have been unimaginable a decade ago, when liberal economists sat closest to the president. Putin’s response was far more risk tolerant. De-offshorization separated Russian banks and businesses from the West, making Putin more willing to provoke Ukraine and its partners through the use of military intervention.

**Factor 2: Military Reforms Expand Putin’s Foreign Policy Toolkit**

A second factor that led Putin to a different course of action—intervention—in 2014 is Russian military reforms, which made Moscow more confident in its ability to intervene in its near abroad. Deficiencies in performance, management, and capabilities left Russia unprepared to execute any sort of military intervention in Ukraine prior to 2008—let alone after the Orange Revolution in 2004—especially in light of NATO expansion in Europe and the risk of conflict escalation. Setbacks in the 1990s illustrate this point, as described by Ray Finch: “The catalog of illnesses was long: corruption flourished while many officers went months without being paid; decent housing was in short supply; draft dodging was rampant while criminality within the ranks increased; equipment maintenance deteriorated and research-development funding was slashed.” Some 457,000 officers resigned between 1993 and 2002, and 80 percent did this so quickly that they forfeited their pensions. There was endemic psychological, emotional, and morale poverty among the officer corps.

Although the need for military reform was evident in Putin’s first term, progress was slow as demonstrated in Chechnya in the mid-2000s. Separatist insurgents posed operational and tactical challenges for heavy, slow-moving conventional Russian forces. The 2008 Georgia War

---

16 Not surprisingly, Putin selectively applied this law, targeting his most immediate challengers while pardoning his allies. Two of the most dramatic attacks were against former railway chief and Bank Rossiya founder Vladimir Yakunin, and former economic adviser Anatoly Chubais. Once one of the most powerful advisers within the Kremlin, Chubais is now closely aligned with the political opposition.
also revealed these shortcomings; though it only lasted five days, the outmatched Georgians inflicted a high number of Russian casualties and shot down three Su-25 jets, one Tu-22m bomber, and several armored vehicles. Poor local intelligence and under-equipped units (for instance, tanks lacked night-vision capabilities) contributed to these disproportionate losses.\(^\text{19}\)

Russia’s poor performance in the Georgian War signaled a need for dramatic reforms to command-and-control systems. Brookings fellow Pavel Baev argues that it is difficult to rationalize the “massive and chaotic” implementation of force in Georgia, which exhibited such a “complete incapacitation of several top layers in the rigid military hierarchy under the completely inexperienced Commander in Chief.”\(^\text{20}\) Russia’s performance in Georgia and Chechnya was also a product of inadequate combat readiness. Every defense minister prior to 2008 from Pavel Grachev to Sergei Ivanov lobbied for reforms to correct this flaw. But by 2008, no more than 20 percent of all Russian units were combat-ready.\(^\text{21}\)

Anatoliy Serdyukov’s appointment as Minister of Defense in 2007 marked a new era for military reforms. Serdyukov previously served as the Kremlin’s chief tax inspector and was infamous for leading the investigation and show trial of oligarch Mikhail Khodorkovsky. With no previous commitments to the military, Serdyukov was in a unique position to upgrade and revamp Russia’s officer corps from its Cold War mentality.\(^\text{22}\) In addition, Putin diminished the influence of the military by 2008—whose core leadership, fearful of losing their jobs, was itself opposed to reforms—by installing trusted security-community colleagues, particularly from the FSB and MVD, into top positions at the Defense Ministry.

These new reforms encompassed five primary goals: (1) improving combat readiness; (2) enhancing command and control; (3) improving officer and troop training; (4) modernizing weaponry and intelligence gathering; and (5) raising wages and living conditions for military personnel.\(^\text{23}\) The cumulative effect of these reforms made military doctrine more flexible, improved command structure and readiness, and improved overall capabilities.

First, doctrine. Today it is synonymous with the name Valery Gerasimov, the current Chief of the General Staff of the Armed Forces and the first Deputy Defense Minister. In his seminal article for the *Military Industrial Courier*, he argues that twenty-first century Russian military tactics ought to utilize a wide range of methods outside of traditional military force,

---

21 Shlykov, “The Secrets of Serdyukov’s Blitzkrieg.”
23 Roger N. McDermott, *The Transformation of Russia’s Armed Forces: Twenty Lost Years* (Routledge, 2016), 55.
including “political, economic, informational, humanitarian, and other nonmilitary measures—applied in coordination with the protest potential of the population.” Traditional military means such as airstrikes or infantry attacks should only be used as a last resort or when the conflict is reaching its final stage; even then they should be of a “concealed character.” This approach is critical in sensitive operations like those in Ukraine to avoid conflict escalation. Military analyst Roger McDermott compares this approach to using a scalpel instead of a sledgehammer.

Second, command structure. Serdyukov’s reforms created four new military districts to replace the Soviet six-district system. The personnel and equipment of the six military service branches are subject to the district commander’s authority and mission objectives. These reforms make military commands capable of quick mobilization in times of war—as quickly as an hour or two after the order is issued—without resupplying subordinate troops with personnel and equipment.

At the highest strategic level, the new National Defense Command Center (NDCC) in Moscow coordinates operations across military commands, serving as the nerve center equivalent of the White House Situation Room. The NDCC prioritizes the regional distribution of resources and training based on the security climate. The Western and Southern Districts bordering Ukraine have been the largest recipients of equipment upgrades and training exercises since 2014. For example, the 10th Armored Division was expected to be among the first to receive equipment upgrades in 2017, including the elite T-14 Armata tank and the Kurganets-25 infantry fighting vehicle. These excel in the quick-strike, mobile ground combat that has characterized new Russian ground offensives in Ukraine. They have carried out over 300 training and war games exercises over the past year, and repositioned forces closer to the Ukrainian border.

Third, personnel. Russia improved both its special operations and conventional capabilities after 2007. First, Serdyukov created the new Special Operations Command (SOC), which parallels the Spetsnaz divisions of the FSB (domestic intelligence), GRU (military intelligence),

---

26 Shlykov, “The Secrets of Serdyukov’s Blitzkrieg.”
and SVR (foreign intelligence). While it consists of only 1,500 personnel (by comparison, Spetsnaz GRU has about 12,000) it is under the direct control of civilian leadership, allowing Putin to directly utilize it to further strategic objectives. The SOC played a critical role especially in Crimea, coordinating a bloodless takeover in only 19 days. Furthermore, special forces had several “soft power” tools that facilitated intervention. They operated radio and television channels in Donbas that promoted Russian versions of events unfolding across the country and inspired fear of invading fascist forces from the West.

From the conventional standpoint, Russia’s improvements in mission planning, unit mobilization, and training were evident in a series of military exercises immediately preceding interventions in Ukraine. It led a series of training exercises with Collective Security Treaty Organization allies in Kyrgyzstan and Kazakhstan in 2014, rehearsing hypothetical scenarios like those seen in Ukraine. And on February 26, 2014, just one day before Crimea’s referendum on independence and a few weeks before hostilities began in Donbas, the Ministry of Defense organized “surprise” snap-inspections and combat readiness evaluations in the Western and Central Military Districts.

Finally, military personnel’s morale and training have improved since 2008. Officers are receiving better benefits packages, including an option to resign earlier than in Soviet times. Non-commissioned officers are receiving comprehensive education and increased pay for the first time since 1917. Other deficiencies such as housing shortages, outdated soldier kits, and dangerous hazing traditions have been addressed to varying degrees. In sum, these reforms have improved the capabilities and combat readiness of the Russian military, raising its effectiveness as a foreign policy tool in the near abroad.

These advances in doctrine, performance, and morale has sharpened the military’s role in Russian foreign policy. While armed intervention is not necessarily the most desirable option, it is at least a compelling instrument in Putin’s foreign policy toolkit that can be used in tandem with other methods.

**Factor 3: Russia’s Escalating Threat Perceptions**

A third factor is Russia’s escalating threat perceptions vis-à-vis the West between 2004 and 2014. The proliferation of “color revolutions,” NATO’s expansion into southern and eastern Europe in the early 2000s, the United States’ withdrawal from the Anti-Ballistic Missile Treaty in 2001, and interventions in Kosovo, Iraq, Afghanistan, Libya, and Syria—carried out despite

---

Putin’s opposition and jeopardizing Russian interests in those areas—forced the Kremlin back on its heels.

The proliferation of so-called “color revolutions” and overthrow of Russian allies in the near abroad was perhaps most unsettling. These include the 2000 Bulldozer Revolution in the former Yugoslavia, the 2003 Rose Revolution in Georgia, the 2004 Orange Revolution in Ukraine, and the 2005 Tulip Revolution in Kyrgyzstan. Overt Western support in the form of financial aid, elections advisers, and political statements added to Putin’s fear that the West was actively undermining Russia’s sphere of influence.

Putin’s alarm reached a boiling point in 2007 at the Munich Conference on Security Policy. In prepared remarks, he openly berated Western hypocrisy for the first time, and in a broader criticism of the global order, he exposed the flaws of unchecked US power that was unwisely “plunging the world into an abyss of permanent conflicts.” He then flatly condemned NATO’s expansion into Eastern Europe, as well as its permanent stationing of troops and equipment in Romania and Bulgaria (actions prohibited in the 1990 Treaty on Conventional Armed Forces in Europe). I quote Putin’s remarks in length to demonstrate his alarm:

I think it is obvious that NATO expansion does not have any relation with the modernization of the Alliance itself or with ensuring security in Europe. On the contrary, it represents a serious provocation that reduces the level of mutual trust. **And we have the right to ask: against whom is this expansion intended? And what happened to the assurances our western partners made after the dissolution of the Warsaw Pact? Where are those declarations today? No one even remembers them. But I will allow myself to remind this audience what was said. I would like to quote the speech of NATO General Secretary Mr. Woerner in Brussels on 17 May 1990. He said at the time that: “the fact that we are ready not to place a NATO army outside of German territory gives the Soviet Union a firm security guarantee.” Where are these guarantees?**

That was 2007. By 2014, the alarm level reached new highs. In the official Russian National Security Strategy published in 2015, Putin blamed the “unconstitutional governmental coup” (Euromaidan) in Kiev directly on the deceptive machinations of the West, now listed as one of the core threats facing Russia’s state and public security. The document’s severe tone is especially significant given its departure from the last security strategy published in 2009, which

---

expressed a short-lived optimism for Russia’s engagement and cooperation with its Western neighbors. In the wake of the Obama–Putin “reset,” that document went so far as to describe that relationship as a “partnership.”  

These destabilizing events had more than just military implications. Putin undoubtedly considered another successful Western-supported color revolution a threat to his political stability. For the past decade Putin had championed Russia as a great power, capable of standing toe-to-toe with Europe and the United States. The overthrow of ally Viktor Yanukovych in February 2014 begged the questions: Was Russia the great power that it claimed to be? Was Putin really a defender against Western expansionism? Russia’s subsequent military intervention was perhaps a silver bullet here. It not only threw a thorn in Ukraine’s side and prevented Kiev from executing a smooth political transition, but rallied Putin’s domestic base and destroyed the fringe political opposition. As scholar Andrei Illarionov argues, this is indicative of what undemocratic regimes typically do when facing such a crisis: “An undemocratic regime worried about the prospect of domestic economic, social, and political crises—such as those that now haunt Russia amid recession and falling oil prices—is likely to be pondering further acts of aggression.”

Due to the way that Russia’s domestic politics (factor 1), military capabilities (factor 2), and threat perceptions (factor 3) changed between 2004 and 2014, it is probable that the each exercised some influence on Putin’s decision-making. But how do we evaluate which of the three factors mattered most? I posit that while factors 1 and 2 can explain why Putin can use force, Hypothesis 3 explains why Putin used force at this particular time and against this particular country. It is the sufficient variable. Putin may have the ideal inner circle and a powerful military behind him, but he would not act without some powerful motivation, especially given the dramatic consequences of failure.

POLICY RECOMMENDATIONS

Several policy recommendations emerge for Ukraine, Europe, and the United States. Regarding factor 1 (domestic politics), countries should beware the negative consequences of economic sanctions that do not effectively target Putin’s inner circle. Though a handful of oligarchs have their assets frozen, Putin has already distanced himself from them politically.

34 The space limitations of this article prohibit me from elaborating further on this question. The balance among the three factors—and the influence that each has on the others—would be a valuable topic for further research.
Indeed, he has used sanctions as just another excuse to continue the process of de-offshorization and further isolate Russia from the West. This makes diplomacy more difficult.  

Second, policymakers should understand that Putin’s invasion of Ukraine is not part of his master plan to restore the Soviet Union. He is not fanatical or irrational. Rather, Putin is reacting to specific threats emanating from NATO expansion, overt US and European support for Ukrainian liberalism, and Western military overreach. Ukraine’s allies should carefully consider which activities are so essential to national security that they are worth provoking Putin. For example, three countries are currently working on a membership plan for joining NATO: Bosnia and Herzegovina, Macedonia, and Montenegro. Is it essential for these countries to join the alliance? Does US or European security increase through a formal alliance with these nations? NATO countries should not be surprised when Putin tries to undermine their ascension, even when the alliance claims to be acting only in its own defense. Russian nationalists’ failed assassination and coup in Montenegro in October 2016 is one sober indication that this effort is already underway.  

Of course, countries vulnerable to Russian aggression should be at least prepared to fend off future attacks from an increasingly capable and confident Russian military. Ukraine’s internal political disorganization and poor military preparedness in 2014 gave Putin an immediate operational advantage. Putin seized that opportunity. If Russia’s adversaries seek to deter aggression, they ought to provide military aid and training to nations that may likewise be vulnerable to Russia’s quick-strike capabilities. The Baltic countries, which have boosted defense spending and performed more joint military exercises with NATO, are a case in point. Improved combat readiness and command-and-control systems will pose a greater deterrent to Moscow and provide fewer opportunities for intervention.  

Even so, Russia can bypass these military deterrents through non-military, “grey zone” tactics that reflect the “total war” approach of Gerasimov’s military doctrine. The Kremlin has funded populist, pro-Russian political parties in several major European elections. Marine Le Pen’s National Front in France has borrowed €9 million from the First Czech-Russian Bank in 2014, and sought another €27 million loan for presidential and parliamentary campaigns in 2016. Heinz-Christian Strache’s Freedom Party in Austria signed a “cooperation agreement” with

---

Putin’s United Russia party ahead of presidential elections in 2016. Russia’s state-funded media channels like RT (formerly “Russia Today”) are emerging as alternate news sources in Britain, France, Germany, and Spain where they have local-language programming. Finally, Russian bloggers, hackers, and social media activists—many sponsored by the Kremlin itself—have taken advantage of the decentralized nature of news and social media to influence elections, most notably in the United States. These “soft-power” tactics are not overtly confrontational, but they can at least shake public confidence and perhaps challenge status-quo politicians.

Instead of thinking in simple binaries of “war” and “peace,” Putin has employed tactics that are not necessarily confrontational, obvious, or even traceable. Adversaries need to beat Putin at his own game. For example, Ukraine should invest more money in funding local media stations in Donbas to counter the Russian narrative. Long before “little green men” appeared, DJs and news anchors in eastern Ukraine were spreading “fake news” to undermine local support for the Ukrainian transitional government and the counterinsurgency forces.36 While there is no silver bullet for deterring Russian intervention, a comprehensive strategy involving diplomatic, military, economic, and technological capabilities would create fewer opportunities for intervention.

COUNTER-ARGUMENTS / ALTERNATIVE EXPLANATIONS

I do not have enough space to address all of the possible factors that influence Russian behavior toward Ukraine. This article simply addresses the three most compelling. Nevertheless, a brief note is requisite about the potential gaps in my research.

First, critics may argue that this article overestimates the success of Russian military reforms. This is a fair criticism. While Russia’s capabilities today are vastly improved compared to the immediate post-Soviet period, they still lag far behind the United States, its peer competitor. Furthermore, Western sanctions have forced Russia to cut parts of its ambitious defense budget and delayed much-needed modernization programs. In addition, Defense Minister Serdyukov—the man charged with carrying out these reforms—was discredited by a budget scandal that led to his firing in 2012 and cost the government some $1 billion rubles.37

Second, even if military reforms were successful, critics may argue that Russian special operations forces played a disproportionate role in inciting separatism in Donbas and Crimea,

36 This is a common practice of Russian unconventional tactics. Through radio and television propaganda, Russia influences local sympathies to support its own operations, long before it deploys military forces. See Janis Berzins, “Russia’s New Generation Warfare in Ukraine” (policy paper presented for National Defense Academy of Latvia, April 2014), http://www.naa.mil.lv/~media/NAA/AZPC/Publikacias/PP%202002-2014.ashx
and that this could have happened absent reforms of any kind. This criticism is less powerful than the first. While it is popular to focus on the rise of hybrid warfare, conventional forces have played and continue to play a critical role in the ongoing stalemate in Ukraine and deterring Western intervention. Indeed, Putin has the option to send the full weight of the Russian military into Ukraine—a “Plan-B” but no less threatening option. Is the West willing to test Putin’s credibility?

Third, some critics may argue that a key driver for Russian intervention in 2014 was to protect beleaguered co-ethnics. This reasoning is flawed on several counts. Yes, Kiev did exacerbate tensions with its Russian minority population through policies such as suspending government pension payments, making Ukrainian the official government language, partnering with right-wing militias, and essentially quarantining the Donbas warzone. But these all happened after war broke out in 2014. More broadly, ethnic identity plays a small mobilizing role in the Russian Federation and the former Soviet Union, and it does not justify why Russia invaded Ukraine in the first place. Furthermore, Ukrainian citizens have frequently debated their country’s future orientation: European versus Russian, West versus East. These debates were evident in both the 2004 and 2014 elections—and every election in between—with electoral maps clearly demonstrating split-orientations. Yet 2004 came and went without any calls to violence. It is more likely that some other factor instigated conflict ten years later, and that Putin cited ethnic grievances to merely justify his actions after the fact.

About the Author

Nicholas Fedyk works in the cybersecurity field. He was previously a project associate at the Berkley Center for Religion, Peace and World Affairs. He graduated from the Security Studies Program at Georgetown University in 2017, where he focused on terrorism and Russian foreign policy.

A Commitment to Peace or Just Good Enough?: Analyzing the Tuareg Uprisings in Niger (1990-2009)

Emily Gilbert

Despite their treatment as two distinct rebellions, the Nigerien Tuareg insurgencies were one phenomenon that witnessed multiple swells of violence. The Nigerien government’s initial response was an attempt at an authoritarian counter-insurgency campaign. The government, however, had neither the institutional capacity nor the means to sustain such an operation. Prolonged fighting both weakened the state’s financial resources and undermined the quality of its armed forces. The state failed equally in its initial attempts at a negotiated settlement, allowing conflict to break out once again in 2007. Ultimately, despite the feebleness in the state’s responses, the insurgency ended not due to government efforts, but due to critical weaknesses in the insurgent groups themselves.

Introduction

Niger experienced two rebellions from its Tuareg minority between 1990 and 2009. These rebellions were not discrete events, but rather upwellings of violence that persisted across decades. The Tuareg were historically marginalized in Niger and individuals had participated in individual acts of rebellion against the state. It was not until 1990, however, that organized violence centered on a collective Tuareg identity burst into reality with the first rebellion. Yet even at the height of the first insurgency, the rebellion failed to garner universal support from the Tuareg civilian population. While the Nigerien government attempted an authoritarian counterinsurgency response, it lacked both the personnel and financial means to carry such a strategy out. Ironically, the government’s first attempts at a negotiated settlement were equally haphazard. Given the weaknesses endemic to the Nigerien state, it is therefore surprising that the insurgents failed to gain more traction in their efforts. In this article, I will examine why the insurgency ultimately ended due to critical personnel and structural weaknesses in the insurgent groups.

This article has several aims. The first is to understand the origins and evolution of the insurgency and its roots causes. Second, this article will examine the government’s counterinsurgency strategy, the effectiveness and evolution of tactics used as part of that strategy between 1990-2009. Third, the article will investigate what role the insurgents themselves played in the eventual outcomes of the rebellions. Finally, the article will examine what lessons can be
drawn from this case. The Nigerien case is unique, yet the strengths and weaknesses in tactics and strategy employed by both insurgents and the government are recognizable across cases. Given the increasing threat of spillover from its neighbor to the west, Mali, it is even more necessary to examine Niger’s ability to maintain a durable peace with its Tuareg communities.

Background

On October 4, 2017, an unidentified armed group ambushed and killed four American servicemen in western Niger. While this attack came as a shock to the American public, attacks on security forces in western Niger have been on the rise as the security situation in Mali continues to deteriorate. Yet, even in the face of increasing attacks on security forces, Niger has avoided another full-blown rebellion despite Mali’s descent into chaos beginning in 2012. This is notable as the two countries experienced mirrored Tuareg uprisings between 1990 and 2009. Yet, spillover is an insidious phenomenon and many of the characteristics that undermined the Nigerien government during the rebellions, particularly corruption and neglect, remain. It is therefore critical to examine Niger’s recent history to better understand and prepare for continued instability emanating from Mali.

Tensions between the Tuareg population and the Nigerien state date back to French colonial occupation; like other colonial administrators, the French engaged in ethnic favoritism in Niger, selecting the Djerma ethnic group for administrative roles over other ethnicities, including the Tuareg, while also encouraging a Tuareg sense of superiority as a tool to maintain ethnic divisions. The Tuareg were left largely to themselves so long as they did not threaten la paix française. However, Tuareg isolation had long-lasting effects. For example, the Tuareg did not receive the same level of education as other ethnic groups, limiting their presence in pre-existing bureaucratic structures following independence in 1960. Some of this division stemmed from Tuareg cultural preferences and a general distrust of western education and political systems, but this ultimately resulted in lower participation in education. Generations of Tuareg were shut out of employment opportunities. Their limited presence in political institutions at the time of independence further decreased their political leverage relative to other groups. Policies

ostensibly aimed at modernization treated pastoralism and nomadic ways of life as obsolete and had a devastating impact on Tuareg communities around the country.\(^4\)

It is unsurprising, then, that relations between the Tuareg and the state, which was dominated by powerful ethnic groups like the Djerma and Hausa, soured over the next decade. Relations between the government in Niamey and the Tuareg communities to the north further declined following a 1976 coup attempt against then-President Seyni Kountché, in which several Tuareg officers participated. Compounding political marginalization, both real and perceived, Tuareg communities would spend the next two decades buffeted by changing environmental patterns, economic shocks, and famine. As a result, a generation came of age with most traditional forms of employment gone and their families displaced. Many young people moved to urban centers in West and North Africa, where they were met with prejudice and limited economic opportunity. For those who remained in Niger, the situation was fraught.\(^5\) When aid arrived, it was often insufficient or stolen by corrupt government officials. By the end of the 1980s, economic conditions had deteriorated in the main host countries for Tuareg migrants, such as Algeria and Libya. Economic decline and increasingly unfriendly host government policies prompted some Tuareg to begin returning to Niger.\(^6\)

This period of displacement was critical for several reasons. First it provided young and increasingly politicized young people with new international connections for organizing, and considerable military experience for those who served in Muammar Qaddafi’s army. Unemployed young men with military training returned to Niger by the tens of thousands, a situation the Nigerien state mishandled by failing to provide returnees with economic opportunities or a mechanism to reintegrate them into Nigerien life.\(^7\) A generation of Tuareg who grew up without access to traditional forms of economic opportunity came home to a country that was both unwilling and unable to provide access to the new ones.\(^8\)

There are differing accounts of the start of the Tuareg insurgency in Niger, but by 1985, armed groups formed around Tuareg grievances began conducting raids on Nigerien security forces.\(^9\) One such incident took place in May 1985, when 14 Libyan-trained Tuareg attacked

---


\(^5\) Pezard and Shurkin, 64.


\(^7\) Pezard and Shurkin, 64.


\(^9\) Minorities at Risk Project, “Chronology for Tuareg in Niger.”
government forces at Tchin Taharaden on behalf of one armed group, the Popular Front for the Liberation of Niger (FPLN), attempting to seize arms and ammunition for use in future Tuareg-led raids. Tensions escalated further in May 1990 when insurgents attacked the town of Tchintabaradene, killing 31 people. The government responded by deploying troops from the south who proceeded to detain or kill hundreds of Tuareg civilians in retaliation; this massacre served as a call to arms for the insurgents.

The country saw sporadic fighting between government forces and armed groups for the next six years, with multiple ceasefires and peace accords signed and broken. The first peace was signed in October 1994, and was followed by treaties signed with breakaway factions in April 1995, January 1997, and June 1998, although the rebellion only formally ended with the Ouagadougou Accord in 1995. The peace accord sought to enact the following: the beginning of a decentralization process; integration of former combatants into the military and government; and increased development and resources for the northern region of Agadez, an ancestral homeland for the Tuareg.

However, execution of these accords was far from completed. The government remained weak and experienced another coup d’etat in 1994. Both government forces and insurgents violated the peace accords in the intervening period. In 2004, gunmen claiming to belong to the Air and Azawak Liberation Front (FLAA) attacked vehicles and passengers in Agadez, and both June and July of that year saw attacks on convoys, including one on July 8 during which gunmen kidnapped civilian travelers and demanded the release of Rhissa Ag Boula, a former rebel leader and Minister of Tourism prior to his sudden arrest by Nigerien authorities in February 2004.

After a decade of noncompliance from both the state and insurgent groups, a second rebellion officially began in 2007. In February of that year, the Mouvement des Nigériens pour la Justice (Nigerien Movement for Justice [MNJ]) claimed a series of attacks on military and economic infrastructure; this new group had been energized by recruiting an estimated 1,000 former soldiers, many of whom had fought in the rebellion in the decade prior. Violence continued through 2007, culminating in a June attack on Agadez’s international airport—an international embarrassment to the government. When MNJ activities began threatening...

---

10 Minorities at Risk Project, “Chronology for Tuareg in Niger.”
11 Ibid.
13 Pezard and Shurkin, 65.
international economic interests, such as the 2008 kidnapping of four French Uranium workers, the international community stepped in to broker a peace deal. As the deal gained traction, MNJ rapidly splintered as multiple groups realized the benefit of negotiating as separate actors and attempted to insert their interests into the peace process. A final peace accord was signed in 2009; it continues to be enforced.

**Root Causes: Grievances and Mobilization**

Political organizing around Tuareg grievances towards the state began prior to any outbreak of violence and these same grievances were included in insurgent propaganda. Foremost were Nigerien policies that marginalized the Tuareg politically post-independence and ensured their vulnerability to economic shocks and environmental disaster in the ensuing decades. Compounding these discriminatory policies was contamination resulting from uranium mines in Tuareg homelands. Lack of political access, along with state policies aimed at increasing irrigated agriculture at the expense of nomadic livelihoods, compounded feelings of resentment in Tuareg communities. Yet, as described in the previous section, the displacement that resulted from environmental catastrophe and state neglect ultimately created the means to rebel.

**Land Use Law and State Policy**

Tension over land rights and access was a flashpoint in the decades leading up to the Tuareg rebellions. A 1992 World Bank study found that land legislation in Niger was created to protect the interests of farmers, often at an explicit cost to pastoralists. In addition, a 1961 land use law, which set a northern limit to farming, was rarely enforced by the state; as a result, herders were often forced to reimburse farmers for crop damage caused by their herds on land the herders had traditionally used. In addition, from 1980 and 1985, the state and nongovernmental organizations began massive anti-desertification projects, restoring thousands of hectares of land traditionally owned and managed by pastoralists. While an admirable goal in theory, there was little attention paid to historical land rights. As a result, land was often given to ethnic groups actively engaged in farming rather than herding, and the original land rights of the

---

Tuareg were ignored. Eventually, Tuareg pastoralists were forced to use vulnerable, marginal land, ensuring their communities were increasingly exposed to drought hazards.

**Drought**

In the 1970s and 1980s, drought eroded Tuareg communities’ resiliency, as famine and massive losses of livestock caused geographic displacement to other areas of Niger or to cities in neighboring Mali. Displacement further intensified feelings of bitterness towards the government. In Niger, the government consistently failed to provide aid or establish services for the influx of internally displaced persons, and their living conditions quickly deteriorated. Some found work as informal, and poorly paid, seasonal laborers, while many more, particularly young, unmarried men, found work as unskilled laborers in the Libyan and Algerian oil-industries. This group was particularly hard hit by economic downturns several years later. After losing their traditional cultural and economic way of life, a generation of young Tuareg was forced to grow up in exile without solid education or employment opportunities.

**Resource Extraction and Uranium**

The northern region of Agadez is home to one of the biggest uranium mines in Africa. Despite being one of the top exporters of uranium, Nigerien communities living near the mines have not benefited. Local communities consistently complained of pollution and ill health, and have seen very few local jobs created. One nongovernmental organization (NGO) found “dangerously high radioactivity levels” in soil, water, and metal scrap close to two mining sites. More importantly, workers at the Areva mine claimed they were not provided with basic protection or warned about the health risks of uranium mining.

Unsurprisingly, grievances around resource extraction and pollution became a rallying point for local communities since the beginning of uranium mining in Niger, and between 1990 and 2009, insurgents regularly attempted to capitalize on the mines’ visibility. Insurgent leader Boubacar Alambo, for example, publicly asserted that the uranium industry hurt Tuareg

---

20 Krings, “Marginalisation and Revolt Among the Tuareg in Mali and Niger,” 58.
22 Minorities at Risk Project, “Chronology for Tuareg in Niger.”
communities and made a nomadic lifestyle impossible,
and insurgents were consistent in demanding an end to what they framed as exploitation of Tuareg territory.

Political Access

The French colonial administration encouraged competition between ethnic groups, creating a zero-sum environment with regards to political power. The Tuaregs believed they had been given the short end of every conceivable stick; the Djerma received the best government positions, and discriminatory land use policies favored groups like the Hausa over pastoralists. Even within the Tuareg clan structure itself, former castes that had historically served as slaves or laborers were being given land and economic opportunity. These efforts upended traditional social structures and strained community resiliency.

Although insurgents at first called for increased autonomy for Tuaregs, their demands eventually centered on these four major grievances: restricted land use, geographic isolation resulting in vulnerability to environmental disaster such as drought, the harmful effects of extractive industries, and lack of political access. While a decade has passed between rebellions, when new insurgent groups emerged in 2007 their demands were remarkably consistent with those of 1991.

Assessing the Government’s Response

The Nigerien state pursued a mostly authoritarian strategy against the Tuareg uprisings in 1991 to 1995 and 2007 to 2009, one that punished not only the insurgents, but the civilian population as well. This strategy was evidenced in three ways: 1) security forces were consistently deployed to control Tuareg civilian centers with limited oversight; 2) state authorities publicly refused to negotiate with the insurgents or (initially) address legitimate community grievances; and 3) the government limited access to and from Agadez and instituted a strict media blackout. According to the Central Intelligence Agency’s (CIA) “Guide to the Analysis of Insurgency,” an authoritarian strategy “seeks to punish not only the insurgents but also the population that supports them.” In the state’s efforts to take the fight to the insurgents, security forces used

---

30 Krings, “Marginalisation and Revolt Among the Tuareg in Mali and Niger,” 59.
excessive force, ignored human rights, and directly targeted the civilian population. While these characteristics of government response were present throughout the conflict, the government’s willingness and ability to conduct a cohesive strategy tapered over the course of the first rebellion. The Nigerien government was forced to modify its strategy and tactics overtime, in part due to an entrenched military stalemate. Years of conflict had put considerable strain on both state finances and force capability, and there were multiple mutinies in the army over unpaid salaries. Financially drained and facing international pressure, the government saw no choice but to negotiate.

An Attempt at Authoritarianism

Although Nigerien authorities did eventually come to the negotiating table in 1993—instigated by the country’s first elections since 1960—the state response in the early 1990s highlights the pitfalls of a strictly authoritarian COIN response for impoverished countries. An authoritarian approach requires both a willingness to ignore international opinion and the military means to carry it out. Over the course of numerous clashes with rebels, however, the Nigerien security forces (Forces Armées Nigeriennes [FAN]) struggled to successfully engage insurgents. Frustrated and undisciplined soldiers were often responsible for incidents of violence against civilians as they were increasingly exposed to insurgent violence.

However, the Nigerien government’s reflexive authoritarian response preceded the official outbreak of rebellion; the Nigerien state ordered a major military operation at the first sign of unrest amongst the Tuareg population in May 1990, and when protests broke out in Tchin Tabaraden, following an insurgent attack, the government responded by ordering inexperienced troops north to Tchin Tabaraden to stabilize the situation. Instead, FAN troops rounded up and executed approximately 400 Tuareg. When the executions became public knowledge, the government quickly arranged sham criminal proceedings. While some military officers were detained during the so-called trial, they were subsequently released. By 1992, Niger decreed “a

35 Westerfield, Decentralisation, Counterinsurgency and Conflict Recurrence, 26.
37 For example, in 2007, the FAN was accused of attacking a Tuareg settlement at Tamazelak after they were overpowered by MNJ insurgent forces. See: Keenan, “Uranium Goes Critical in Niger,” 454.
38 Krings, “Marginalisation and Revolt Among the Tuareg in Mali and Niger,” 59.
security precaution zone” in Tuareg territory, stating that increasing insecurity required broad authority for use of force by military forces in the region.39

The events at Tchin Tabaraden were not the only reports of human rights abuses by armed forces with minimal oversight from the government. Between 1992 and 1994, there were numerous accusations of government forces engaging in excessive violence against both suspected rebels and civilians.40 In August 1992, security forces captured some 180 alleged Tuareg insurgents in a series of raids in Agadez, but an unknown number were never accounted for and are assumed to have been killed extrajudicially.41 Government forces were also regularly accused of human rights violations when conducting interrogations. This record of extrajudicial killings and illegal detentions followed the government into the 2000s, even in periods of relative calm. For example, in 2004, President Mamadou Tandja was accused of attempting to provoke Tuareg communities in order to capitalize on material support from the “Global War on Terror” after he arrested Rhissa ag Boula, then a member of government and formerly the leader of the FLAA.42 Rhissa ag Boula was released without charge after 13 months, but not before violence once again flared up in the Air region.43

To obfuscate the reality on the ground, the government instituted a media blackout in Agadez and actively threatened both Nigerien and international journalists attempting to report on the conflict with arrest, going so far as to expel several media outlets, including Radio France International. In August 2004, the government arrested Moussa Kaka, who managed a radio station and served as a correspondent for RFI. Kaka was charged with conspiracy following his reporting on the resurgence of the Tuareg rebellion in June.44 The blackout and arrests complicated efforts to get accurate numbers on combatant and noncombatant casualties, giving the government some cover in its operations in contested areas.45

The third prong of the government’s COIN strategy was psychological warfare. This was partly achieved through collective punishment, but could also be seen in government efforts to play up divisions between the Tuareg civilian population and the insurgents. By December 1991, the government publicly rejected the existence of any Tuareg political movement, and began referring to insurgents as criminals and bandits;46 President Tandja often described insurgents as bandits and drug traffickers, increasing the public focus on the role of insurgent leaders in

39 Westerfield, Decentralisation, Counterinsurgency and Conflict Recurrence, 26.
43 Ibid.
46 Minorities at Risk Project, “Chronology for Tuareg in Niger.”
criminal enterprise.  

This was not far from the truth: Boubacar Alembo, one of the primary leaders in the 2007 attack on Iferouane, had a known criminal history as a smuggler. Alembo was talked of as unstable and as having brought “shame” on his people. Tuareg elders are accused of having attempted to assassinate him with the government’s blessing in 2003.  

Weaknesses in Strategy and Tactics

Undermining the government’s ability to efficiently enact its authoritarian COIN strategy were persistent issues with the quality and caliber of Nigerien troops. Inexperienced troops were regularly accused of excessive violence against civilians, and multiple mutinies limited the government’s ability to protect the civilian population and target the insurgents. One such incident occurred in August of 1992, when, under the orders of an unofficial paramilitary command stationed in Agadez, troops raided Agadez, Arlit, and Tchirozerine. During the raids, they arrested several people who were allegedly members or sympathizers of the FLAA. The central government appeared to be caught unprepared and was unable to intervene. One month later, soldiers stationed in Agadez rioted, threatening to execute 110 Tuareg civilians if the rebels failed to free 40 police and army hostages within 48 hours.  

This served to galvanize the insurgents, who saw proof of government weakness, as well as the impunity with which security forces behaved.

The Nigerien government’s COIN strategy slowly evolved over the almost two decades it fought the insurgency. In the early 1990s, the government attempted a strictly authoritarian response to the rebellions using a state of emergency that involved extrajudicial punishment, human rights abuses against civilians, and a media blackout. The government’s public attitude towards the insurgency began to change in 1993, following the country’s first free and fair elections since 1960. The new government made a concerted effort to achieve peace through negotiations, but infighting and weak institutions ultimately undermined a coherent strategy. The government’s inability to enact reforms directly contributed to the ongoing crisis; armed groups renewed attacks on both civilians and security forces following government inaction despite a robust peace agreement signed in 1995. After several more years of stalled agreement implementation, rebellion reoccurred in 2007.

49 Minorities at Risk Project, “Chronology for Tuareg in Niger.”
Assessing the Insurgency

Despite this apparent momentum, the rebels were consistently unable to sustain the pace and scope of their operations outside the Air Mountains to the far north between 2007 and 2009.\textsuperscript{50} This begs the question: given the weaknesses of the central government and the brutality and ineffectiveness of state security forces, why did the insurgency fail in 2009? In the following section, I will argue that the insurgents suffered from structural weaknesses resulting from factionalization, which precluded unification, as well as illegitimacy with the very civilian population they were alleged to represent.

\textit{Factionalization}

Tuareg culture is rigidly hierarchical, with entrenched divisions along clan lines. Early Tuareg revolutionaries in the 1970s and 1980s attempted to abolish these divisions under a larger nationalistic umbrella, but traditional Tuareg leaders, as well as communities themselves, resisted these changes.\textsuperscript{51} Mali and Niger witnessed independent Tuareg nationalist separatist movements, but in both cases the movements split along clan affiliation lines soon after beginning.\textsuperscript{52} Another example of the strength of clan loyalties is the failure of Tuareg groups in Algeria and Libya, the Kel Hoggar and Kel Ajjer respectively, to join the rebellions following repeated recruitment attempts by early Tuareg revolutionaries.\textsuperscript{53} Clan divisions remained a potent force.

Tuareg insurgent groups again fell victim to factionalization in the 1990s and in 2007. The Air and Azawak Liberation Front (\textit{Front de Liberation de l’Aïr et de l’Azawak [FLAA]}) officially led the early insurgent rebellion in Niger, but there were as many as three proto-insurgent groups jockeying for leadership roles.\textsuperscript{54} Pre-existing divisions meant the FLAA quickly fractured into smaller armed groups.\textsuperscript{55} The goal of these groups for more autonomy in the northern regions of Niger also fostered disunity as it raised the inherent question of which Tuareg clans would hold positions of power in this new political government.

The structure of the peace negotiations further incentivized fractionalization. During the talks, each organized group was entitled to access to post-conflict benefits as a peace negotiator.\textsuperscript{56} Rebel leaders were offered positions within the government as part of the agreement. For

\begin{flushright}
\textsuperscript{50} Emerson, “Desert Insurgency,” 676.
\textsuperscript{51} Lecocq, “Unemployed intellectuals in the Sahara,” 107.
\textsuperscript{52} \textit{Ibid}, 104.
\textsuperscript{53} \textit{Ibid}, 106.
\textsuperscript{55} Pezard and Shurkin, 65.
\textsuperscript{56} Guichaoua, “Circumstantial Alliances and Loose Loyalties in Rebellion Making,” 10-12.
\end{flushright}
example, Mohamed Anacko, for example, was made the High Commissioner for the Restoration of Peace [Haut Commissaire à la Restauration de la Paix], and Rhissa ag Boula was offered the position of Minister of Tourism, a prestigious role as tourism was a significant income-generator in Agadez and an industry traditionally controlled by the Tuaregs. These promised benefits led to the 1994 formation of a new group, the Coordination de la Résistance Armée (CRA). A formal agreement was finally reached in April 1995, but, not all armed groups participated in its negotiation; it was not until 1997 that the last armed group joined the peace process.

The 2007 attack on Iferouane, which launched the second rebellion, should be viewed as a continuation of this factionalization. Insurgent leaders Amoumoune Kalakoua and Boubacar Alambo were former combatants who had fought with the FLAA. Critically, neither benefited from the 1995 peace accord integration efforts that had promised political access and job opportunities. Furthermore, both Kalakoua and Alambo had earned reputations as smugglers and bandits in the period between 1997-2007.

Interpersonal conflict, competing objectives, and petty disagreements caused a rift in the insurgency in early 2009, resulting in a landscape similar to that surrounding the 1990s peace talks. Commanders within MNJ, the primary insurgent group broke with leadership and announced the formation of the Nigerien Patriotic Front [Front Patriotique Nigerien or (FPN)] in March. At the same time, then-President Mamadou Tandja caved to international pressure to begin negotiations with the insurgents. This convergence of rebel group splintering and negotiations incentivized insurgents to form even more groups to negotiate with the government, lest they lose out on the benefits of the peace process.

Lack of Legitimacy with Target Communities

In addition to entrenched internal divisions, there are numerous characteristics unique the Nigerien Tuareg community that made it more resilient to continued insurgency. First, traditional Tuareg leadership did not embrace the insurgency. Second, the insurgency itself did not convince the Tuareg population that it should be supported. Finally, Niger’s Tuareg population has historically been dispersed and integrated into Nigerien society.

When Niger gained independence, traditional chiefs, including Tuareg traditional leaders, dominated the primary political party, the Nigerien Progressive Party. Critically, despite a coup d’état in 1974, the traditional power structure remained intact within Niger post-

58 Westerfield, Decentralisation, Counterinsurgency and Conflict Recurrence, 24.
60 Lecocq, “Unemployed intellectuals in the Sahara,” 106.
independence, and elites had no immediate qualms with Niger’s new political system.\textsuperscript{61} The second point of contention between insurgents and traditional leaders was the hierarchical organization of Tuareg communities, with tribal chiefs holding the most powerful positions. Criminal upstarts who threatened to upend a functioning political system and way of life were anathema to most Tuareg communities to the extent that traditional leaders are thought to have ordered an assassination attempt on rebel leader Boubacar Alambo at some point between 2003 and 2004.\textsuperscript{62} The enmity between traditional leaders and insurgents was not one-sided. Many traditional leaders spoke out against the rebellion and multiple village chiefs were assassinated during the uprisings.\textsuperscript{63}

In addition to resistance from traditional leaders, the communities themselves had no stomach for another rebellion after the uprising in the 1990s. Following devastating drought and famine in the 1980s, communities saw no benefit from a rebellion allegedly in their name. Abused by both insurgents and the military, popular support for the uprisings remained low relative to the total Tuareg population.\textsuperscript{64} More critically, and much like the military, insurgents often targeted civilian communities; in February 1993, insurgents were identified as responsible for multiple attacks on villages that killed 30 civilians.\textsuperscript{65} In addition, insurgent leaders were not respected members of their communities, and Tuareg civilians (not unjustifiably) accused the rebel elite of being out for personal gain to the detriment of the common people.\textsuperscript{66} Leaders like Amoumoune Kalakoua and Boubacar Alambo were considered criminals and shamed individuals. Both of these factors undercut insurgent legitimacy among the population.

Finally, the demographic makeup of Niger provided some resiliency against the insurgency. While Agadez is the ancestral homeland of many Tuaregs, the Tuareg ethnic group is not a monolith and is dispersed across Niger. In addition, Tuaregs played an important role in Niger’s culture and history predating independence. While the Tuaregs had legitimate grievance with regard to political access and economic opportunity, they have also held positions in the military and government since independence. In addition, the Agadez region is accessible to the rest of the country, which has kept the flow of goods and ideas open between different communities and ethnic groups.\textsuperscript{67}

\textsuperscript{61} Lecocq, “Unemployed intellectuals in the Sahara,” 106.
\textsuperscript{63} Minorities at Risk Project, “Chronology for Tuareg in Niger.”
\textsuperscript{64} Frédéric Deycard, “Le Niger entre deux feux. La nouvelle rebellion touarègue face à Niamey,” Politique Africaine 108 (2011): 127-144.
\textsuperscript{65} Ibid.
\textsuperscript{66} Lecocq, “Unemployed intellectuals in the Sahara,” 107.
\textsuperscript{67} Pezard and Shurkin, 68.
A combination of critical shortcomings in the insurgency and Niger’s demographic characteristics demonstrate that the government should have been able to tackle the rebellion. There were clearly serious flaws in the government’s COIN strategy and tactics, and peace was only sustained when the government adhered to and implemented the terms of the negotiated peace settlement.

Lessons from Niger’s Experience

The preceding passages lay out a complex but common case study involving a weak post-colonial state, an aggrieved community suffering from state neglect and catastrophic environmental changes, and a largely unsuccessful insurgency that failed to win the support of the people it claimed to represent. Yet the insurgency lasted for years, signifying that the failed strategies of the state could serve as useful lessons for those studying counterinsurgency.

Niger’s original attempts at an authoritarian crackdown provided mixed results. The state was largely successfully at limiting both media penetration in Agadez and reporting on the insurgency more generally. This allowed the government to maintain a modicum of control over the conflict’s narrative and avoid international scrutiny. The state was far less successful in its military efforts, and its crackdown alienated local communities and overstretched its military’s capacity, leading to mutinies and lack of discipline. In addition, repeated military losses undermined troop morale and government legitimacy and served to embolden insurgents.

While it is not clear that the government’s attempts at psychological warfare—particularly in referring to insurgents as “criminals” or “bandits”—was effective, the tactic showed that the government recognized potential avenues via which to undermine the insurgents’ relationships with local communities. This narrative also served to give the government cover in refusing to recognize the legitimate political objectives of the armed groups and in negotiating.

While many counterinsurgency lessons can be taken from the Nigerien case, it is ultimately a unique one. Mali, its western neighbor, home to a similar marginalized and aggrieved Tuareg population, has had an entirely different outcome in the decade since the second rebellion. The Nigerien counterinsurgency was somewhat effective at best and completely ineffective if not actively harmful at its worst. What is critical about the Niger case, though, is the government’s recognition of the opportunity they had in 2009 to capitalize on the new peace agreement and institute critical and robust reform, hopefully preventing future insurgencies.
Mali and Niger

Since the end of hostilities in 2009, Niger largely avoided the chaos battering Mali, its neighbor to the west. The variance in the outcomes of these two states is significant as both experienced uprisings from their Tuareg minority in through the mid 1990s and mid 2000s.\(^\text{68}\) This is partly due to a stronger determination to keep the peace, but also to key structural differences between Mali and Niger.

The demographic makeup of Niger provided some resiliency against the insurgency. While Agadez is the ancestral homeland for many Tuaregs, Tuaregs are dispersed across Niger and have played an important role in Niger’s culture and history predating independence.\(^\text{69}\) This is not the case in Mali, where the Tuareg remain concentrated to northern territories. In addition, the Agadez region is accessible to the rest of the country, keeping the flow of goods and ideas open between different communities and ethnic groups.\(^\text{70}\) Thus, while the Tuaregs had legitimate grievance with regard to political access and economic opportunity, there is a more established working relationship between the state and the Tuareg community than there is in Mali.

In the cases of Mali and Niger, weak state institutions and political instability limited cohesive state action and strategy. However, since 2009, Niger has succeeded in meeting many of its obligations set forth in the last peace settlement; Mali has consistently failed to do so to its own detriment. In 2010, newly elected President Mahamadou Issoufou made a series of calculated decisions that appear to have reaped dividends. He chose Brigi Rafini, a Tuareg, for prime minister, and gave multiple posts within the government to former rebels, cementing efforts to integrate aggrieved Tuaregs into the political system.\(^\text{71}\) In addition, the government established the High Authority for Peacebuilding (HACP), which has been given a mandate to monitor political tensions through an “early warning system.” Most importantly, the HACP remains a legitimate body in the eyes of the public, with the authority and means to make good on its founding principles.\(^\text{72}\)

Conclusion

Despite often being treated as two separate rebellions, the Nigerien Tuareg insurgencies were one phenomenon that witnessed multiple swells of violence. Not only did organized


\(^{70}\) Pezard and Shurkin, 68.

\(^{71}\) Guichaoua, “Crise au Sahel.”

\(^{72}\) *Ibid.*
violence around Tuareg grievances began prior to the official start of the insurgency, but violence continued even during peaceful years. In addition to consistent violence around an organized Tuareg struggle, the publicly given root causes remained the same across both periods in the insurgency. The government originally tried to implement a fully authoritarian response, but it had neither the institutional capacity nor the means to sustain such an operation. Prolonged fighting both weakened the state’s financial health and undermined the quality of its armed forces. Eventually, domestic political changes and conflict fatigue brought insurgents and the government to the negotiating table. While the government struggled to maintain a fully authoritarian approach, it successfully implemented narrow parts of its counterinsurgency strategy. Ultimately, however, the insurgency ended not due to government efforts, but rather weaknesses in the insurgent groups themselves.

*About the Author*

*Emily Gilbert is a master’s degree candidate at Georgetown University’s Security Studies Program (SSP).*
The Role of the Security Services in Russian Foreign Adventurism and Its Consequences for US Policy

Nicholas McCarty

Russian intelligence services have garnered a great deal of press attention in the last year over cyber warfare, hacking, and their influence on Western democracy. Missing from this conversation (in the West at least) is the influence of the security services on Russia itself. As Vladimir Putin and Russia have become increasingly isolated from the international community, Russia’s foreign policy has become dominated by the so-called siloviki, ex-security service members who hope to steer the state toward their interests. Greater awareness of the history and role of the state security services in Russian society is needed if US policymakers are to respond correctly to future crises.

Much ink has been spilled in recent years over the conduct of Russian foreign policy under Vladimir Putin. For many, Russia’s newfound adventurism reflects the culmination of realist thought as Russia seeks security in the face of perceived NATO encirclement. While Putin himself likely welcomes these attributions of realist genius, solely considering national interests fails to adequately explain Russian adventurism abroad. While security and power seeking plays a role in renewed Russian interest in its near abroad, realpolitik fails to consider the personal interests of the Russian ruling class, the siloviki (derived from the Russian word sila, meaning power, to refer to those currently or formerly associated with the Soviet and Russian security services). By examining the interests of Putin and the siloviki, one can better explain Russian concerns over popular revolt (as seen in the color revolutions in other post-Soviet states) or intervention in Ukraine, as well as make predictions for the future.

Emerging from the chaos of the fall of the Soviet Union and the 1990s, Putin offered Russians what they dearly needed at the time: stability and basic competence. Putin himself made that clear in his first address to the Russian Federal Council in 2000, asserting that “patient work” would be needed to right the ship of state. The First Chechen War embarrassed and demoralized Russian society, while the 1998 sovereign debt default and subsequent financial crisis derailed an already struggling economy. The country’s leadership offered little solace.

---


Russian president Boris Yeltsin, a prime mover behind the fall of the Soviet Union, was proving useless in managing affairs of state. Beyond his mismanagement of the economy and the war, he was widely viewed as a drunk who had sold out the country to Western reforms and handouts. Shortly after leaving office, Yeltsin’s approval rating was as low as 14% and is barely better fifteen years later at 18%. It is not hard to imagine that the Russian public would be looking for somebody, anybody, to steady society.

The security services have long had an influence over the Soviet and Russian governments. Names like Felix Dzerzhinskii, Nikolai Yezhov, and Lavrentii Beria cast a dark shadow over the Gorbachev and Yeltsin governments, reminding them of the chaos of the past. But that fear often proved counterproductive for intelligence chiefs as Party officials sought to mitigate the coercive power of the security services. In fact, the sole intelligence officer to attain ultimate power in the Soviet Union was the KGB titan Yuri Andropov. Though he ruled the USSR for only fifteen months, Andropov ran the KGB for fifteen years and left his mark on the service. A survivor of the 1956 Hungarian uprising against Soviet rule, he was a dedicated servant of the Soviet state and career advocate for the KGB. Throughout Andropov’s time as the head of the KGB, he cultivated the image of the security service in Soviet society as the last of the uncorrupted—the only remaining men and women willing to put the interests of the state above all else. He deliberately recruited the best and brightest from Soviet universities, offering them access to power even while imprisoning thousands and locking up dissidents in psychiatric hospitals. That in the 1980s the recruitment of the “best and brightest” had degenerated into little more than the nepotistic hiring of the scions of Soviet elite mattered little as the idea permeated Soviet society and more importantly the KGB itself.

Yet Andropov also favored economic liberalization. He understood that the Soviet Union’s economy was overly reliant on oil and natural gas, and that diversification was desperately needed. During his short period in office managed to endorse market reforms that would be built upon during the Perestroika era. Indeed, Gorbachev’s rise to premiership would

---

8 Galleoti, “Yuri Andropov Would Drop Assad Like a Hot Kartoshka.”
have been impossible without Andropov’s support for him and his liberal reformers in the Politburo. Andropov’s idea of the ideal KGB man (and ruler) lived on in many security service members’ hearts: strong, opportunistic, ruthless, and dedicated to the state’s advancement.

But just like the rest of Russian society, the security services (successors to the Soviet KGB) were crippled by the fall of the Soviet Union and the chaos of the 1990s. After the failed coup by Soviet hardliners (including KGB chief Kryuchkov), newly independent Russia dissolved the KGB, fearing the dreadful consolidation of power that had marked Soviet rule. Thousands were laid off, while those that remained in intelligence found themselves split and forced to fight among themselves for scant resources. Instead of one KGB, there was now the Foreign Intelligence Service (SVR), responsible for covert collection abroad, while communications intel to the Federal Agency for Government Communications and Information (FAPSI). The border guards were spun off as well, along with the equivalent of the Russian secret service. This left domestic intelligence to an entity now known as the FSB (originally the FSK), but even they were weak and forced to fight with the interior ministry and tax police for attention. Split and devoid of funding, the security services were left adrift in the chaos of Russia in the 1990s. Failure stalked the security services everywhere it went. Multiple failures in efforts to combat Russian organized crime and Chechen separatists rocked the agencies, all while they continued to fight among themselves.

Yet despite the struggles of the institutions themselves, individual members of the security services were able to adapt remarkably well to the new realities of capitalism in Russia. Few became oligarchs themselves, but for those who possessed the right ambition matched with skills could carve out a niche. In the “Wild East” of Russian capitalism in the 1990s, any advantage over a competitor could and would be used. Many were able to use their old connections in the intelligence world to tap phone lines or trail opponents, gaining compromising (or worse) material and becoming rich offering intelligence capabilities to the highest bidder. Using traditional Russian (and former Soviet) patron-client relationships, many

---

9 Whitmore, “Andropov’s Ghost.”
10 Soldatov and Borogan, The New Nobility: The Restoration of Russia’s Security State and the Enduring Legacy of the KGB, 12.
11 In Russian: Sluzhba Vneshnei Razvedki, SVR and Federal’noye Agenstvo Pravitel’stvennoi Svyazi i Informatsii, FAPSI. FSB stands for Federal Security Service (Federal’noye Sluzhba Bezopasnosti.
12 Soldatov and Borogan, The New Nobility: The Restoration of Russia’s Security State and the Enduring Legacy of the KGB, 12.
became extravagantly wealthy shielding allies from corruption while shaking down enemies.\textsuperscript{15} But few \textit{siloviki} became businessmen themselves, being relegated to the “second and third tiers of the new business structures,” supporting the oligarchs.\textsuperscript{16}

The dream that was Andropov however persevered. Why couldn’t the security service run things, reasoned some. Russia needed a steady hand, after all.\textsuperscript{17} It was from this chaos that Vladimir Putin emerged. A former KGB Lieutenant-Colonel, he was the first, or at least most successful, of the \textit{siloviki} to turn to politics. Putin first attracted attention as the mayor of Saint Petersburg, before serving as Yeltsin’s FSB chief and eventual prime minister. A believer in capitalism and fiercely loyal to his supporters, Putin was blessed with connections and the right bit of luck. When he was appointed head of the FSB and then Prime Minister, he offered the security services a new path to power. With Putin at the helm (Yeltsin continued to decline in influence), the security services stabilized and Putin’s influence grew. Russian business was forced to recognize the power of the state. Ex-KGB men like Igor Sechin became the head of Rosneft (Russia’s state oil company) while shuffling the old guard out of power.\textsuperscript{18} Selective state prosecution empowered Putin and his allies, wielding the power to pursue corruption charges against enemies like a cudgel against those who would oppose him.\textsuperscript{19} The \textit{siloviki} solidified themselves as a clan through the exploitation of the highest Russian offices, each looking out for another in covering up their corruption.\textsuperscript{20} As Russians at the time said, “the distinguishing feature of Boris Yeltsin’s rule was that businesses were shaken down by bandits, whereas under Putin, they were shaken down by the \textit{siloviki}.”\textsuperscript{21}

Unlike other Russian oligarchs, the \textit{siloviki} preferred not to advertise their wealth, preferring the appearance of austerity Andropov taught them. As Putin solidified his hold on the presidency, he continued these practices on a grander scale, transforming the nation into a kleptocracy. Headed by the Saint Petersburg clan in particular (the city where Putin and his main allies hailed from), men such as FSB chief Aleksandr Bortnikov, Security Council Secretary


\textsuperscript{18} \textit{Ibid}, 33.

\textsuperscript{19} For a prime example, see the trial of Mikhail Khodorkovsky in 2003, then the wealthiest man in Russia.


Nikolai Patrushev, and former SVR chief Mikhail Fredkov now not only dominate the “power”
security services, but make up some of the richest men in Russia.\textsuperscript{22}

Putin and his security chiefs have been ruthless in consolidating power. In exchange,
Putin and the security elites have been generous to the men and women who keep them there.
As mentioned, the Soviet Union’s KGB fell with the empire, its directorates scattered into a
variety of federal agencies or simply dissolved altogether. Putin reversed this trend, allowing the
FSB to reabsorb the border guards, signals intelligence, and drug enforcement while setting up
parallel foreign intelligence operations separate from the SVR or military intelligence.\textsuperscript{23} This is
not to say inter-agency competition doesn’t still exist, but that the consolidation of agencies has
allowed for a common operational vision across the agencies that has resulted in increased
popular support.\textsuperscript{24}

Now comfortably at the top of Russian society and loyal to Putin for their newfound
wealth, positions, and power, the siloviki have adapted Andropov’s lessons to the new reality of
Russian life. Fulfilling the promise of a return to stability (albeit through the use of often
heavy-handed controls), they nevertheless remained obsessed with holding on to the fruits of
their corruption. As Soldatov and Borogan describe it:

“They are not, it should be said, a junta united by common perspectives on
Russia’s present and future. Their motives are much more personal…[They] have
quickly moved to pursue their private interests.”\textsuperscript{25}

These “private interests” can be boiled down to one phrase: regime preservation.
Meanwhile, the costs of these policies are passed on to the rest of Russian society.\textsuperscript{26} The interest
of staying in power and ensuring kleptocratic access to wealth represents a parallel national
interest to Russia’s ruling class.

The results of those post-Soviet leaders who failed in this task provide a stark warning for
the siloviki. Color revolutions in Georgia (2003), Ukraine (2004), and Kyrgyzstan (2005) forced
corrupt leaders to flee to Russia, devoid of their wealth and power.\textsuperscript{27} For the Russian siloviki,

\begin{itemize}
  \item \textsuperscript{22} Orlova, “Who Would Dethrone the Tsar?”
  \item \textsuperscript{23} Soldatov and Borogan, The New Nobility: The Restoration of Russia’s Security State and the Enduring Legacy of the KGB, 28.
  \item \textsuperscript{25} Soldatov and Borogan, “Russia’s New Nobility: The Rise of the Security Services in Putin’s Kremlin.”
  \item \textsuperscript{27} Color revolution refers to the pattern of mostly nonviolent popular movements that ousted numerous post-Soviet
governments in the 2000s (along with the events of Maidan in 2014 in Kyiv). “Color” refers to the revolutionary
\end{itemize}
there is nowhere to flee. Putin recognizes this, stating publicly that, “For us this is a lesson and a warning. We should do everything necessary so that nothing similar ever happens in Russia.”

Faced with the prospect of a possible revolution at home and surrounded by (perceived) existential threats abroad, Putin has no choice but to wield Russian foreign policy as a weapon against democracy and the West—a bastion of encroaching liberalism.

That said, the interests of the siloviki remain a parallel driver in Russian politics, working both in tandem with and influencing Russian security policy. After all, the siloviki were, and in some cases remain, security officers. To be a silovik meant internalizing the state interests as the sole prime directive in public policy. As Michael Kofman correctly notes, the use (or threat) of military force to further state policy was a favorite tool in Soviet times as well as the Yeltsin years. The first so-called “frozen conflicts” were set up by Yeltsin in Transnistria and Abkhazia, while the 2008 Georgian War blazed under the non-silovik Dmitry Medvedev. These wars (and the many diplomatic actions in between) reflect traditional Russian security-seeking behavior, meant to guarantee Russian interests and prevent a perceived NATO encirclement. The difference is that now regime survival has become inextricably tied to Russian security interests.

The greatest example of this marriage between siloviki interests merging with Russian national interests remains the ongoing Russian intervention in Ukraine. For Russia, the loss of Ukraine to the Western European sphere of influence and NATO represents a seemingly existential military threat, appealing to long-held Russian fears of encirclement. To Putin and the siloviki, the popular revolt (culminating in the Maidan revolution) against the kleptocratic regime of Ukrainian President Viktor Yanukovych presented the most dangerous threat to his regime. Secure in their ability to rig popular elections, the siloviki recognize their greatest risk stems from popular revolution. For years, Russia had accused US Intelligence agencies (and US Ambassador to Russia Michael McFaul) of supporting the Russian opposition and encouraging regime change. Throughout the Ukraine crisis, rumors abounded in the Russian media that the United


States was behind the demonstrations, as well as the funding and organizing of the opposition as a trial run for revolution against Putin.

Within this context, Ukraine’s 2014 Maidan revolution and Yanukovych’s ouster represented a turning point in Russian foreign policy, with the threat to siloviki interests adding to the strategic threat. If Ukraine could escape the kleptocratic orbit, then in Putin’s eyes the United States would use the same playbook in Moscow. To protect his rule, Putin launched an operation intended both as a “pre-emptive strike against the idea of a Russian Maidan,” and as a move to prevent other Russian border areas from escaping Moscow’s influence.32

The Russian capture and annexation of the Crimea in 2014 coupled with the continued support of rebels in the Donbas must, therefore, be seen as vital to both Russian security interests and regime survival. The failure of the Ukrainian army to resist the annexation or to break the “frozen conflict” in the Donbas has effectively ended Ukraine’s ability join NATO or the EU.33 Meanwhile, Russian media continues to highlight the chaos in Ukrainian civil society.34 These persistent and highly visible failures (in Putin’s view) serve to discredit the idea of western democracy in both Ukraine and Russia. Through this Putin hopes to imbue in Russian society the inherent dangers and chaos of liberal democracy.

Vladimir Putin’s pattern of action as described in the Ukrainian case study is unlikely to stop. The interest of the siloviki and Russia go hand in hand and even complement each other. Russia’s support for the Assad regime in Syria reflects similar currents to the intervention in Ukraine, in which propaganda sources have succeeded in painting revolutionary figures as destabilizing while standing up for Russian strategic interests in the Middle East.35 In Putin’s eyes, Syrian President Bashar Al-Assad represents another potential victim to Western subversion. Russian Defense Minister Sergei Shoigu revealed as much when he described the intervention in Syria: “The deployment of our group in the Syrian Arab Republic helped solve the geopolitical task of breaking the chain of ‘color revolutions.’”36 To that end, Russian airstrikes prioritized Western-backed insurgents rather than the more radical ISIS because they

represented the real threat to Russian interests.\textsuperscript{37} For Putin and the \textit{siloviki}, regime preservation at home now means proactive intervention abroad.

Meanwhile, successful demonstration of Russian arms technology has driven demand for weapons exports and further enriched the Russian state.\textsuperscript{38} The ongoing Russian interference efforts in Western democracy reflect similar efforts to undermine the concept of democracy in Russian eyes.\textsuperscript{39} These are deliberate policies aimed not at the promotion of Russian state interests but instead the interests of \textit{siloviki} power. Going forward, US policymakers must take this into account when pursuing policies affecting Russia and adjust accordingly.

The United States’ inability to decouple the rest of Russian society from the \textit{siloviki} belies the power of the security services within the Kremlin. US-led anti-kleptocracy efforts such as the Global Magnitsky Act, along with punitive sanctions against Putin’s inner circle (men like Sechin, Bortnikov, Fredkov, and Petrushev) have largely failed to alter Russia’s foreign policy. Russia’s military and business community continue to stand united with the security services, despite even nationwide sanctions and countersanctions implemented by Russia, the European Union, and the United States.\textsuperscript{40} Russians allow the status quo to continue because they believe that, overall, their interests are represented by leaving the \textit{siloviki} in charge, even with all their corruption. The upsurge in national pride and confidence in continued stability that has accompanied the Crimean annexation has so far offset the economic damage inflicted by Western sanctions. But the intertwining of foreign policy successes with regime legitimacy has opened up a dangerous Pandora’s box for Putin and his regime.

In the past eighteen years of Putin’s rule (be it directly or indirectly), it has become impossible to separate Russian strategic interests from the interests of the \textit{siloviki}. The question then becomes, if the Russian \textit{siloviki} are operating according to a generally realist model, why does it matter that it is the corrupt ex-security service members that run it? The answer is key to understanding why US strategists have consistently been surprised and outwitted by their Russian counterparts. For many other countries, geopolitical events may threaten relative standing in world power, but not the survival of the ruling regime. For example, flashpoints in the South China Sea might pose long-term strategic problems for the United States and China,

\begin{itemize}
\item \textsuperscript{37} ‘More than 90%’ of Russian airstrikes in Syria have not targeted Isis, US says,” \textit{The Guardian}, October 7, 2015, \url{https://www.theguardian.com/world/2015/oct/07/russia-airstrikes-syria-not-targetting-isis}.
\item \textsuperscript{38} Richard Connolly and Cecilie Sendstadt, “Russia’s Role as an Arms Exporter: The Strategic and Economic Importance of Arms Exports for Russia” \textit{Chatham House} (March 2017), 8, \url{https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-03-20-russia-arms-exporter-connolly-sendstad.pdf}.
\item \textsuperscript{39} Shevtsova, “The End of an Epoch.”
\item \textsuperscript{40} Margaret Vice, “President Putin: The Russian Perspective,” \textit{Pew Research Center’s Global Attitudes Project}, June 20, 2017, \url{http://www.pewglobal.org/2017/06/20/president-putin-russian-perspective/}.
\end{itemize}
but few serious analysts believe it will threaten the survival of the Communist Party in China. The same cannot be said with regard to Putin and the *siloviki*. Any change from the status quo in traditionally Russo-friendly nations like Belarus or Kazakhstan constitutes a direct threat to the regime, worthy of military intervention. Indeed, one could see Russia’s Zapad 2017 military exercises in Belarus as training to prepare for this possibility.

This is especially true as the United States continues to try to support democracy abroad while clamping down on global kleptocracy. Beyond geostrategic concerns, the Russian government now has an entrenched interest in seeing the rule of law, anti-corruption efforts, and democracy fail. Personal sanctions like the Global Magnitsky Act that freeze assets located in US banks are powerful tools for fighting Russian kleptocracy, but as the vice tightens Russian *siloviki* may increasingly find themselves out of options.

Of course, this is not to say that all exercises of Russian state power abroad can be attributed solely to Vladimir Putin and the *siloviki* clique’s desire to remain in power. The Kremlin is a confusing place, filled with backstabbing and political infighting that will only continue to grow as Putin nears retirement. Other powerful interest groups include oligarchs such as Arkady and Boris Rotenberg, who remain essential to Vladimir Putin’s hold on power and have significant input on Russian foreign policy. It does mean, however, that Russia’s actions cannot be predicted by a simple recourse to “realist thinking.” Instead of seeking national power or security, key figures within the Russian state are united instead in seeking to prolong their kleptocratic theft for as long as possible under the guise of historical revanchism. Russia’s security concerns have been subsumed to the sole interests of regime preservation, making events in the countries near abroad much more unpredictable and potentially deadly. To discount the interests of the *siloviki* clan therefore risks misunderstanding the basis of Russian foreign policy today. In a policymaking environment, increasingly bitter and hostile towards Russia, it is vital that the United States understand what motivates Russian action abroad. As the Trump administration tries to navigate the Russian knot domestically, it must be careful not to force either the US or the Russian regime into a corner from which neither can escape.

---


About the Author

Nicholas McCarty is a master’s degree candidate in the Security Studies Program in the Walsh School of Foreign Service at Georgetown University. Concentrating on Russian and Eurasian security concerns, Nicholas wrote his undergraduate thesis on Soviet and Russian internal propaganda and memory while in Saint Petersburg, Russia. He has since interned under Hudson Institute Research Fellow Hannah Thoburn, researching Eastern European and Eurasian kleptocracy before beginning a new internship within the Special Projects Division of the Special Inspector for Afghanistan Reconstruction (SIGAR) in December 2017. He graduated from the University of Notre Dame in 2016. All views expressed are his own.
An Unorthodox Call to Arms: The Humanitarian Case for Military Intervention in the DPRK

Bryant King

In the landmark 2014 Report of the Commission of Inquiry on Human Rights in the Democratic People’s Republic of Korea (DPRK), the United Nations claims that the DPRK is presiding over “systematic, widespread, and gross human rights violations” against its citizenry, whose “gravity, scale, and nature reveal a state that does not have any parallel in the contemporary world.” Consequently, it is appropriate for the United States and its allies to consider whether military intervention might be justified to address this situation, based on the Responsibility to Protect (R2P) framework developed by the International Commission on Intervention and State Sovereignty (ICISS) and the UN’s 2005 World Summit Outcome Document. Because preventive and non-military reactive measures implemented against the DPRK have not ameliorated the state’s human rights situation, the United States and its allies should view military intervention as a viable and legitimate course of action. However, the United States and its allies must recognize the ethical and political challenges they would face in the period leading up to and during the execution of a military intervention, and be willing to support long-running and extensive post-intervention state-building operations lead by the United Nations. While conducting a military intervention might seem a counterintuitive measure to address the DPRK’s human rights crisis, recent history proves that it might represent the only course of action.

In the more than six decades since the signing of the Korean Armistice Agreement in July 1953, the Democratic People’s Republic of Korea (DPRK) has largely earned its moniker of the “hermit kingdom,” isolating itself from all but a few members of the international community. In recent years, most focus on the DPRK has concerned the state’s burgeoning nuclear weapons program and missile testing. Despite the serious international security threat this program and testing poses, such a focus often overshadows the reality that the DPRK is arguably the most oppressive regime in the world, presiding over what the United Nations has identified as “systematic, widespread, and gross human rights violations” against its citizenry, whose “gravity, scale, and nature reveal a state that does not have any parallel in the contemporary world.” Amid increasingly heated rhetoric about a potential US invasion of the

---

DPRK in response to the state’s rapidly developing nuclear weapons program, whether the DPRK’s human rights crisis might justify military intervention also merits consideration.

This article will examine the historic and potential response of the United States and its allies to the human rights crisis in the DPRK, using the International Commission on Intervention and State Sovereignty’s (ICISS) three-pronged framework for the Responsibility to Protect (R2P): Prevention, Reaction, and Rebuilding. A brief history of the preventive measures taken to address the DPRK’s recurring abuses of state sovereignty will first be presented. Next, an overview of the non-military reactive measures implemented against the DPRK in response to such abuses will be provided, along with an analysis of whether military intervention in the DPRK is justified, based off the UN’s 2005 World Summit Outcome Document and the ICISS’ Principles for Military Intervention. The following two sections will provide an overview of the major ethical and political challenges the United States and its allies would face in the lead up to and during the execution of a military intervention in the DPRK. Finally, hypothetical post-intervention state-building operations in the DPRK will be considered, with a specific focus on the components of human security the United Nations should prioritize, using the UN Development Program’s (UNDP) framework. A brief analysis of the security implications of a continued failure to address the human rights crisis in the DPRK will follow, supplemented with recommendations the United States and its allies might consider to more effectively fulfill their obligations concerning the DPRK and R2P today.

An Overview of Preventive Measures Taken Against the DPRK

The ICISS defines the responsibility to prevent as requiring states “to address both the root causes and direct causes of internal conflict and other man-made crises putting populations

notes that the DPRK “did not respond to the commission’s repeated requests for access to the country and to information on the human rights situation.” This problem also affects other parties, including human rights organizations, with mandates to investigate and document human rights violations in the DPRK. The Commission of Inquiry collected the information in its landmark 2014 report and came to its above-mentioned conclusion by collecting “first-hand testimony through public hearings” in Seoul, Tokyo, London, and Washington, D.C. Other methods for obtaining information included confidential interviews, calling for written submissions from UN Member States, and engaging “with a number of UN entities and other humanitarian actors.” Consequently, there is little hard data to demonstrate the extent of the human rights violations perpetrated in the DPRK, with the United Nations instead providing estimates on the number of individuals affected by human rights violations (e.g. the Commission of Inquiry estimates “that between 80,000 and 120,000 political prisoners are currently detained in four large prison camps” in the DPRK). Notable ongoing attempts to document the DPRK’s human rights violations outside of the UN system include the Transitional Justice Working Group’s July 2017 report, titled “Mapping Crimes Against Humanity in North Korea: Mass Graves, Killing Sites, and Documentary Evidence,” and the Database Center for North Korean Human Rights (http://www.nkdb.org/en/main.php).

A tighter conception of this responsibility, according with the UN’s 2005 World Summit Outcome Document, requires states to prevent “genocide, war crimes, ethnic cleansing, and crimes against humanity.” The document establishes the obligation of the international community to “encourage and help States to exercise this responsibility.”

Adhering to this tighter conception, it is now appropriate to conduct an overview of the steps the United States and its allies have taken in recent years vis-à-vis the human rights crisis in the DPRK and the responsibility to prevent. The ICISS offers a host of potential preventive measures, including “early warning and analysis” and “direct prevention efforts,” to guide this effort.

Following the prescription of the ICISS, the United States and its allies have (largely ineffective) early warning and analysis mechanisms in place to prevent potential DPRK violations of state sovereignty of the nature highlighted in the 2005 World Summit Outcome Document. The United Nations has established several of these mechanisms in recent years, largely in response to recent reporting efforts that have documented the DPRK’s ongoing and egregious violations of its citizenry’s basic rights, including the perpetration of crimes against humanity and policies akin to genocide that are detailed below. However, the DPRK’s relative isolation challenges the efficacy of these mechanisms, which focus mainly on information gathering and reporting activities. The UN Office of the High Commissioner for Human Rights (OHCHR) in Seoul, as well as the Special Rapporteur on the Situation of Human Rights in the DPRK, are among the primary early warning and analysis mechanisms in place today. Government intelligence agencies, NGOs, faith-based groups, diaspora advocacy groups, and other actors bolster the efforts of these UN mechanisms.

The ICISS identifies several sectors where states can implement direct prevention efforts: political/diplomatic, economic, legal, and military. In relation to the human rights crisis in the DPRK, the United States and its allies, mainly under the auspices of the United Nations, have implemented some direct prevention efforts in the political/diplomatic sector. Such efforts include the establishment of the Special Rapporteur on the Situation of Human Rights in the DPRK in 2004, the landmark fact-finding work of the UN’s Commission of Inquiry on Human Rights in the DPRK, and the UN Human Rights Council’s Universal Periodic Review mechanism. In the economic sector, a limited number of states provide humanitarian assistance to the DPRK due to the state’s self-imposed isolation and hostile politics, while the DPRK also receives assistance directly from various UN agencies and funds, as well as from unidentified

---


5 ICISS, 21-27.
private actors. In terms of what the ICISS identifies as “negative inducement,” the United States and its allies constantly threaten the imposition of further sanctions on the DPRK through the United Nations, although not in direct response to the human rights crisis, as will be expounded upon below. This applies to US pressure on China and the DPRK’s other primary trading partners to limit their economic relationships with the state as well.

In the legal sector, the United States and its allies have failed to hold DPRK officials accountable for the perpetration of war crimes or any other human rights violations, although the UN Human Rights Council recently voted to install “international criminal justice experts...to develop plans for the eventual prosecution of North Korean leaders and officials responsible for human rights crimes” at the OHCHR office in Seoul. The politicization of the International Criminal Court and the UN Security Council (UNSC), as well as the high costs associated with the establishment of ad hoc tribunals, suggest that international criminal law will likely not be

---

6 “DPR Korea Needs and Priorities 2017.” UN Financial Tracking Service. Online. 17 December 2017. The UN’s global humanitarian aid tracker records the total amount in humanitarian aid pledged to the DPRK in 2017 as $39.4 million. 32 pledges from state actors, unidentified private actors (individuals and organizations), and directly from UN agencies and funds, including the World Food Programme and the Central Emergency Response Fund, account for this total commitment. The state actors that made humanitarian aid pledges to the DPRK in 2017, listed in order of size of total commitment, include Switzerland, Russia, Sweden, Canada, the United States, France, and Lichtenstein. Contributions from state and private actors are directed toward either UN agencies or independent humanitarian organizations in one of the following sectors: (1) food security; (2) health; (3) nutrition; (4) Water, Sanitation, and Hygiene; (5) not specified. The UN’s 2017 humanitarian aid appeal for the DPRK was only 31.2% funded; Choe Sang-Hun, “$8 Million to Aid Poor North Koreans? South Korea and Japan Disagree.” New York Times. 15 Sept. 2017. Online. 19 Nov. 2017. While the UN’s Financial Tracking Service is a valuable tool, it only records humanitarian aid contributions that state actors voluntarily report to the United Nations. Consequently, South Korea’s recent $8 million humanitarian aid pledge to the DPRK is not reflected in the $39.4 million figure noted above, suggesting that the $39.4 million figure represents a minimum baseline for humanitarian aid committed to the DPRK in 2017; Mark E. Manyin and Mary Beth D. Kikitin, “Foreign Assistance to North Korea.” Congressional Research Service, U.S. Library of Congress. R40095 (2014): 3-4, 10-19. As reflected in the UN Financial Tracking Service’s data above, the United States has made minimal humanitarian aid commitments to the DPRK in recent years. This is in contrast to the period between the mid-1990s and mid-2000s, when the United States provided hundreds of millions of dollars in food aid through the World Food Programme, in exchange for concessions regarding the DPRK’s nuclear weapons program.

7 Kent Boydston, “North Korea’s Trade and the KOTRA Report.” Peterson Institute for International Economics. 1 August 2017. Online. 17 December 2017; Karishma Vaswani, “What if Trump Cut Ties with North Korea’s Trade Partners.” BBC. 4 September 2017. Online. 17 December 2017. While China represents the DPRK’s largest trading partner by a large margin, accounting for approximately 90% of the DPRK’s total trade in 2016, a report from Korea’s Trade Investment Promotion Agency notes that dozens of states have trade relationships with the DPRK. Other significant trade partners with the DPRK include Russia, India, Thailand, the Philippines, and Pakistan. For an excellent visualization of the DPRK’s global trade, including the state’s primary industries for imports and exports, visit the Observatory of Economic Complexity’s website. For successful examples of the United States pressuring China into limiting its economic relationship with the DPRK in the last year, please see footnote 18.

utilized as a preventive measure against the DPRK in the future. The United States and its allies have also failed to implement direct prevention efforts in the military sector, designated as “preventive deployments” by the ICISS, against the DPRK. Overall, efforts to fulfill the responsibility to prevent vis-à-vis the human rights crisis in the DPRK have been variable.

Historic and Potential Reactive Measures Against the DPRK

The failure of the United States and its allies to comprehensively fulfill their obligations under the responsibility to prevent, combined with the DPRK’s abrogation of any such responsibility, fosters an environment conducive to the government’s regularly abusing its sovereignty and the basic rights of its citizenry. In its landmark 2014 report, the Commission of Inquiry on Human Rights in the DPRK “establishes that crimes against humanity have been committed in the DPRK, pursuant to policies established at the highest level of the State” and “finds that crimes against humanity are ongoing in the DPRK.” The United Nations organizes these crimes against humanity under several thematic areas, and argues in the same report that the DPRK’s extermination campaigns carried out in its political prison camps are “akin to genocide.” Regardless of whether these campaigns accord with the legal definition of genocide, the DPRK’s continued and documented perpetration of various crimes against humanity necessitates collective action by the United States and its allies, under the R2P framework laid out in the 2005 World Summit Outcome Document.

The ICISS defines the responsibility to react as obligating states “to react to situations of compelling need for human protection,” with non-military and, in extreme cases where certain thresholds are met, military measures. According to the 2005 World Summit Outcome Document, the use of such measures can only occur when preventive efforts have failed and the state in question has abrogated its responsibility to protect its population through the perpetration of “genocide, war crimes, ethnic cleansing, and/or crimes against humanity.” To date, there are only limited instances involving the implementation of non-military reactive measures against the DPRK specifically in response to the state’s human rights crisis. In recent years, the United States and its allies have implemented several of the ICISS’ proposed non-military reactive measures against the DPRK, including the imposition of arms embargoes,

---

10 ICISS, 57-58.
11 Human Rights Council, 319-52. These thematic areas include: (1) crimes against humanity in political prison camps; (2) crimes against humanity in the ordinary prison system; (3) crimes against humanity targeting religious believers and others considered to introduce subversive influences; (4) crimes against humanity targeting persons who try to flee the country; (5) starvation; (6) crimes against humanity targeting persons from other countries, in particular through international abduction.
targeted sanctions, “restrictions on income generating activities,” and diplomatic strategies to further isolate the state.\textsuperscript{12} However, these measures have been in response to the DPRK’s burgeoning nuclear weapons program, with only limited mention given in UN documents to the potentially negative effects that such measures might have in further deepening the state’s humanitarian crisis.\textsuperscript{13} One exception to this pattern is the North Korea Sanctions and Policy Enhancement Act of 2016, which specifically empowers the President of the United States to impose targeted sanctions against “entities found to have contributed to North Korea’s human rights abuses.”\textsuperscript{14}

While the United States and its allies have implemented non-military reactive measures suggested by the ICISS, although technically not in direct response to the DPRK’s continued perpetration of crimes against humanity, such measures have had little positive effect in ending the perpetration of said crimes against humanity. Considering this reality, it is appropriate that the United States and its allies seriously evaluate the possibility of military intervention against the DPRK to fulfill the responsibility to react, in accordance with the 2005 World Summit Outcome Document. Because the United Nations has formally documented and condemned the DPRK for the perpetration of crimes against humanity, and because preventive efforts and non-military reactive measures have failed to stem the perpetration of such crimes, military intervention in the DPRK is legally justified under Chapter VII of the UN Charter. Additionally, an intervention carried out in such a manner appears to satisfy the ICISS’ “just cause threshold,” which warrants military intervention in the case of “large scale loss of life, actual or apprehended, with genocidal intent or not, that is the product either of deliberate state action, or state neglect or inability to act, or a failed state situation.”\textsuperscript{15} However, the United States and its allies would face two central challenges in the period leading up to such an intervention that will be explored in the following section.

**Pre-Intervention Challenges: Jus Ad Bellum and China**

Before examining the consequences of the execution of a military intervention in the DPRK, the United States and its allies must consider two central challenges, one ethical and one political, that would emerge in the period leading up to said intervention. As alluded to above, just war theory has a significant influence on the R2P framework laid out by the ICISS and in

\textsuperscript{12} ICISS, 29-31.
\textsuperscript{15} ICISS, 32-35.
the 2005 World Summit Outcome Document. In the period leading up to military intervention in the DPRK, the United States and its allies must seriously evaluate whether said intervention adheres to the six principles of *jus ad bellum*: (1) just cause; (2) right intention; (3) last resort; (4) proportional means; (5) reasonable prospects; (6) right authority. A military intervention conducted by the United States and its allies in the DPRK on humanitarian grounds would clearly adhere to the principles of just cause and right intention, as outlined above. Despite the potential costs of such an intervention, which will be explored in the following section, the United States and its allies would certainly have reasonable prospects for success, while planning for the humanitarian intervention would necessarily adhere to the principle of proportional means. The United States and its allies would have to deploy, in good faith, all possible preventive and non-military reactive measures, particularly preventive diplomacy, prior to intervening to ensure adherence to the principle of last resort.

The United States and its allies would face the most difficulty in fulfilling the principle of right authority, which in the case of military intervention in fulfillment of R2P is manifested in the form of the UNSC. It is unlikely at this time that either China or Russia, both Permanent Members of the UNSC with veto-wielding power, would abstain or vote in favor of a military intervention in the DPRK led by the United States and its allies. Two options exist that the United States could pursue to technically adhere to this principle without the UNSC’s authorization, a scenario anticipated by the ICISS in light of NATO’s intervention in Kosovo in 1999 without the UNSC’s authorization. However, this difficulty points to the single greatest political challenge the United States and its allies would face in conducting a military intervention in the DPRK: winning over China.

In recent years, largely as a result of the increasing belligerence of the Kim regime, relations between China and the DPRK have deteriorated considerably. In a recent article in

---

16 ICISS, XII-XIII (Foreword), 31-37.
17 ICISS, 53-55. If the UNSC fails to authorize a military intervention that satisfies the conditions for R2P, the ICISS suggests two other methods for obtaining right authority. The first method involves garnering support for an intervention by calling an Emergency Special Session of the UN General Assembly under the “Uniting for Peace” procedure. The second method involves regional or sub-regional organizations engaging in an intervention within their jurisdiction under Chapter VIII of the UN Charter. The UNSC can give its approval to an intervention after the intervention has been completed.
Georgetown Security Studies Review 6:1

*Foreign Affairs*, Georgetown University professor Oriana Skylar Mastro argues that “China is no longer wedded to North Korea’s survival,” and notes that “the Chinese military assumes that it would be opposing, not supporting, North Korean troops,” in the event of a new Korean war. The same article, titled Why China Won’t Rescue North Korea, suggests that “China will intervene extensively and militarily on the peninsula” to pursue its interests, including the neutralization of the DPRK’s nuclear threat, if the United States and its allies intervene in the DPRK. While this article presumes that the United States and its allies would intervene in the DPRK to neutralize the state’s nuclear threat, nothing suggests that the aforementioned logic concerning China and the DPRK would change if said intervention was instead pursued on humanitarian grounds.

Beyond the recent deterioration in China-DPRK relations, the construction of massive refugee camps along the Chinese-DPRK border suggests that China views increasing instability and potential conflict in the DPRK as an inevitability. Additionally, recent reports suggest that the United States has made clear to China that, following an intervention in the DPRK, the United States would allow China and South Korea to decide who would manage and govern the territory previously belonging to the DPRK. This assurance should serve to quell most concerns that China might hold about potential ulterior motives underlying US intervention in the DPRK. China would presumably not give the United States a free pass, including through its vote in the UNSC, to intervene in the DPRK on humanitarian grounds today. However, the above-mentioned developments collectively suggest that continued belligerence and increased signs of instability from the DPRK could make China more amenable to the idea of a US intervention, particularly if said intervention involved tasking China with the responsibility of seizing control of the DPRK’s nuclear weapons infrastructure. If the United States follows Professor Mastro’s advice to “recognize that some forms of Chinese intervention would actually be beneficial to its interests,” a US intervention in the DPRK on humanitarian grounds could empower China to play a major role in eliminating the DPRK’s nuclear weapons threat, potentially leading to the killing of two metaphorical international security birds with one intervention stone. However, while the ethical and political objectives that might arise in the lead up to military intervention in the DPRK appear surmountable, the United States and its allies

---

would also have to seriously consider the devastating humanitarian consequences and regional security implications such an intervention would potentially bring about.

The Ethics and Security Implications of Military Intervention

Though the United States and its allies should seriously consider the prospect of military intervention in the DPRK to uphold R2P, they must also take seriously the potential humanitarian consequences and regional security implications of said intervention and perform a thorough cost-benefit analysis before committing to any action.\(^2\) Estimates suggest that “one million people (civilians and military) could die on the first day of a second Korean war” alone, with Scott Sagan, a prolific contributor to *Foreign Affairs*, arguing that there is “no military solution” to the situation in the DPRK.\(^3\) While Sagan is discussing the potential consequences of military action in response to the DPRK’s nuclear weapons program, there is no reason to think that the above-mentioned estimate of potential deaths would be any different for a military intervention initiated on humanitarian grounds. The DPRK will not view an intervention on humanitarian grounds as any less of an existential threat than an intervention launched primarily in response to its nuclear weapons program, and the prospect for the use of nuclear, chemical, and biological weapons would not differ in either scenario. The use of any of these weapons would have fatal and long-lasting humanitarian consequences for citizens in the DPRK, as well as the ROK and Japan potentially, compounding the current situation. However, the threat of nuclear weapons use could be mitigated if the United States encouraged China to seize control of the DPRK’s nuclear weapons infrastructure, as mentioned above.

Beyond the obvious potential humanitarian impact a military intervention could have on the DPRK and its neighbors, such an intervention could also have serious regional security implications. Military intervention would spark massive refugee flows from the DPRK into the ROK and China, posing a major challenge to those states and relevant humanitarian actors. Japan and the ROK would also look unfavorably on any action that increases their insecurity in the short-term, particularly if China decides to pursue a concurrent intervention with the United States and its allies. Chinese intervention would also threaten the position of the United States in a post-intervention East Asia. However, the preemptive measures China has taken in response to potential refugee flows, the continued guarantee of extended deterrence to the ROK and

---

\(^2\) This section of the paper is written under the assumption that the United States and its allies would respect and adhere to the *jus in bello* principles of discrimination and proportionality during the course of a military intervention in the DPRK.

\(^3\) Scott D. Sagan, “The Korean Missile Crisis: Why Deterrence is Still the Best Option.” *Foreign Affairs* 96.6 (2017): 78-80. This estimate accounts for citizens from the DPRK and the Republic of Korea (ROK), as well as military personnel from the United States, the ROK, and the DPRK.
Japan by the United States, and the potentially beneficial impact of Chinese intervention seem to at least partially mitigate some of these concerns. A potential compromise solution to address concerns about a diminished post-intervention role for the United States in East Asia is offered in the following section. The elimination of the DPRK threat would enhance the security of the United States and all other state actors in East Asia, and presumably outweigh any short-term costs of military intervention. Regardless, military intervention in the DPRK would exacerbate what is arguably the world’s worst environment for the protection of human security, raising serious questions concerning the moral righteousness of military intervention, despite its legal standing and long-term benefits.

Ultimately, the long-running and unchanging nature of the human rights crisis in the DPRK suggests that a military intervention might be the only path toward achieving substantive and lasting change in the state. Since the Korean Armistice Agreement nearly 65 years ago, the human rights crisis in the DPRK has only worsened, and the United Nations and individual state actors have been largely unsuccessful in ameliorating the situation. While military intervention could result in serious potential humanitarian consequences and have regional security implications in the short-term, comprehensive and long-lasting post-intervention state-building operations, as described below, could only serve to enhance the humanitarian situation in the DPRK and bolster regional stability in the long-run. The United States and its allies should not continue to view offering inconsistent criticism of a regime that takes advantage of a fragile peace built upon a foundation of fear as a sustainable course of action. While controversial, the United States and its allies should accept military intervention in the DPRK as a legitimate course of action for addressing the state’s human rights crisis.

Post-Intervention State-Building Operations in the DPRK

The devastation that a military intervention would inflict on the DPRK and its citizenry would be substantial, and would necessitate comprehensive post-intervention rebuilding operations unparalleled in the modern age. The ICISS defines the responsibility to rebuild as requiring states “to provide, particularly after a military intervention, full assistance with recovery, reconstruction, and reconciliation.” While the United States would presumably desire to lead such operations, the United Nations would in fact be the actor best suited to fulfill the leadership role, for reasons explained below. Before doing so, this section will demonstrate the magnitude of hypothetical post-intervention state-building operations by providing a brief overview of the current state of human security in the DPRK, using the UNDP’s seven component framework:

---

24 ICISS, XI (Foreword).
• **(1) Economic Security:** Approximately 40% of the DPRK’s citizenry lives under the poverty line, and the government “systematically uses forced labor from ordinary citizens” to support its collapsing centrally-planned economy that depends largely on black market operations. Sanctions have devastated the DPRK’s economy, while the *songbun* discrimination system has perpetuated an economically stratified society that is particularly discriminatory toward women.

• **(2) Food Security:** The United Nations accuses the DPRK of having “committed crimes against humanity by implementing actions, decisions, and policies known to have led to mass starvation, death by starvation, and serious mental and physical injury.” Government policy and vulnerability to natural disaster has left the DPRK dependent on food aid from the international community, although the government has at times hindered the delivery of such aid. The World Food Programme estimates that 70% of North Koreans are food insecure.

• **(3) Health Security:** Amnesty International reports that, “the people of North Korea suffer significant deprivation in their enjoyment of the right to adequate health care.” Problems include crumbling infrastructure, inadequate medical supplies and training, and a stratification of the health care system that favors those who are wealthy and live in urban areas. Government reluctance to accept international aid exacerbates this situation. In connection to food insecurity, “widespread and chronic malnutrition” has “triggered epidemics and mass outbreaks of illnesses related to poor diet,” including an ongoing tuberculosis epidemic.

• **(4) Environmental Security:** Deforestation is a major problem in the DPRK, while widespread land degradation, over-farming, and the ever-present threat of natural disaster leave the state vulnerable to famine. Water-borne diseases are prevalent in the

---


DPRK, while increasing levels of air pollution and a continued reliance on coal pose major environmental threats to the DPRK’s citizenry.\(^30\)

- **(5) Personal Security:** As has been explained through the descriptions of the DPRK’s perpetration of crimes against humanity and policies akin to genocide, levels of personal security throughout the state are very low. The high occurrence of torture and enslavement, as well as the perpetration of rampant sexual and gender-based violence, are but a few of the personal security threats the DPRK’s citizenry faces today, largely at the hands of its government.

- **(6) Community Security:** The DPRK does not tolerate political dissension, and sends dissidents to political prison camps situated throughout the country for reeducation purposes. The US Department of State has designated the DPRK a “Country of Particular Concern” for “having engaged in or tolerated particularly severe violations of religious freedom” since 2001.\(^31\) Additionally, homosexuals, the disabled, and other minority communities face high levels of government persecution.

- **(7) Political Security:** The UNDP defines this aspect of human security as ensuring that “people live in a society that honors their basic rights.” The report goes on to site “systematic torture, ill treatment, or disappearance,” along with the exercise of “control over ideas and information,” as manifestations of political repression.\(^32\) The DPRK is guilty of committing egregious manifestations of these and other acts of political repression, and is arguably the world’s most politically insecure state. The fact that the DPRK maintains the world’s fourth largest active military and dedicates a disproportionate amount of its annual budget to military expenditures further reinforces these high levels of political insecurity.\(^33\)

As mentioned above, the United States and its allies would be best advised to relinquish leadership of all post-intervention state-building operations in the DPRK to the United Nations. The primary reason for this recommendation is that the United Nations would serve as a neutral and impartial leader of rebuilding efforts. This neutrality would bolster the ability of the United

---


Nations to mitigate the inevitable political disputes over the future of the DPRK that would break out between the United States and a China that would presumably be interested in leading such rebuilding efforts. In this way, the leadership of the United Nations would allow for the perspectives and interests of both the United States and China to be heard and recognized, while preventing the outbreak of a potentially disastrous competition between the two parties to dominate the rebuilding efforts. An additional reason for this recommended delegation of responsibility is the sheer size of the hypothetical post-intervention state-building operations, which would place an undue burden on a United States that is still heavily involved in Afghanistan and Iraq, among other locales. Tied to this point is the presumption that public opinion both at home and abroad would look unfavorably upon the prospect of the United States leading additional state-building operations, as the shadows of Afghanistan and Iraq continue to loom large on the collective consciousness. Delegating leadership to the United Nations, which has past experience in state-building operations, might represent the only compromise solution that the United States, China, and other relevant parties deem acceptable for rebuilding a post-intervention DPRK.

As with any post-intervention rebuilding operations, the United Nations should first prioritize the protection and promotion of personal, community, and political security in a hypothetical scenario concerning the DPRK. Political security will likely take longer to establish due to the presence of lingering vestiges of the Kim regime, thereby placing a large burden on a hypothetical transitional administration. The United Nations must then concentrate on the provision of basic needs through the bolstering of food and health security. Economic and environmental security represent the components of human security that require a longer-term focus, yet must be engaged alongside those components that are achievable in the short-term to ensure a peaceful and sustainable future for the DPRK.34

Security Implications of Inaction and Recommendations

When considering whether and how it might address the human rights crisis in the DPRK, the United States and its allies must understand the security implications of failing to substantively address this crisis. Among other issues, this failure will allow for a continued weakening of the DPRK’s economy, making illicit economic activities like human and drug trafficking more attractive and contributing to greater regional instability. Allowing conditions to persist that heighten the possibility of famine and increased refugee flows will further impact regional stability, and could potentially weaken the ability of the United States and China to

---

address the many challenges the DPRK poses to the international community in a unified and comprehensive fashion. Naturally, failing to address the human rights crisis in the near term will also make potential post-intervention rebuilding operations much more difficult.

More broadly, the continued failure of the United States and its allies to fulfill their obligations under R2P and respond to the DPRK’s abuses of state sovereignty will undermine the authority of the United Nations and the legitimacy of international law. While military intervention without the UNSC’s authorization would similarly undermine the United Nations and international law, such action would arguably have a lesser impact with more easily solvable consequences than would a failure to uphold R2P and hold the DPRK accountable. The United Nations has survived and grown from previous episodes where the politicization of the UNSC forced external actors to subvert the council’s authority and take action in response to human rights crises, most notably in the case of NATO’s intervention in Kosovo in 1999. Intervention by the United States and its allies could spur much-needed reform of the UNSC that would allow the council to better respond to future crises, while the delegation of leadership of post-intervention state-building operations to the United Nations would provide the international organization a significant opportunity to regain any authority or legitimacy lost in the period leading up to the intervention. The process of undermining associated with a failure to uphold R2P could have wide-ranging effects with much more serious implications, from giving cover to and empowering other regimes that violate the rights of their citizenry to rendering the UNSC impotent in its attempts to address conflicts throughout the globe in the future.

The DPRK continues to perpetrate crimes against humanity and carry out policies akin to genocide against its citizenry, thereby obligating the United States and its allies to respond to this crisis, in accordance with the R2P framework laid out in the UN’s 2005 World Summit Outcome Document. Variable preventive efforts, as well as non-military reactive measures, have failed to stem the DPRK’s regular abuses of state sovereignty. Accordingly, it is appropriate and justifiable to consider a military intervention in the DPRK in response to the state’s grave human rights crisis, as opposed to the state’s burgeoning nuclear weapons program. However, the United States and its allies must realize the ethical and political challenges they would face in the period leading up to such an intervention, including adherence to the principles of just war theory and dealing with Chinese national interests. These actors must also acknowledge the potentially devastating humanitarian consequences and regional security implications of military intervention in the DPRK, and be willing to support large-scale and long-term post-intervention rebuilding operations led by the United Nations.
The bottom line is that the United Nations is correct in labeling the human rights situation in the DPRK “without parallel in the contemporary world,” and all members of the international community have an obligation to address this crisis in a comprehensive and substantive way. The United States and its allies must recognize military intervention as a viable and legitimate course of action to address the human rights crisis in the DPRK. Beyond the security implications of failing to address this crisis, inaction will leave an indelible stain on the moral standing of every state that continues to treat what is going on in the DPRK as politics as usual.

About the Author

Bryant King is a senior in Georgetown University's School of Foreign Service (SFS) and first-year Security Studies Program (SSP) student, concentrating in International Security and pursuing a certificate in Refugees and Humanitarian Emergencies.
Lessons Learned from the Russian Active Measures Campaign in the 2016 United States Presidential Elections: A Crossroads of Success and Failure

Susanne Boss

Over the past year, allegations have solidified into judgments surrounding Russian involvement in targeting multiple facets of the US 2016 Presidential Election. Known as active measures, Russian actions strategically blended the use of covert intelligence operations with overt activity in three method areas: Malicious Cyber Activity, Disinformation, and Possible Collusion between Russia and Trump Campaign officials. Examples of these method areas range from the exposure of more than 126 million users on Facebook to posts created and disseminated by Russian operatives, to the Russian-linked hacking and leaking of thousands of emails associated with the Hillary Clinton Campaign and the Democratic National Committee. This article examines the Russian active measures targeting of the US 2016 Presidential Election as a case study of both successful Russian covert action and failed American counterintelligence. As Russia will certainly apply lessons learned from this campaign to future influence efforts against the United States and other democracies, it is critical for policy makers to identify and apply lessons from this experience to better prepare for and counter future active measures operations.

Introduction

The Russian covert intervention in the United States 2016 Presidential Election illustrates the use of successful Russian intelligence operations, termed as active measures (aktivnye meropriyatia in Russian), involving the utilization of numerous malicious cyber activities and influence operations. These active measures will be examined as a case study of both successful Russian covert action and failed American counterintelligence.

Allegations have evolved into judgments over the past year, surrounding Russian involvement in targeting multiple facets of the US 2016 Presidential Election. To fully comprehend Russia’s campaign, it is necessary to understand the strategic use of blending covert intelligence operations with overt activity into three method areas: Malicious cyber activity (hacking and leaking), disinformation (infusion of false and manipulative information into US political discourse), and possible collusion between Russian representatives and Trump campaign officials. While legal and intelligence analyses regarding these contemporary events are still emerging, this article examines the known events and seeks to identify lessons learned based upon current publicly available information and unclassified US intelligence assessments.
Malicious Cyber Activity

This section provides a non-exhaustive summary of several malicious cyber activity events perpetrated by Russian operatives that took place leading up to the US 2016 Election. In September and November 2015, the FBI attempted to alert the Democratic National Committee (DNC) to a potential breach,\(^1\) indicating that Russian hacking schemes had been specifically targeting election elements for more than a year leading up to the presidential election.\(^2\) These hacks resulted in breaches of at least one computer system of the DNC and a spearphishing attack directed at the Chairman of Hillary Clinton’s Campaign John Podesta’s personal email account.\(^3\) Thousands of emails from these attacks were later strategically and incrementally leaked over the stretch of the election\(^4\), producing detrimental effects on the Clinton campaign and fracturing the unity of the Democratic Party.\(^5\) An October 2016 Department of Homeland Security (DHS) and Office of the Director of National Intelligence (ODNI) joint statement judged with high confidence that the Russian Government directed those compromises, as the disclosures from DCLeaks.com, WikiLeaks, and the Guccifer 2.0 online persona were “consistent with the methods and motivations of Russian-directed efforts.”\(^6\)

A December 2016 DHS and FBI Joint Analysis Report details technical specifics on the indicators\(^7\) of tools and infrastructures utilized by Russian civilian and military intelligence services. It is notable that no previous Joint Analysis Report has attributed malicious cyber activity to specific countries or threat actors.\(^8\) The Russia cyber activity of this case, referred to as

---


\(^7\)To see specific indicators of malicious RIS activity, visit: DHS and NCCIC. February 10, 2017. Enhanced Analysis of GRIZZLYSTEPPE Activity, Joint Analytical Report by the DHS and NCCIC. Available at: https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf.

GRIZZLY STEPPE in the report, included spear phishing campaigns, disruptive cyber-attacks on critical infrastructure networks, as well as masquerading as third parties designed to misattribute attacks.\(^9\) Though the Russian military intelligence service (GRU) was not yet directly identified in either of these joint statements, the January 2017 Intelligence Community Assessment names the GRU as a source of cyber espionage against US political organizations, as well as theft and public disclosure of Russian-collected data.\(^{10}\) Crucially, these malicious cyber activities are linked to a Russian military service, indicating that the Russian Government itself, beyond civilian actors, was directly involved in attempts to target and manipulate elements of the US Presidential Election.

**Disinformation**

The January 2017 Intelligence Community Assessment (ICA) states that the Intelligence Community has high confidence that President Putin ordered an influence and disinformation (termed dezinformatsiya in Russian) campaign surrounding the election, aimed at influencing public opinion, undermining the US democratic process, and skewing support against Hillary Clinton towards now-President Trump.\(^{11}\) This campaign blended covert intelligence operations with overt efforts by “Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or ‘trolls’.”\(^{12}\) The ICA assesses with high confidence that the GRU used Guccifer 2.0 and DCLeaks.com to release hacked US data to the public through media outlets and WikiLeaks. The disclosures to WikiLeaks did not contain apparent forgeries, and Republican material was also collected, but did not result in a “comparable disclosure campaign”.\(^{13}\) Hacking groups such as Cozy Bear and Fancy Bear (termed by CrowdStrike) were found to have ties to the Russian government according to the Joint Analysis Report.\(^{14}\) Russian state-sponsored and pro-Kremlin media, such as RT (formerly known as Russia Today) and Sputnik, as well as quasi-governmental trolls, such as the Internet Research Agency, were specifically named as actors who contributed to the Russian campaign by “serving as a platform for Kremlin messaging to Russian and international audiences.”\(^{15}\) For example, the Internet Research Agency is linked to buying thousands of divisive Facebook ads costing more

---


\(^{11}\) *Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections (Hereafter: ICA)*. ii.

\(^{12}\) Ibid., iii.

\(^{13}\) Ibid., 3.

\(^{14}\) Bump. The Washington Post.

\(^{15}\) ICA. Page 3.
than $100,000.\textsuperscript{16} Beyond this, according to an October 31, 2017 Facebook, Twitter, and Google testimony to Congress, Russian-linked online posts reached more than 126 million users on Facebook alone, during a three month period leading up to the election.\textsuperscript{17} Twitter estimates that more than 36,000 accounts associated with Russia generated automated, election-related content producing 1.4 million tweets that were presented to users of the micro-blogging platform 288 million times.\textsuperscript{18} These efforts are elements in Russia’s specific goals of messaging to diminish the image of Hillary Clinton, displaying a preference for the Trump campaign, as well as sowing divisiveness and attempting to erode confidence in the US democratic election process.

In reaction to these malicious cyber and disinformation activities, the US government has (1) implemented new and hardened old sanctions on Russia since 12/29/2016, (2) expelled 35 Russian diplomats and confiscated two Russian-linked compounds, (3) spurred investigations by a Special Counsel via the Justice Department, the Senate Intelligence Committee, the Senate Judiciary Subcommittee on crime and terrorism, the House Intelligence Committee, and the House Oversight and Government Reform Committee\textsuperscript{19}, and (4) ordered antivirus software suspected of providing a back-door for Kremlin access made by a Russian company, Kaspersky Lab, to be removed from government computers.\textsuperscript{20}

**Possible Collusion**

Another element of the Russian covert action may involve possible collusion between members of the Trump campaign and Russian officials. *All five* of the federal investigations initiated in reaction to the Russian influence campaign are investigating whether there are ties between Trump associates and Russian officials.\textsuperscript{21} The Special Counsel investigation, headed by Robert Mueller, has thus far resulted in indictments of four Trump-related officials: George Papadopoulos, Paul Manafort, Rick Gates, and Michael Flynn.

\textsuperscript{21} Kim and Krishnakumar. *A guide to every Russia investigation happening right now.*
On October 5, 2017 George Papadopoulos pled guilty to lying to the FBI about having ties to Russian nationals during his tenure as a foreign policy advisor to President Trump. This indictment and plea was not unsealed until several weeks later. Trump’s former campaign chairman Paul Manafort, and campaign adviser Rick Gates were indicted on October 30 for laundering millions of dollars in oversees shell companies. Beyond this, Manafort was allegedly still laundering money obtained through his illegally “unregistered foreign agency on behalf of Ukraine and its Party of Regions” which was heavily connected to Pro-Russian former Ukrainian President Victor Yanukovych, at the same time that Papadopoulos admits he was working with Russian individuals to obtain “dirt” on Hillary Clinton in the form of thousands of emails, in April 2016.

Finally, Trump’s now-former National Security Adviser Michael Flynn failed to disclose income that he received from Russian-linked entities, including a $45,000 speaking fee from RT for a 2015 speech and dinner in Moscow during which he sat next to President Putin. On December 1, 2017 Flynn was charged and plead guilty to making false statements to the FBI regarding conversations with Russian officials, including the Russian ambassador Sergey Kislyak, in December 2016.

It is important to note that questions remain surrounding the extent and exact nature of these interactions and whether a higher level of covert operations exists. However, due to the high level of Trump advisers involved, as well as the frequency and timing of these interactions, it is an important element of possible Russian methodology to acknowledge.

23 Ibid.
Success or Failure?

The executed Russian active measures feature several attributes of a successful covert action campaign, while America’s counterintelligence apparatus will need to quickly and efficiently adapt to improve its capabilities in the future. US counterintelligence failed in its objective, defined in the 2016 U.S. National Counterintelligence Strategy as both a defensive mission in protecting US elements against foreign actors, as well as an offensive mission in gaining knowledge of the capabilities and intentions of foreign actors. The subsequent reaction of the United States to these engagements was hampered due to domestic, political, and social fracturing, as well as intended and unintended miscommunication between US stakeholders.

Russian covert action was used as a facet of Russia’s foreign policy, rather than as a “magic bullet”, integrated within a larger and well-coordinated policy context against carefully considered targets. Timing, resources, and sustainable leadership circumstances were favorable components spearheaded by the vertical structure of power in Putin’s hierarchical presidency, which were able to strengthen Russia’s active measures effort. Finally, there was a “symbiosis” between the goals of the Russian influence operation and Russia’s historical intelligence culture in covert intervention, overall policy, and government efforts. Well-established purposes of covert action include influencing the internal balance of power in a country, the climate of political opinion, and inducing specific desired actions. It is difficult to ascertain Russia’s success with regards to its ability to induce particular actions without knowledge of specific Russian prerogatives, as well as to quantifiably measure how much effect the propaganda campaign had on the American psyche. Yet, Russia did successfully execute covert malicious cyber-attacks, as well as an expansive disinformation campaign, representing “a significant escalation in directness, level of activity, and scope of effort compared to previous operations.”

Analysis

Russia successfully utilized covert action within a larger foreign policy context by virtue of the vertical governmental power structure with Putin as its executive pinnacle (termed vertical vlasti in Russian). For example, between the 2013 and 2016 editions of Russia’s Foreign Policy

---

30 Ibid., 121-132.
31 Ibid., 134.
32 ICA. 5.
*Concept of the Russian Federation*, media and the legitimate use of force has been elevated both under Russia’s listed foreign policy goals as well as in reference to combating terror threats. The official policy statement mirrors the unofficial and more covert policy tool of dezinformatsiya, linking domestic and foreign policy through similar goals of increasing Russian global power and influence, as well as a desire to continue Russia’s recent economic growth. This cohesion enables Putin to expand efforts of active measures through the financial, political, intelligence, social, and operational avenues of the Russian Government.

Beyond this, Russia’s chief of the general staff, General Gerasimov, stated that the methods of conflict for Russia have changed towards the “broad use of political, economic, informational, humanitarian, and other nonmilitary measures—applied in coordination with the protest potential of the population.” This critical statement simultaneously acknowledges Russia’s strategy for exploiting predispositions of a given population—the “protest potential” of a group—while alluding to the necessity for Russia to turn to asymmetric and unconventional means in the security sphere. Following the collapse of the Soviet Union, the militarily diminished Russian Federation has found a new approach to its methods in conflict. These views are further codified in the 2014 official Russian military doctrine, paragraph 15. In other words, Russia is combining two emerging norms: the emphasis of active measures dating to Russia’s (Soviet and Bolshevik) historical pre-Cold War roots, and the norm of the past 20 years to utilize aggressive digital espionage, through the expansive use of disinformation layered upon and referencing disclosed material resultant from malicious cyber activity.

Russia, through long-term research programs and sheer scope of action, has excelled in understanding its target audience. For example, since early 2014, Russian intelligence has researched US electoral processes and related technology and equipment, and Russia has for years attempted to breach US government computer software. Beyond this, the Kremlin-linked and Russia-based Internet Research Agency has been associated with numerous disinformation

---

38 *ICA*. 3.
campaigns targeting the United States. In one example, the agency attempted to sow fear and chaos on September 11, 2014 by orchestrating a fake explosion of a chemical plant in Centerville, Louisiana. This disinformation effort targeted St. Mary Parish in Louisiana with many facets including text messages, Twitter and Facebook posts, as well as YouTube videos.

Cyber capabilities have also enabled a versatile function of malicious attacks and disinformation: software applications may be breached and utilized as amplification platforms for certain views, while group and individual-based hacking facilitates personalized targeting, increasing the odds of successful reception of manipulated information by a target audience. Though Russia may not have successfully kept the covert nature of its sponsored activities hidden for very long, this may be irrelevant to the leadership in the face of simply demonstrating Russia’s intentions and capacity to undermine the US democratic process. However, this neglect of tradecraft may ultimately come to haunt Russian leadership, if the United States decides to apply more drastic consequences either through legal, economic, military, or reciprocal cyber or covert actions.

The United States was neither unified in its counterintelligence preparation nor in its response to Russia's actions. There is a historical suspicion of centralized counterintelligence and skepticism of concentration of power within America, leading to a weak foundation for effective communication between the intelligence community and the public sphere. As General Gerasimov alludes, disinformation is most effective when its target audience is predisposed to be receptive to manipulated narratives. Roy Godson states that the forger, in this case Russia, is primarily focused upon identifying, exploiting, and reinforcing predisposed beliefs, before necessarily considering the quality or plausibility of the created disinformation. Cyber security expert Thomas Rid details that disinformation and propaganda, particularly of the cyber variety, has evolved to have the ability to target not only groups, but also specific individuals. This is illustrated during the DNC hack, when Russian hackers gained access to and exploited Hillary Clinton’s campaign chairman, John Podesta’s personal email account, and the attached 60,000+ emails.

41 Ibid.
43 Godson, 155.
44 Ibid.
Furthermore, even once the success of Russia’s threat was established, US domestic actors, such as the Trump campaign and later administration, the US government, the Intelligence Community, the media, and the general public, remained fractured and lacked collaboration. The schism between these actors is a national security threat in and of itself: Russia acknowledged and subsequently exploited this. While there is a long history of occasional tension between intelligence and policy in the United States, the “hostility between the incoming administration and the intelligence community is unprecedented”, with President Trump’s contempt towards the intelligence and media communities evident in his many tweets, statements, and interviews.47 Despite congressional and judicial efforts to investigate the nature of Russia’s exploits, the Intelligence Community has found that the relationship with its primary consumer, the President, has become strained with the inauguration of President Trump. Lack of communication, trust, and cooperation between various American actors and sectors appears to have adversely affected the US’s defensive and offensive counterintelligence abilities.

Lessons Learned

Based upon the successes and failures described above, several best practices of covert action and lessons learned in counterintelligence can be extracted from the Russian active measures in the 2016 US Elections.

Russian Covert Action

To be fully effective, covert action should be used as one of many policy tools in tandem with a larger, coordinated policy. Russia’s hierarchical government structure facilitated Putin’s efforts to easily expand active measures into multiple sectors. The subsequent coordination of these efforts resulted in a comprehensive influence campaign utilizing varied approaches that had the full weight of a unified government behind it. Moreover, in order to be an effective covert approach, propaganda and disinformation should carefully consider its target audience, and ensure the tradecraft necessary to keep sponsorship disguised. Russia, through its long-term research program and sheer scope of action, has effectively considered its audience, enabling various group and individual-leveled targeting to increase the odds of successful reception. While Russia failed to keep its sponsorship hidden, the leadership may ultimately deem this a tolerable cost, depending upon the extent of US retaliation.

**US Counterintelligence**

As much as the Russian intervention in the 2016 US elections was a Russian covert action success, it also highlights a US counterintelligence failure. The United States did not leverage essential aspects of strategic counterintelligence in either the defensive or offensive realms. This degraded the US ability to identify the intent and neutralize the consequences of a Russian cyber-based covert action operation. The lack of counterintelligence knowledge of, and ultimately action against, the Russian intervention stems from interdependent defensive, offensive, and communication vulnerabilities.

There is a need to improve security and cyber hygiene within political, federal, and private infrastructures. A defensive action that can render short-term results and enhanced resilience to foreign interventions includes improving security infrastructure to increase the odds of preventing cyber hacks, breaches, and attacks. Technical improvement of critical infrastructures will in turn enhance the efficacy of cyber hygiene behaviors: habits that may be as simple as utilizing a firewall, frequently changing passwords, and upgrading antivirus programs in order to improve a user’s overall security. Security aspects are often the first line of defense in cyber crime and attacks, and awareness of the necessity of computer hygiene is the first step in implementing security elements. Therefore, educating and increasing awareness within the public, private, and intelligence sectors will enable stakeholders to practice proper computer hygiene, identify and mitigate potential threats, and react effectively when a threat is established.

Such an approach necessitates close coordination, cooperation, and collaboration among relevant stakeholders in both the public and private sectors. In his written testimony to the Senate Select Committee on Intelligence in March 2017, Roy Godson details that historical precedence for such efforts already exists: the administrations of Presidents Truman and Eisenhower formulated a “national ‘whole of government’ and ‘whole of society’ political strategy to neutralize Soviet active measures from the late 1940s and on.” Furthermore, President Reagan sought to develop a strategic approach to counter Soviet active measures by “mobilizing an interagency effort,” which required a synergy between the President, Congress, and the Intelligence Community. The President initiated requests for and received support from Congress for the authorization and funding of increasing information gathering and analysis of Soviet active measures: these efforts were ultimately buttressed by the creation of an interagency

---

Active Measures Working Group, which was first based in the State Department, and later the United States Information Agency. Reinvigorating such efforts would further improve understanding of, resilience to, and ability to counter foreign influence campaigns.

However, due to contemporary socio-political fracturing and distrust among various institutions and actors—including the Trump administration, the Intelligence Community, the media, and the American public—communication and cooperation between US stakeholders is distinctly lacking. This lack of intercommunication between threat assessors and potential or realized victims was evident in the FBI’s two attempts, first in September and then in November 2015, to warn the DNC of a potential breach. Better paths of communication between these entities are necessary to ensure that when a breach or attack is identified, the proper stakeholders are clearly notified. This will also assist in mitigating “zero-day vulnerabilities,” unknown structural vulnerabilities in the code of software that are spotted and exploited by threat actors before the original developer realizes them.

An additional obstacle to improved inter-actor collaboration is the tenuous relationship between the US Intelligence Community and the private sector. It is paramount to improve the relationship and clarify responsibility between the public and private spheres in identifying and countering foreign threats that blend both overt and covert techniques. However, the ability to distinguish these responsibilities remains nebulous, as seen in the October 31st and November 2nd, 2017 Congressional hearings of Facebook, Twitter, and Google. Going forward, it will be necessary for the Intelligence Community to better inform the public of its pertinent mission and goals, to the extent possible, in an effort to build trust and understanding with private and public stakeholders. This is a prerequisite step in order to engage these actors in a cooperative manner to successfully anticipate and mitigate future disinformation campaigns. Strategically addressing the core mistrust, miscommunication, and lack of cooperation between relevant public and private stakeholders is a critical element of a whole of government approach, as schismatic predispositions have amplified the impact of Russian covert action while degrading American capacity for defensive protection and effective reactive abilities.

Finally, in order to mitigate future influence campaigns, there is a need for a structural change to US counterintelligence. The 2016 National Counterintelligence Strategy illustrates that while there is an evident focus placed upon security elements, a comparable public emphasis on the offensive capabilities of counterintelligence is lacking. For example, the word “security” is

---

51 Ibid.
53 Isaac and Wakabayashi. “Russian Influence Reached 126 Million Through Facebook Alone.”
stated 52 times throughout the body of the document, while “counterintelligence” appears only 8 times, of which defensive counterintelligence is stated 3 times, and offensive counterintelligence once. While solid security measures and practices are undeniably vital to national security, particularly with regard to malicious cyber activities, protection may only go so far, and must also be reinforced robust counterintelligence capabilities. The cornerstone of counterintelligence goes beyond security, to “engage and confront the adversary” in an offensive approach. Ultimately, it is necessary that US counterintelligence abilities are able to successfully identify intentions of malicious actors, assess the capabilities of threat actors to technically implement their intentions, and to act, with either covert action or offensive counterintelligence methods to stop, or mitigate those threats. As Roy Godson has stated, it is critical for the United States to be able to “anticipate—not necessarily predict—Russia’s likely future operations.” This will necessitate an increased vertical communication within agencies, as well as horizontal cooperation between Federal agencies and ultimately with the private sector. If the United States leverages its full weight into all aspects of strategic counterintelligence, both defensive and offensive, the odds of identifying and neutralizing the intent and implications of a Russian covert action threat will improve. These categories of improvement are critical elements to help mitigate the US counterintelligence vulnerability to future foreign influence campaigns and malicious cyber activity.

Conclusion

It is essential that US national security policy makers fully understand, appreciate, and act upon these lessons well before the next national elections, as Moscow will certainly apply its own lessons learned from this campaign towards “future influence efforts worldwide, including against US allies.” This assessment is already confirmed: actors likely associated with Russian civilian and military intelligence services continued to launch spearphishing campaigns just days following the 2016 Election. The threat to the integrity of US elections is genuine and needs to be effectively countered. This election operation signals a “new normal” in Russian covert

---

Note: Excluding page headers and titles.

“National Counterintelligence Strategy of the United States of America 2016.”


Godson. “Disinformation: A Primer in Russian Active Measures and Influence Campaigns.” Written Testimony to the Senate Select Committee on Intelligence, Open Hearing.”

ICA. iii.

Joint Analysis Report GRIZZLY STEPPE – Russian Malicious Cyber Activity. 3.
influence efforts as well as a broader foreign policy trend,\textsuperscript{60} and will need to be matched by a fully effective US counterintelligence apparatus.

\textit{About the Author}

Susanne Boss is a first year master's degree student in Georgetown University’s Security Studies Program, concentrating in intelligence. She currently works as a research assistant for Dr. James B. Bruce, Senior Political Scientist at the RAND Corporation and former Vice Chairman of the DCI Foreign Denial and Deception Committee in the National Intelligence Council, on an independent project regarding Russian active measures.

\textsuperscript{60} ICA, 5.
Roles and Missions of the Armed Forces and Civilian Control Mechanisms in Colombia: 1991-2016

Carlos F. Castillo

As the recently signed peace agreement between the government of Colombia and the Fuerzas Armadas Revolucionarias de Colombia (FARC) insurgency moves forward to the implementation phase, revisiting the role of the armed forces, as well as civilian control mechanisms, is needed for civil–military relations to adapt to the new transitional strategic environment – especially, given the ongoing political and institutional changes that could result in additional stress between civilian authorities and the military. In this paper, I compare the recent dynamics in civil–military relations in theory and practice, to discuss, assess, and inform decision-makers about the most prevalent challenges concerning the relationship between civilian authorities and the officer corps in the country. Furthermore, I argue that the ruling elites in Colombia have instrumentally used the armed forces through institutional and ideological control mechanisms, neglecting broad national security concerns and limiting the roles and missions of the different armed services. In this way, the government of Colombia has exercised a form of subjective control by matching their private interests with the martial values of the officer corps, and enabling the armed forces to effectively shape domestic politics.

Introduction

Civil–military relations in Colombia are embedded within the context of persistent civil war, coexisting with a functional but limited long-standing democracy controlled by traditional ruling elites—periodic elections, but only amongst a narrow elite, result in a continuously contested legitimacy of the political system.1 Due to Colombia’s strong tradition of civilian control of the armed forces, and in contrast to other Latin American countries, military coups have not been used as a recurrent means to achieve transfers of power.2 In fact, the only military coup in Colombian history, 1953, was partially authorized by civilian authorities as a political

---

1 Despite being one of the countries that has held more uninterrupted elections in the region, in practice only members of the traditional ruling elites are elected to office, and other democratic institutions like freedom of speech, assembly, free and independent press, or the liberty to create unions or protest have being curtail and repress over time. See: Bushnell, D. and Montilla. C. (2002) Colombia, una Nación a Pesar de sí Mism: de los tiempos precolombinos a nuestros días. Bogota Planeta. & Safford, F., & Palacios, M. (2002). Colombia: Fragmented land, divided society. New York: Oxford University Press.

solution to the previous bipartisan civil war. As such, the main concerns for the study of civil-military relations in Colombia’s atypical case have been related to the contested legitimacy of the government and the uncharacteristic military obedience to civilian rule (predominantly during the 1950s bipartisan violence), the question about military autonomy to address domestic security threats (since the 1960s until the rise of organized crime to the late 1980s), and to a lesser extent the role of ideology guiding the use of force as a policy instrument.

However, the existing, and very limited, research on contemporary Colombian civil-military relations has failed to consider the interplay of institutional and ideological mechanisms of civilian control, particularly since the enactment of the 1991 Colombian Constitution, as well as how the use of the armed forces for political purposes has affected the way roles and missions of the military are conceived. As the government and the Fuerzas Armadas Revolucionarias de Colombia (FARC), the main insurgent organization in the country, move forward with the implementation of a peace agreement signed in November 2016, there is an urgent need to update the understating of the politics of both recent and current civil-military relations in the country in order to cope with the upcoming changes in the strategic environment—from active warfighting against an insurgency, to maintaining security and stability during a political transition.

Therefore, in this case study I compare the institutional civilian control mechanisms in the standing legal framework with the civilian designation of missions in practice, drawing examples from the five presidencies since the enactment of the 1991 constitution. I will argue that civilian control through a strong central presidential system has effectively ensured that the armed forces perform designated tasks without challenging civilian authority. Furthermore, I will also argue that the military, despite high levels of professionalization, has shaped domestic politics due to the primarily internal nature of Colombia’s security threats—which prevents the existence of objective neutrality. Finally, I will detail how the new professionalism, or the

---


5 The Colombian Government and the Fuerzas Armadas Revolucionarias de Colombia (FARC) reached in 2016 an agreement after four years of negotiations. In late November, both chambers in congress ratified the agreement for implementation.
expansion of the traditional role of external security of the military in practice, has led to the instrumental use of the armed forces by the ruling elites in a context of contested legitimacy of the existing constitutional order.\(^6\)

To support these claims, I will first briefly revisit the recent history of civil-military relations in the country, to contextualize the current interplay of regulatory frameworks and the actual decision-making processes concerning the designation of military missions, and to describe the standing civilian control mechanism—or, the institutional rules and procedure by which control over the military is deferred to civilian authorities. I will mainly focus on the implications of the tacit pact between the military and the traditional ruling elites after the civil war of 1948 to 1953, as well as how the military assistance and training provided by the United States (US) since the 1960s has affected the professionalization of the Colombian armed forces. The second section will revisit the 1991 constitution, as it is the current legal framework for the institutional civilian control mechanisms. The third section discusses the current state of civil-military relations by drawing examples from the five presidencies since the enactment of the 1991 constitution. And finally, the last sections will conclude by stressing Colombia’s future challenges in light of congressional approval of a peace agreement with the FARC in late 2016,\(^7\) as well as by revisiting the most important trends in civil-military relations during the past two decades.

### A Brief Note on the History of Civil-Military Relations in Colombia

The civil war of the 1940s and 1950s, between the ruling conservative party and a liberal party-led insurgency known as *La Violencia* (1948-53), ended with a coup staged by General Gustavo Rojas Pinilla in 1953, followed by a short authoritarian regime partially endorsed by the ruling elites of both parties—mainly, because of their failure to achieve a decisive outcome in the war. After four years of military rule, General Rojas pacified the country, offered amnesty to the Liberal rebels, and returned power to civilian authorities in 1957-58.\(^8\) A shared power solution was agreed, known as *El Frente Nacional*, in which both parties would alternate the presidency

---

\(^6\) For further reference on the concept of new professionalism in other presidential Latin American political systems (Peru and Brazil) see Stepan, A. (1973). The new professionalism of internal warfare and military role expansion. In A. Stepan (Eds.), *Authoritarian Brazil* (pp. 47-65). New Haven CT: Yale. For an example on the role of ideology in Colombian civil-military relations see Avilés (2006). And, for further reference regarding the enduring state of contested legitimacy in Colombia, or competing visions of what the legitimate constitutional order is, and its effects on civil-military relations see Watson, C. (2000). Civil-military relations in Colombia: A workable relationship or a case for fundamental reform? *Third World Quarterly*. 21 (3), 529-48.

\(^7\) The Colombian Government and the Fuerzas Armadas Revolucionarias de Colombia (FARC) reached in 2016 an agreement after four years of negotiations. In late November, both chambers in congress ratified the agreement for implementation.

for sixteen years, suggesting that the military was not seeking to permanently replace the civilian authorities. The military was given this position of power during the final stages of the war because the elites in both parties felt that it was the only way to break the unsustainable stalemate. Meanwhile, the subsequent and rather peaceful transition back from military rule, hinted an enduring ideological match between military doctrine and civilian authority interests.\(^9\)

In May 1958, after years of domestic unrest and a short-lived military dictatorship, president Alberto Lleras Camargo proposed during his inaugural speech an “informal pact” with the armed forces that has since shaped contemporary civil-military relations in Colombia.\(^10\) President Lleras’ proposed pact was born out of the significant role played by the armed forces in domestic politics during the civil war. During the bipartisan civil war, by convincing the armed forces that their corporate interests would only be safeguarded under conservative rule, the conservative party was able to transfer its ideological views to the officer corps and use the military instrumentally against their liberal adversary. Hence, by using ideological indication as a control mechanism to portray the liberal party as an existential threat to the military institution’s values and traditions, the conservative government justified brutal and unlawful tactics that included the targeting of the civilian population.\(^11\) President Lleras’ pact recognized the counterproductive effect of the over-politicization of the military during the civil war and sought to prevent this from happening again.\(^12\) Thus, the pact granted the military substantial autonomy to conduct national security policy, including control over the Defense Ministry, in exchange for the armed forces stepping aside in bipartisan politics.

Despite military isolation from bipartisan politics, after La Violencia and the subsequent military regime, new threats to the private interests of traditional ruling elites emerged, and the use of ideology continued to be a recurrent tool of instrumental civilian control.\(^13\) The shared power agreement, mentioned above, unified the elites but excluded the wider population, including part of the liberal rebels in the countryside that had refused to take the amnesty offer. These rebel factions were peasant guerrillas claiming autonomy in the absence of political representation and had no initial ties to international communism, nor a shared the agenda of

---


\(^10\) Cepeda, F. (2003). Poder civil y poder militar. In F. Cepeda (Eds.), Las relaciones cívico – militares en tiempos de conflicto armado (pp. 21-68). Bogotá, Colombia: Embajada de los Estados Unidos y FIP.


\(^13\) Instrumental use of the armed forces by the civilian authority, trough diffusion of ideology to match military values with ruling elites interest and preferences, is consistent with Samuel Huntington’s description of subjective control in civil-military relations.
the Clandestine Colombian Communist Party (PCC) of taking power from the traditional ruling elites.\textsuperscript{14} However, as they fought the US-backed Colombian military, the rebels merged with the PCC and adopted the name Fuerzas Armadas Revolucionarias de Colombia (FARC) in 1964.\textsuperscript{15} Thereafter, ruling elites saw the insurgency as a potential challenge to their shared power arrangement, and sought to portray any sort of social mobilization seeking representation or a more fair and inclusive socioeconomic and political model as a linked issue to the spread of communism. This thus effectively pulled in the United States as an external patron by American foreign policy, the contention of communism, with the Colombian government interests, regime survival of the ruling elites.\textsuperscript{16} Reframing the political confrontation, which was initially a disagreement concerning the inclusiveness of the political and economic systems, in terms of the great power politics of the Cold War era during the 1960s, reduced the likelihood of reaching new political agreement and prolonged the violence for decades.

Therefore, the ruling elites crafted a military doctrine to protect their privileged access to power and were very eager to accept US military assistance, training, and ideology. Evidence of this dynamic can be found in the fact that during the Cold War era, Colombia sent the largest number of officers to the School of the Americas, a controversial training facility with a heavy ideological taint, and became the main recipient of US military assistance in the region.\textsuperscript{17} Similarly to what happened during \textit{La Violencia} in respect to conservative ideology, during the early Cold War period the ruling elites transferred anticommunist thinking into the armed forces through a mixed formula of ideological indoctrination and institutional controls, which reinforced each other, and tied together the martial traditions of the military with the traditional


\textsuperscript{15} The joint Colombia-US military offensive known as Plan Lazo was conducted within the framework of the Alliance for Progress. A bilateral understanding, part of the US containment doctrine, signed with the Kennedy administration in 1961. In 1964, the rebel held territories were bombed, US Napalm was used (the Marquetalia bombing). See: Pizarro, E. (1991). \textit{Las FARC: De la Autodefensa a la Combinación de Todas las Formas de Lucha}. Bogotá, Colombia: Universidad Nacional de Colombia Instituto de Estudios Políticos y Relaciones Internacionales.


\textsuperscript{17} The School of the Americas is a US training facility located at Fort Gulick in the Panama Canal from 1946 to 1984. During the Kennedy administration, it was tasked with the mission to train Latin American armies in counterinsurgency as part of containment policy to avoid another revolution like the one in Cuba (1959). In 1984, the school was moved to fort Benning, Georgia, and Fort Rucker, Alabama (helicopter school). See: Gill, L. (2004). \textit{The school of the Americas: Military training and political violence in the Americas}. Durham and London: Duke University Press. & Latin American Working Group. (2013). \textit{Time to listen: trends in U.S. security assistance to Latin America and the Caribbean}. Washington DC: LAWG. Retrieved from http://www.lawg.org
ruling elites interest to stay in power—indefinitely. Since, the government has used the military to suppress the insurgency, along with any kind of social mobilization or political opposition that has challenged their privileged access to power.

Consequently, the Colombian military’s roles and missions have focused exclusively on domestic security threats to the traditional ruling elites. These threats have mutated and evolved over time, making it difficult to confine them within a single analytical framework. Broadly speaking, they have been broken down into three categories or stages: communism (until the late 1980s), leftist narco-guerillas and organized crime (since the 1990s), and insurgent terrorism (after September 11, 2001).

Methodological Note and Conceptual Framework

I use a simple within case comparative approach to contrast the standing legal and institutional framework for civilian control and mission designation of the military in Colombia with the actual political process by which civilian decision-makers exercise their authority over the armed forces. This was done mainly to determine if the roles and mission of the military in practice correspond to those established by the legal framework and if civilian authorities are sticking to the established institutional control mechanisms or appealing to alternative forms of ideological indoctrination. Hence, I can assess if civilian control and mission designation occurs within the boundaries of the legal standards, or if there are other political drivers affecting the way the military is used as a policy tool.

To achieve this objective, I apply a qualitative content analysis methodology to compare the standing legal framework with an episodic record of the interactions between civilian authorities and the officer corps. Content analyses encompass the possibility to observe the evidence of social interactions amongst actors, civilian authorities, and the officer corps in this case in the residual documentation left behind by such an exchange. In this particular case, I use this methodology to account for variation across the same unit over time—Colombia over a 25-year period.

In the following section I revisit primary regulatory sources, such as legal rulings, articles from the 1991 constitution, and amendments, to establish a baseline understanding of how civilian control and mission designation should work in theory. In the subsequent section, I go

---

through official documents, reports and statistics, media outlets, available scholarly research, and personal communications to determine how civil-military relations work in practice, and if civilian control and mission designation are concomitant with the standing legal framework—or not.

To guide the assessment of the effectiveness of civilian control in Colombia—a country characterized by a strong presidential system, the lack of the armed forces neutrality despite professionalization, and the link between expanded roles of the military and their involvement in domestic politics, I consider two conceptual frameworks for the discussion concerning the current state of Colombian civil-military relations: Feaver’s (2003) principal-agent model, and Stepan’s (1973) new professionalism concept. Feaver argues that civil-military relations can be described as a relationship between principals (i.e. the president or the legislature) hiring an agent (the military) to fulfill a role and perform set or tasks. However, this contractual relation is mediated by information asymmetries that create both an adverse selection and moral hazard problems. The adverse selection problem refers to the uncertainty the principal has about the true “preferences or capabilities” of the agent—for example, a newly elected president not having complete information about the interests of an officer she or he chooses to promote. The moral hazard problem refers to the behavior of the agent once it has been employed. As the principal cannot truly observe the employee at all times to ensure that tasks are being performed as intended, the agent has an incentive to only partially fulfill with the contract, or complete tasks in a manner that satisfies its own interest—for instance, a general choosing to report back incomplete or misleading information regarding the implementation of a defense policy.21 Stepan, on the other hand, suggests that in cases where security threats to the standing regimes come from within the country—like in Latin American countries—the principals (i.e. presidents, military juntas, dictators, legislatures) have political and ideological incentives to expand the traditional role of the armed forces away from external security—as it is intended in the normative theories of civil-military relations (Huntington’s approach).22

I use Feaver’s (2003) principal-agent model of civil-military relations to discuss whether the presidential system stated in Colombia’s 1991 constitution has been able to ensure military compliance from a functional and relational standpoint. Put in terms of Feaver’s model, I assess whether the officer corps (the agent) performs its designated tasks and abstains from challenging civilian authority (the principal). I use Stepan’s (1973) expanded role conceptualization, or new

---


professionalism, to assess whether existing legal regulations actual limit the scope of the armed forces’ roles and missions, or whether civilian authorities have been able to use the military instrumentally to shape domestic politics in accordance with their private interests of excluding potential political competitors—hence, finding a convenient justification in the internal nature of the security threats to widen the range of the use of force as policy option beyond legal regulations. Contently, resulting in an instrumental form of subjective control that prevents the armed forces from remaining politically neutral.23

Overall, the most prominent research on civil military-relations during political transitions has focused on cases of state transformation or regime change (in Latin America usually after military rule), see for instance Barany (2012) and Loveman (1994).24 However, the case of Colombia, a protracted armed conflict with a negotiated settlement and no regime change, is certainly a valuable and perhaps infrequent study case for the advancement of applied civil–military relations theory.

The 1991 Constitution: Normative Framework and Institutional Mechanisms for Civilian Control

The Colombian constitution envisions the military as a politically neutral and professional force, under what Samuel Huntington would describe as objective control.25 The armed forces should not be decisive in any political process, except those directly related to the services or the “martial morality” of the military itself—or, the moral standards of the military conduct. The officer corps shall not engage in any political activity related to any party or politically motivated movement, unionize, or vote as long as they are active members of the military. Members of the armed forces cannot be political appointees or be elected to hold any office. Officers must take an oath swearing to defend Colombian sovereignty, territory, and above all, the constitutional order.26 Therefore, the military is constitutionally bound not to

---

question civilian authority or the established political system that has kept traditional ruling elites in power, even if governments are oppressive, ineffective, or promote undemocratic practices.\textsuperscript{27}

\textit{Roles, Missions and Force Structure of the Colombian Armed Forces}

Under the Constitution, the military and the police fall into the categories of traditional war fighters/defenders in advanced established democracies.\textsuperscript{28} The security forces in Colombia are comprised of the military (Army, Navy, and Air Force) and the national police—there are no local civilian polices forces. By constitutional mandate, the military’s main role is to conduct warfare abroad and to defend the “sovereignty of the nation” at the borders from external threats, while the police, characterized as a “permanently armed” and centralized force, are charged with overseeing domestic law enforcement exclusively. No explicit mention of potential external threats is made in the constitution.\textsuperscript{29} In practice, the militarization of the police has blurred the distinction of the roles and mission for each service, and the internal nature of the security threats has led to the military’s permanent involvement in domestic affairs.

The Colombian military and the police are composed of both volunteers and conscripted men.\textsuperscript{30} Every male national is eligible for conscription and every Colombian must take up arms when necessary to defend the national independence and the state institutions.\textsuperscript{31} Conscripts can serve as regular enlisted soldiers in the army (between 18 to 24 months), high school draftees (12 months) in the Army or the police, or as peasant soldiers in the army.\textsuperscript{32} No conscripts serve in the Navy or Air Force. In peacetime, there are several exceptions to mandatory military service.\textsuperscript{33} In this regard, internal armed conflicts or civil wars do not count as an official declared war with another country, so the peacetime exceptions apply and a compensation tax must be paid if a

\textsuperscript{27} Certainly, a significant difference from the legal framework that regulates civilian affairs, which enables private citizens to rebel and resist oppressive rule if necessary. In Colombia, the act of rebellion is considered a right and simultaneously a political crime. If civil resistance and civil disobediences is not conducive to violence or other crimes, like war crimes or human rights violations, it cannot be prosecuted in the same terms that regular crimes. See: Corte Constitucional [C.C] [Constitutional Court], diciembre 2, 2010 (2012), Sentencia C-986/10, Relatoría de la Corte Constitucional [R.C.C]. Retrieved from http://www.corteconstitucional.gov.co/relatoria/2010/C-986-10.htm
\textsuperscript{30} The officer corps is made up exclusively from volunteers.
\textsuperscript{32} Peasant soldiers are entitled to a loan for agrarian development after they are done with their service.
\textsuperscript{33} Women and minors (under 18) can volunteer for enlistment, the later with written authorization of its parents, but in both cases with restrictions regarding combat roles.
male is exempted from mandatory service. As Colombia has not been in an international war since 1991, the military has enjoyed a budgetary surplus from conscription waivers, or slack, that is usually more valued by the officer corps than the marginal gain of extra conscripts.

Currently, Colombia has the second largest armed forces in the region (446,000), second only to the United States. The Army is the most prominent and best financed of the services, with 120,000 volunteers, 80,000 conscripts, and 30,000 support personnel (Navy, 35,000; Air Force, 14,000; Police, 167,000). The main civilian intelligence agency, Departamento Administrativo de Seguridad (DAS), was disbanded because of human rights abuses in 2011, de facto leaving all intelligence gathering activities to the military and the police.

To enhance the combat effectiveness of army units, a professional soldier force of volunteers was established in 2000 for those conscripted men who want to continue to serve after their mandatory time is over (additional schooling and training is provided to improve professional soldiers into elite shock-troops). The officer corps in all services is made up of volunteers trained in military academies, and the Army established a specialized training school for non-commissioned officers. There are no officer educational programs in place within any civilian college or university, which has helped to maintain a gap between military values and civil society, resulting in a further isolation of the armed forces that facilitates ideological indoctrination by the ruling elites.

---

34 Peace time exceptions to mandatory services includes: the clergy, convicted criminals, single children, orphans in charge of the household livelihood, the brother or son of service men or officer who has been killed or injured in action, students in college, handicap male population and merry men who do not want to volunteer for service – in practice conscription law applies to young, single, unemployed high school graduate without the means to go to college. Ministerio de Defensa Nacional (1993). Funciones organismos de reclutamiento. Retrieved from Comando de Reclutamiento https://www.ejercito.mil.co/www.reclutamiento.mil.co/


37 A new civilian intelligence agency was created but it has been very ineffective in practice. The deferral of all intelligence gathering to the military has also impacted civil-military relations. Ruling elites have used the intelligence agencies to spy on the political opposition, while the military have specialized in tactical and operational level counter-insurgency intelligence gathering—cases of unlawful espionage on critics of the military, human rights activists and opposition leaders are not uncommon. Further research in this regard is required.


Mechanism of Civilian Control

The Colombian constitution establishes a dual principal system, the Presidency and Legislature, for civilian oversight over the armed forces. The Presidency, as an institution and main civilian authority for oversight, is the commander in chief of the Colombian military with the following functions: “do as he/she sees fit” with the armed forces (strategy making), choose all officers for promotion (contingent upon Senate approval), ensure or re-establish public order within the national territory, defend the national borders, declare war (with Congressional approval), and “direct war operations whenever he/she esteems necessary.” Congress oversees incentives such as the fixing of wages for all military personnel and approving all the promotions for officers selected by the president. Public budgets for all policy sectors, including the defense budget, are allocated by the executive branch and approved by Congress. After the constitution was adopted, the armed forces retained a centralized command and control structure based on a traditional presidential system (see Figure 1).

Figure 1: Command and Control Structure of the Colombian Armed Forced

- Institutional reform was not discussed during the peace negotiations. However, this institutional innovation was created as a response to future strategic needs.

The most recent regulatory framework in Colombia is consistent with the Latin American trend of emphasizing presidential control in matters of civil-military relations.\textsuperscript{43} The Ministry of Defense, chaired only by civilians since 1991, is the president's deputy office in the management of the military establishment and security policy-making. Additionally, the president has the constitutional prerogative to declare states of emergency to gain transitory executive powers and enact new laws, or temporarily suspend existing legislation, including regulations that apply to the armed forces.\textsuperscript{44} These transitory powers, which also include enforcing martial law and limitations on due process, are deemed to be under direct oversight of the Congress. However, the legislature has frequently deferred judgment to the presidency regarding the suppression of civil rights when states of emergency are declared.\textsuperscript{45}

Lastly, recent legal developments have established the judiciary as an additional, and perhaps more formal, constitutional mechanism of civilian oversight—although military tribunals are not entirely new. According to a 2015 amendment to the constitution, military tribunals will only prosecute crimes by active members of the armed forces that are related to the military service. Crimes related to the internal armed conflict, human rights violations, or war crimes will be prosecuted by the civilian justice system or by special military justice tribunals with independent judges from the armed forces command and with proven expertise in international humanitarian law.\textsuperscript{46} This amendment was the result of a legal compromise between human rights activists, who pushed for more oversight given the less than desirable human rights record of the Colombian armed forces, and the government, who wanted to safeguard the military establishment since it is a key policy instrument for the ruling elites. Yet, the legitimacy of special military tribunals is frequently questioned by civil society organizations, which claim they would lack the necessary independence to prosecute human rights and war crimes cases.\textsuperscript{47} Nonetheless, transnational networks of human rights activists and non-governmental organizations have managed to use international pressure through third-party states, like the United States or the European Union (EU), to empower the judiciary in Colombia to effectively

restrain the military from tactical or operational practices that are contradictory with human rights standards.  

Contemporary Civil-Military Relations in Colombia

In practice, civil-military relations in Colombia have not been fully concomitant with the standing legal framework. Although the primacy of the presidency as a strong principal has remained, over the past five administrations the roles and missions of the army and the police have been blurred and intertwined, ideology has been used as an important but informally institutionalized mechanism of civilian control, and congress has become rather inconsequential to decisions regarding military expenditure. Hence, realizing the ideal standards of objective and neutrality has been rather impossible, as the ruling elites found compelling incentives to instrumentally use force against domestic threats. However, the recent peace process with the FARC might constitute an opportunity to further security sector reform, including the considering the reframing of civil-military relations, and the role of the military.

The Gaviria (1990-94) and Samper (1994-98) Administrations

Despite the enactment of a new constitution in 1991, the roles and missions of the Colombian armed forces have not matched constitutional regulations, and professionalization has been contingent on domestic security issues. In practice, the armed forces fulfilled a nontraditional mission. The police became highly militarized to face organized crime and the military spent much of their time focused on internal security and counterinsurgency operations rather than on external threats.  

For instance, during the Gaviria and Samper administrations (1990-94 and 1994-98), a special police task force, known as the Search Block, was upgraded with military training and capabilities to face organized crime. This unit was created specifically to counter the Medellin Cartel, which had created a governability crisis by using widespread terrorism tactics, including high profile kidnappings and bombings, undermining the government’s ability to protect its most valuable supporters within the privileged social class. Similarly, during the Samper

50 The Search Block was officially created in 1992 with the assistance of US Special Forces. During the 1990s, the Medellin Cartel sought to retaliate against the members of the upper classes, from where ruling elites come form, after government approved an extradition treaty with the US. See: Alvarado, A. (2010). The Militarization of
administration, the Cali Cartel managed to corrupt the 1994 presidential election campaign causing the resignation of top members of the cabinet.\textsuperscript{51} After the corruption scandal, the government’s priority was targeting the Cali Cartel leaders that had been linked to the administration, seeking political redemption and effectively conditioning the mission of the armed forces to the ruling elites’ interest of regaining the lost legitimacy.\textsuperscript{52}

Another persistent trend since the early 1990s was the Congress’ unwillingness to push back against the presidency’s decisions on defense budget allocation, mainly because both principals represented the same narrow segment of the civil society—the traditional ruling elites. This is an unusual feature when compared to other policy sectors where budget allocation is frequently the result of exhaustive negotiations between the executive and the legislature.\textsuperscript{53} The legislature’s lack of willingness to challenge defense expenditure decisions underscores how politicians leading both institutions shared concerns for the same threat—drug cartels in 1990s and, more recently, the FARC insurgency. The result was a cumulative and unrestricted increase in defense spending throughout the last two decades (see Figure 2).

During this early period, however, civilian authorities prioritized budget allocation to ensure the security of their supporters in the cities and neglected the growing insurgent groups in the countryside. Simultaneously, the army’s corporate interests became secondary to policymakers, as they prioritized police militarization as their main tool against organized crime—the army jurisdiction was tacitly limited to rural areas, it had a limited role in countering organized crime, and its funding was not as prominent.\textsuperscript{54} This political and instrumental use of the armed forces to protect political support in the cities undermined democratic institutions, outsourced rural security to private armies in the service of organized crime and landowners (wrongly referred to as paramilitary groups), and prevented the successful implementation of a


\textsuperscript{52} The Search Block is the predecessor to the contemporary joint police and army GAULA anti-kidnaping and anti-extortion units. Two types of security threats that affect mostly the upper social classes, which have the power to influence decision-makers to prioritize defense resource allocations and mission assignments.


nationwide security policy. Mainly, because the narrow focus of the security policies left significant portions of the territory in an institutional vacuum, where the only state presence was a weaken and frustrated military fencing a growing insurgency, which found an incentive to tolerate and collude with the paramilitary militias—circumstances that combined with the little political will for civilian oversight to result in increased corruption, violence, lawlessness, and recurrent human rights abuses.

Figure 2: Colombia Defense Budget

- The Colombian Congress has traditionally deferred judgment to the executive branch and rarely abstains from approving defense budget allocations.
- Despite the Plan Colombia funding, congress has allowed an exponential growth of defense budget.
- US military assistance has a been essential for sustaining civilian instrumental control.
- Military assistance has varied according to Colombia relevance in US domestic politics agenda during the different US administrations (war on drugs or human rightist) – a new post conflict stabilization assistance package, “Paz Colombia”, has been approved by the US Congress.
- Although the defense budget has decreased in the last two years, because of the ongoing peace negotiations, the government continues to have an incentive to allocate significant amounts of resources to face post-conflict security threats and ensure the armed forces do not turn into active spoilers during the peace agreement implementation.

Source: World Bank data and Security Assistance Monitor

Disagreements between civilian authorities and the armed forces command regarding the possibility of reaching a negotiated solution with the FARC insurgency during this period illustrate how military corporate interests were affected during the 1990s. For example, in 1997 the Armed Forces Commander, General Harold Bedoya, had a public quarrel with President Samper about granting the FARC a demilitarized zone for engaging in peace negotiations. This resistance was not unprecedented and suggested that the military was aware of the...

shortcomings of the overall security strategy and knew how underfunded and ill-equipped they were compared to police units targeting organized crime. These disagreements added to the lack of legitimacy of the Samper administration, which was under scrutiny by the judicial authorities on accounts of its alleged financial connection with the Cali Cartel—several top advisers of the president including the Defense Minister Fernando Botero were found guilty in this investigation,\(^57\) and could have evolved into more aggressive forms of resistance by the military if they had found more support within the opposing conservative party.\(^58\)

Other instances of the military attempting to resist civilian control and defense polices could be observed in the way orders and operation were executed. For example, while the new constitution was being drafted in 1991, the army launched a surprise attack on the FARC rebels seemingly without clear authorization form the government, known as the Casa Verde Attacks. Although President Gaviria had authorized the use of force, he was unaware of the time and location of the attack. The assault effectively ended the failed 1980s peace negotiations and generated tensions with the left-wing sectors at the constitutional assembly.\(^59\) Nonetheless, cases of military resistance to civilian control have been very infrequent and were motivated by personal ideological stances, corruption, or the imbalance of resource allocation across services. In this case, by launching an unauthorized attack the army leadership was making an unspoken statement about the peace process and the participation of former rebels in the constitutional assembly—a political space from which the military was excluded. Yet, it was not an attempt to completely overturn civilian control over the armed forces.\(^60\) In most cases, commanders have been easily replaced to make sure that their preferences match the presidency’s vision of what constitutes a threat, regardless of the effectiveness of the security policies.\(^61\)


\(^{60}\) The Casa Verde attacks ended the negotiations conducted in the 1980s in La Uribe, Meta. Also, a few years before the enactment of the 1991 constitution, the army high command issued a public statement rejecting the possibility of amnesty for the rebels as part of the 1984 La Uribe negotiations. EPL and M19 former combatants, amongst members of other demobilized insurgencies, war part of the 1991 constitutional assembly.

The Pastrana Administration (1998-2002)

Modernization and professionalization of the armed forces did not start until the Army’s shortcomings were self-evident, and the ruling elites felt threatened by the rise of the insurgency. As already mentioned, professionalization of the officer corps in Colombia has been highly influenced by what Alfred Stepan has called new professionalism, or a particular focus on expanded-role counterinsurgency doctrine adopted from US military assistance and training since the Cold War era (and more recently counterterrorism). Once socialized into the whole of the armed forces, the new professionalism facilitated ideological indoctrination as a non-institutional mechanism of civilian control. This mechanism was reactivated during the late 1990s, when the focus of the security policy shifted as the civilian authority became aware of a rising insurgent offensive and sought to match its own private interests of political survival with the officer corps’ enduring martial values. The army welcomed this new policy shift, away from an overemphasis on police militarization to counter organized crime, because it helped its corporate interests by obtaining an overwhelming amount of funding, training, equipment, and autonomy.

---


Table 1: New Professionalism in Colombia

<table>
<thead>
<tr>
<th></th>
<th>New Professionalism</th>
<th>Colombia</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function of the Military</td>
<td>Internal security</td>
<td>Yes, no external threat</td>
</tr>
<tr>
<td>Civilian attitudes</td>
<td>Segments of the society challenge</td>
<td>Insurgency, social movements, activists, opposition political parties,</td>
</tr>
<tr>
<td>government</td>
<td>government legitimacy</td>
<td>communal organization, interest groups (e.g. labor union, ethnic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>organizations, victims’ organizations)</td>
</tr>
<tr>
<td>Military skill required</td>
<td>Highly interrelated political and</td>
<td>Counterinsurgency, interdiction, law enforcement, internal patrolling and</td>
</tr>
<tr>
<td></td>
<td>military skills</td>
<td>policing</td>
</tr>
<tr>
<td>Scope of military</td>
<td>Unrestricted</td>
<td>Humanitarian relief and nation building. The military is usually the only</td>
</tr>
<tr>
<td>professional action</td>
<td></td>
<td>institution in remote or conflicted areas (de facto replacing other</td>
</tr>
<tr>
<td></td>
<td></td>
<td>civilian state institutions).</td>
</tr>
<tr>
<td>Impact of professional</td>
<td>Politicizes the military</td>
<td>The military actively shapes domestic politics by defending the existing</td>
</tr>
<tr>
<td>socialization</td>
<td></td>
<td>institutional order from those who question its legitimacy from within.</td>
</tr>
<tr>
<td>Impact on civil-military</td>
<td>Contributes to political managerial</td>
<td>Civilian authority is not representative of social sectors. Ruling elites</td>
</tr>
<tr>
<td>relations</td>
<td>and role expansion</td>
<td>instrumentally uses the military through institutional and ideological</td>
</tr>
<tr>
<td></td>
<td></td>
<td>control mechanisms (match between private interests and new professionalism</td>
</tr>
<tr>
<td></td>
<td></td>
<td>martial values).</td>
</tr>
</tbody>
</table>

The increase in US military assistance through the Plan Colombia (1999) was crucial for strengthening civilian control, as it offered the military a new pool of resources and ensured a set of preferences aligned with the ruling elites. It also enabled the United States to constrain the missions of Colombia’s armed forces as a condition of receiving military assistance. In this regard, the Colombian government linked US anti-drug policy with the FARC rebels, who controlled about 40% of the cocaine production, to upgrade the Colombian military forces for counterinsurgency missions.65

The drug cartels had ceased to be the main threat to the ruling elites, while rebels continuously ambushed army units, blocked roads, conducted kidnappings, attacked military strongholds, destroyed critical infrastructure, and controlled some of the territories surrounding

65 FARC’s cocaine trade participation estimate can be done by overlapping the areas with coca crops with the territories controlled by the insurgent organization.
Thus, in order to revive US interest in supporting counterinsurgency operations, political elites drew the connection between the FARC rebels and transnational organized crime. This meant that for the United States to remain committed to shaping the Colombian military into a highly mobile force—capable of conducting search-and-destroy operations with enhanced intelligence technology and precision bombing capabilities—narcotics interdiction missions had to be regular undertakings. In practice, the military became an unprecedented policy tool for the Colombian ruling elites to use against their adversaries, even though it had little effect on illicit drug exports.

Regardless of the effects on anti-drug trafficking enforcement, this military assistance program helped the Colombian government revitalize anti-communist sentiment and reframe the insurgency threat. Mainly, suggesting the insurgency, as well as any social resistance movement that challenged the status quo of the political system, fell into a single category of narco-terrorist organizations. It also changed military doctrine to fit the US principles of jointness—or inter-service cooperation for the military process, technological dependency at the operational level, and reliance on close air support tactics.

Almost simultaneously, the failure of the El Caguán peace negotiations between the Colombian government and the FARC (1999-2002) and the rise of paramilitary groups created new tensions for civil-military relations and exposed the limitations of civilian control. The lack of meaningful advances in the negotiations led to President Pastrana’s renewal of the demilitarized zone on several occasions, which in turn resulted in the resignation of the defense minister and sixteen generals. Despite the public act of defiance, their resignations were not accepted and the armed forces never challenged the ceasefire with the FARC rebels.

During this period, collaboration between the wrongfully labeled paramilitary groups and the armed forces was not unusual. The paramilitary groups defended the private interests of

---


68 After fifteen years of the Plan Colombia, 90% of the US cocaine continues to come from Colombia and the average price of the same drug has dropped 70%. See: UNODC. (2015). *Colombia monitoreo de cultivos de coca 2014*. Bogota: United Nations Office on Drugs and Crime. Retrieved from http://unodc.org


70 Paramilitary groups in Colombia were comprised by former associates of the drug cartels and traditional landowners that had a vested interest in sustaining an unequal structure of ownership of the land in the countryside for political and economic reasons. They were heavily involved in drug-trafficking, share a common enemy with the national government (the FARC rebels that promoted land reform and sought control over the cocaine business) and adopted a right-wing ideology to indoctrinate their death squads in contraposition to the insurgency. See:
regional elites in control of local governments and were heavily involved in drug trafficking. They coopted a significant percentage of the national legislature in the early 2000s and have been linked to Pastrana’s successor, President Uribe, his family, and his political associates—which came from these provincial political elites. Because the paramilitary groups shared a set of common interests and values with these provincial or regional political class, some units within the armed forces were incentivized to cooperate with these criminal organizations against any adversaries that challenged the traditional elites’ access to power, including rebels, human rights activists, social leaders, journalists, labor unions, students, and demonstrators. Several high-ranking officers and politicians that served between the mid-1990s and 2006, when the paramilitaries were disbanded, have been prosecuted and found guilty of collaboration with this illegal armed group.

What remains certain, irrespective of the illegal commands civilian authorities issued to the officer corps, is that at least several administrations chose not to restrain the armed forces from engaging in questionable human rights practices and promoted a tacit tolerance of paramilitary groups. Turning a blind eye to paramilitary groups allowed the ruling elites to establish an extra, yet unlawful, line of defense against the FARC insurgency—an effective tool to keep in place a highly exclusionary political system.

The Uribe Administration (2002-2010)

The security crisis of the late 1990s led to civilian micromanaging of the military at the operational level and more intrusive methods monitoring officer corps performance. In 2002, President Uribe’s administration (2002-10) declared a state of emergency, started to demand periodic quotas of FARC rebels’ casualties from the military without a clear definition of the desired political outcome, and openly depicted opposition members, activists, and critics as terrorist collaborators.

---


The Uribe administration represents one of the most severe examples of instrumental civilian control through institutional and ideological mechanisms. According to an activist from an international human rights advocacy organization observing the situations in Colombia at the time, it was not unusual for officers to receive phone calls from the President himself to pressure the units in the field and reward those who reported the most rebels killed in action. This ideologically charged stigmatization led to several instances of human rights violations, including the False Positives Scandal in which thousands of unarmed civilians were executed and later dressed as rebels and reported as combat casualties (see Figure 3). Publicly dismissing or replacing officers that did not produce the desired results (or agree with his ideological stance), interfering in the planning of military operations, as well as personally keeping records on field officers’ performance were common types of punishment meted out to those within the armed services who did not comply. Simultaneously, Uribe reframe both the FARC and all other forms of nonviolent civic resistance within a single narrative of presumed supporters of terrorism. Uribe instrumentally used US foreign policy—The War on Terror—to justify the enactment of special presidential powers by Congress, and to abuse power towards his contradictors. This resulted in an increase of violence against journalists, activists, and social movements, as well as the systematic practice of illegally taping the communications of judges and members of the opposition—recurrently, activities that were enabled or tolerated by the military, including the police, as well as the intelligence agencies. Clearly, this was a deviation from the established roles and missions for the military by the constitution.

75 Activist (2016, November 7). Personal interview on civil-military relations on Colombia.
Even though the prevalence of the presidency as the main principal for civilian control never eroded, the Uribe administration marked the beginning of a much more active intrusion of civilian authorities, and third parties, in military affairs. For instance, the government’s interest in fomenting foreign investment to assure private sector support in the fight against the FARC insurgency led to the practice of leasing army units to companies in the business of extracting natural resources. Such was the case with some hydroelectric power plants that used army brigades to protect their operations, which are commonly at odds with local populations effected by the diversions of water sources to generate electricity. This policy generated extra revenue for the military, but neglected broader security concerns and made critical infrastructure a common target for the rebels by drawing attacks directed towards the stationed army brigades.

Another example of third party intrusion in military affairs was the restriction the US Congress imposed on the Colombian military in 2006 because of reported human rights violations. The United States suspended shipments of helicopter fuel, effectively restricting the military’s ability to conduct search-and-destroy missions. This suspension reduced the army to

---


81 Former Security Consultant (2016, October 3). Personal interview on the role of army units in security for hydroelectric plants in Colombia.
constabulary police patrolling for several months, given the impossibility of conducting more aggressive operations without the required capabilities for fast deployments.\textsuperscript{82}

\textit{The Santos Administration (2010–2018)}

After the strategy of seeking a decisive victory shifted to reaching a negotiated solution with the insurgency in 2012, a balance between punishment and concessions was used as a new form of civilian control to ensure military compliance.\textsuperscript{83} This policy shift was due to the strategic stalemate with the FARC and the new administration’s more pragmatic stance holding that a long-term attrition campaign was neither feasible nor desirable. Facing an “adverse selection problem,” or uncertainty about the preferences and capabilities of potential candidates for promotion within the armed forces, the Santos administration (2010–18) changed the military leadership and promoted officers that were seemingly supportive of the peace negotiations.\textsuperscript{84} Congress approved the new promotions without much hesitation and the judiciary used the opportunity to push forward pending human rights investigations. From the concession perspective, active and retired officers were designated as part of the government delegation in the negotiations, which technically did not contradict constitutional law given that there are no legal regulations regarding the appointment of representatives to negotiate with irregular armed actors like the FARC. Therefore, presidential prerogative took precedence during this exceptional circumstance by shifting the mission of the military from fighting to safeguarding the peace negotiations.

This unprecedented participation of the military in politics was decisive for reaching the final agreement with the FARC in 2016 by assuring representation of the armed forces’ corporate interests in the post-conflict transition (including access to transitional justice benefits).\textsuperscript{85} However, some retired officer associations “built alliances” with the opposition and publicly questioned the peace talks.\textsuperscript{86} Some retired officers that have been subjected to years of

\begin{itemize}
\item \textsuperscript{82} Activist (2016, November 7). Personal interview on civil–military relations on Colombia.
\item \textsuperscript{83} Improved intelligence equipment, precision bombing and a helicopter fleet (unprecedented mobility), shifted balance of power and facilitated the peace negotiations by pressuring the FARC to quit the armed struggle.
\item \textsuperscript{85} The armed forces will have alternative judicial benefits like the FARC rebels that tell the truth about war crimes committed during the armed conflict.
\end{itemize}
ideological indoctrination or that fear being held responsible for the acts of their subordinates resisted the idea of a negotiated solution with the FARC, whereas enlisted men that had experienced combat more recently or been imprisoned for human rights abuses were more eager to support a peace agreement.\(^{87}\) In response, the administration publicly supported a 2015 constitutional amendment to the military justice code that promoted leniency towards military personnel under criminal investigations in order to rally support for the peace process within the armed forces.\(^{88}\) Additionally, the Defense Ministry incentivized the more active involvement of think tanks and scholars to address the debate regarding the redefinition of post-conflict armed forces’ roles and missions.\(^{89}\)

Finally, it is worth mentioning that after the failed plebiscite to ratify the peace agreement in late 2016, army command followed the order to sustain the ceasefire and to abstain from making any public declarations—an adjusted version of the agreement was ratified by congress later the same year. So far, military corporate interests have not been threatened by the agreement itself, as no budget cuts were made, there have been no announcements about downsizing the forces of any of the armed services, and active representation of the armed forces in the peace talks was granted. No security sector reform was negotiated in the peace agreement, and all institutional reforms are being crafted by a special military command—known as, El Comando Estratégico para el Ejército del Futuro.\(^{90}\)

However, disagreements between the officer corps and the civilian authorities about how to conduct the peace process implementations are likely to happen. For instance, despite the reported success of the demobilization process of the FARC combatants—conducted in early 2017 and under UN and Colombian armed forces supervision—several pockets of rebel dissidents have been identified.\(^{91}\) Differences on how to portray the magnitude of and address these new security issues might result in new tensions regarding civil-military relations. According to a former advisor to the Colombian government, the government prevented the military from making public information about violations to the terms of the agreement by some

---


\(^{90}\) Comando de Transformación Ejército del Futuro – COTEF (https://www.ejercito.mil.co/comando_transformacion_ejercito_futuro_cotef)

of the FARC factions. This is a situation that allegedly might be related to a recent change of leadership and some recognitions within the armed forces officer corps, as the government has an incentive not to release any information that could signal failure of its most prominent policy success: the peace agreement with the FARC—although there is no official confirmation, nor has the military leaked critical information to the media. Similarly, the decision concerning the role of the military in countering organized crime in a post-conflict scenario remains pending, and it might lead to inter-service rivalry or perhaps further disagreement with the civilian authorities.  

Civil-Military Relations Trends 1991-2016

Overall, the presidency has been the main civilian oversight institution as put forth in the constitution, while congress has generally deferred judgment, quickly approving budgets and promotions. Furthermore, with the professionalization of the security forces, accountability and the socialization of international humanitarian law have become extremely important. Hence, the judiciary has also become a third relevant principal in terms of civilian oversight.  

In practice, civilian control has been subjective and ideology has played an important role in determining mission designation. By linking the ruling elites’ preferences and interests with military doctrine (counterinsurgency, counterterrorism, etc.), civilian authorities were able to instrumentally use the armed forces against their opponents. Thus, the armed forces cannot be politically neutral because they are embedded in a contest for the legitimate access to power. Despite their level of professionalism, the armed forces are shaping domestic politics by defending the constitutional order from those who question its legitimacy from within. Thus, as Watson suggested, the military does not have a unified conception of nation-state to defend, given the lack of legitimacy of the Colombian government.  

Since the 1991 constitution was enacted, the moral hazard problem, or temptation of the agent (the armed forces) to not cooperate, has been properly managed by allocating resources, granting autonomy, enforcing punishment, and supervising performance. Functionally, the

---

armed forces have performed civilian-designated tasks; from a relational standpoint, they have not successfully challenged civilian control.⁹⁶

Changes in policy or strategy by civilian authorities, even when proven ineffective, have not resulted in the military replacing civilian control. In simple words, civilians successfully exercised their right to be wrong, making strategic mistakes on several occasions, yet institutional and ideological control mechanisms were never fully eroded, nor was the principle of civilian government ever overthrown. The use of military force domestically continues to be a key instrument to shape politics in the service of civilian authority.

With the recent unparalleled de-escalation of violence with the FARC and the political contest moving from the battlefield to the democratic institutions, civilian authorities are faced with the challenge of assigning new roles and missions for the military. To ensure civilian control and good governance during the implementation of the peace agreements, redefining the role of the armed forces will entail both institutional reforms and the deconstruction of a longstanding ideological premise that enabled stigmatization and repression as an accepted practice by the military.

Looking forward, closing the gap between civil society and the armed forces may help to make the military more resilient to ideological indoctrination and prevent the instrumental use of force by exclusionary elites. Promoting higher levels of education and joint university level programs with civilians among the officer corps (ROTC-like programs) might also be beneficial⁹⁷—mainly, because joint education can be conducive to higher levels of mutual understanding, the generation of shared identities, and the strengthening of cooperation across civilian and military professional. Additionally, this could lead to a hypothetical increase of the level of restraint, an important trait when facing domestic security challengers, by the officer corps. Urging the legislature to adopt a more assertive oversight role in respect to both budget allocation and the legality of military operations and practices, as well as empowering the civil society to conduct academic or journalistic independent research, might also help to improve civil-military relations by ensuring a more transparent and democratic assignment of roles and missions. Adopting these measures would prevent criminal investigations by the judiciary from being the sole deterrent against unlawful behavior by the armed forces, while fulfilling sensitive missions at the operational and tactical levels.

Although institutional reform of the armed forces was not negotiated with the FARC, the military has anticipated the upcoming changes by creating the Strategic Transition


⁹⁷ Reserve Officer Training Corps (ROTC).
Command for post-conflict stabilization, and the Special Command for the Army of the Future, tasked with institutional reform. Additional research regarding challenges for civilian control and redefining the roles and missions of the armed forces must consider: the possibility of demilitarizing the police, probably resulting in new tensions giving that the Defense Ministry would be giving up operational scope and resources; the role of the army in the fight against organized crime; reemerging radical right-wing paramilitary groups and the FARC dissidents; potential conflict spill-over from an increasingly unstable Venezuela (border control, interdiction operations, countering transnational criminal networks); and the legislative debate about the size and budget of the armed forces, their role in state-building in the most conflict-affected areas of the country, as well as the controversy regarding a special transitional justice tribunal in the agreement that has jurisdiction over members of all the armed services.

Overall, and despite the effective control by civilian authorities, healthy civil-military relations continue to be elusive in Colombia, at least from Huntington’s normative standard of objective control. The domestic nature of the security threats and the severe limitations of the democratic system in the country—which serves the interest of narrow elite segment of the population seeking to retain political power—have resulted in a recurrent incentive for the instrumental use of the military, mainly through institutional and ideological control mechanisms. Therefore, improving civil-military relations towards a less political biased form of control, as well as attaining a more inclusive and comprehensive state of actual stability and security in the country, seems to depend on the possibility of largely improving the quality of democracy in Colombia.

*About the Author*

Carlos Castillo is currently a master’s degree student at the Georgetown University Security Studies Program, and a Research Fellow of the Latina American Initiative in the same university. He also has a BA and MA in Political Science from Universidad de los Andes in Bogota, and he has worked for the UN, the Colombian Attorney General’s office and collaborated with several think tanks and research centers in Colombia and in Washington DC.

---

The Drivers of Iranian Cyber Strategy: From Stuxnet to the Present

Jack Rock Lucas

Despite being a relatively young cyber power, Iran’s execution of several prominent cyber-attacks demonstrate that Tehran is willing and able to operate in the cyber domain to achieve its strategic objectives. This article proposes that, since Iran began investing in cyber capabilities in reaction to the 2010 discovery of the Stuxnet attack, it has sought to use the cyber domain to maintain control of its population through extensive monitoring, exert influence on its neighbors through proxy organizations, and deter its technologically advanced adversaries through the threat of costly cyber-attacks on critical infrastructure. Iranian cyber strategy is investigated by identifying three phases of development for the country’s cyber capabilities: the creation of formal cyber organizations, the demonstration of ‘loud’ retaliatory capabilities, and the ‘quiet’ collection of critical vulnerabilities for sophisticated attacks. Lastly, this article speculates as to what factors will make Tehran more or less likely to reactively execute cyber-attacks on critical infrastructure in the future.

Introduction

Iran has developed a cyber strategy centered around deterring interference from its technologically advanced adversaries through demonstrating its willingness to continuously develop and execute critical infrastructure attacks, all while Tehran maintains control over its population and influences its region. Iran exhibits these offensive capabilities through domestic front organizations and regional proxy groups in Syria,1 Yemen,2 and elsewhere3 to reduce the likelihood of escalation by its cyber-adept adversaries. These adversaries’ attacks against Iranian critical infrastructure not only kick-started Iran’s cyber development, but also keyed Tehran into the influential potential of targeting critical infrastructure. To reach a holistic understanding of Iran’s cyber strategy, it is first necessary to review the history of cyberpower development in the Islamic Republic. In that context, this piece will lay out Iran’s cyber strategic objectives and how

it has dealt with inherent challenges. Finally, the conclusion will present how these strategic objectives will influence the future of Iran in the cyber domain.

**History & Structure**

The discovery of Stuxnet in 2010 was a watershed moment in Iranian cyber history that defined their future targets for retaliation and prompted the development of cyberpower. Cyber capabilities were developed by first creating organizations to increase the regime’s level of control in cyberspace, then executing ‘loud’ cyber operations against adversaries, and culminating in a matured focus on ‘quiet’ cyber espionage.

In 2010, Tehran feared its vulnerability to western influence could bring the Arab Spring to Iran, a concern amplified by the Stuxnet attack. When the Iranians discovered the Stuxnet worm in 2010, President Ahmadinejad’s disputed election was still a rallying call to protesters, whose impact benefitted enormously from social media. The internal security arm of the Islamic Revolution Guard Corps (IRGC), the Basij, failed to effectively mitigate these protests and, to avoid another possibly fatal mistake, the Basij Cyberspace Council was established in 2010 to develop online propaganda and monitor Iranian Internet for counter-ideological behavior and indications of dissent. By November 2010, the IRGC claimed to have over 1,500 trained ‘cyber-warriors’ in the Basij plus a growing number of volunteers. While other groups dedicated to developing Iran’s cyberpower grew during these early stages, including telecommunication companies established as fronts by the IRGC and the Ministry of Intelligence and Security’s increased signals intelligence capabilities, the creation of the Basij Cyber Council indicated a noteworthy change in Iranian strategic thinking: Tehran would embrace the cyber domain to address both domestic and foreign security issues. Domestically, this was reflected in the country’s earliest cyber-attacks, against Comodo and DigiNotar, two European certificate

---

authorities. While technically unsophisticated, the attacks stole web certificates that allowed the Basij to impersonate Google services and penetrate more than 300,000, mostly Iranian, computers for monitoring.\textsuperscript{11}

Iran’s advancement from leveraging cyberpower almost entirely for the purpose of domestic control to developing full-fledged offensive cyber operations is most clearly exemplified by two 2012 attacks, dubbed Shamoon and Operation Ababil.\textsuperscript{12} In addition to being made possible by continued development of Basij cyber techniques, this phase, like the first, was motivated by sophisticated intrusions against Iran. Most notable is the highly sophisticated “Flame” malware, which conducted extensive espionage against Iranian oil companies.\textsuperscript{13} Unlike post-Stuxnet in 2010, however, Iran now possessed the capability to retaliate. Shamoon was executed on August 15, 2012,\textsuperscript{14} at which point it destroyed the data on three-quarters of Saudi Aramco’s computers, rendering the hard drives of the multi-trillion-dollar Saudi oil company useless.\textsuperscript{15} Operation Ababil, conducted weeks later, was a massive, persistent distributed denial of service (DDoS) attack against major US financial institutions that caused losses estimated in the tens of millions of dollars.\textsuperscript{16} The Shamoon attack was likely done as a response to a cyber-attack on Iran's oil terminal on Kharg Island, and the Ababil attack was likely a response to newly imposed US sanctions.\textsuperscript{17} Both are noteworthy in their explicitness. While not employing the most sophisticated methods, these attacks nonetheless signaled that Iran could credibly and effectively retaliate in the cyber domain.

In its most recent evolution, Iranian cyberpower reached maturity in being able to both execute costly attacks as well as conduct sophisticated, stealthy espionage operations necessary to keep their cyber arsenal of critical infrastructure attacks refreshed and ready-to-fire. Operation Cleaver was publically uncovered by Cylance, an American cybersecurity firm, in 2014 as an Iranian operation harvesting critical infrastructure vulnerabilities from around the world for future use.\textsuperscript{18} The use of advanced custom exploitation tools that specifically targeted essential

\begin{enumerate}
\item Ibid.
\end{enumerate}
critical infrastructure systems worldwide indicated Iran had evolved to become a top player in the cyber domain.\textsuperscript{19}

**Objectives and Challenges to Overcome**

Despite being relatively new to the field, Iran is regarded as a top cyber power with a demonstrated interest in targeting critical infrastructure and influencing its region via proxies.\textsuperscript{20} Tehran will employ these capabilities to fulfill three cyber strategic objectives: to maintain control over its population, to influence its region through proxies, and to deter foreign interference through the threat of costly retaliation.

The Basij have continued to control information in ways that are now typical of authoritarian regimes, ranging from monitoring Internet cafes to defacing dissident websites with propaganda.\textsuperscript{21} However, these tactics are insufficient to handle two recent social changes in the country: the connectedness of its population and the rise of progressivism. Smartphone ownership in Iran has rapidly risen in the last few years and smartphones now outnumber people in the country.\textsuperscript{22} Not unrelatedly, the re-election of progressive President Rouhani over hardline candidate Ebrahim Raisi, who was supported by the Supreme Leader,\textsuperscript{23} signals an increased acceptance of open policies, especially given the beneficial potential presented by recently reduced sanctions.\textsuperscript{24} This forced the IRGC to build a solution for monitoring an increasingly connected population without inciting protests or stifling the economic benefits of Internet access. Out of this dilemma came the National Information Network (NIN) a “halal” intranet for the country.\textsuperscript{25} Through a gradual, multi-phase rollout process, the NIN will give the IRGC unprecedented ownership of the physical infrastructure of Iran’s intranet, allowing better cyber monitoring and faster responsive action. Most importantly, the NIN will feature a massive performance improvement over the previous system of state-controlled Internet access, which was ranked among the world’s most unstable infrastructures.\textsuperscript{26} Tehran hopes that the NIN will

\begin{footnotesize}
\begin{itemize}
\item\textsuperscript{19} Ibid., 10.
\item\textsuperscript{21} Gabi Siboni and Sami Kronenfeld, “Iran’s Cyber Warfare,” INSS Insight No 375 (October 15, 2012). 2.
\item\textsuperscript{26} Ibid.
\end{itemize}
\end{footnotesize}
allow monitoring to keep pace with the growing connected population while its clear performance advantages will draw Iran’s technology firms back to being hosted in-country, reducing vulnerability to foreign attacks, killing two birds with one stone.\(^{27}\)

Iran’s approach taken to influencing other countries in its region, while less innovative than the NIN, focuses on supporting proxy organizations to carry out cyber-attacks with a degree of deniability. Similarly to how the IRGC has supported multiple Iraqi Shia militias in Iraq (an assertion the IRGC denies),\(^{28}\) Iran has applied the same method in the cyber domain with the Syrian Electronic Army (SEA)\(^{29}\) and Yemen Cyber Army (YCA).\(^{30}\) While proving Iran’s connection to these groups with complete certainty is, by their covert nature, impossible, the likelihood of Iranian involvement can be assessed through contrasting the techniques, tactics, and procedures of these groups before and after they had an opportunity to conduct attacks that benefitted Iran’s interests in the region. In 2011, the SEA was known for relatively unsophisticated attacks to impose minor annoyances on Syrian rebels, such as defacing anti-Assad websites.\(^{31}\) However, just as western involvement in Syria was ratcheting up in 2013, the SEA rapidly matured. In a matter of months, the group was carrying out targeted attacks against rebels that used infected files sent to known rebels to remotely steal battle plans, which would then be delivered to Assad’s forces.\(^{32}\) The sudden increase in sophistication from vandalism to cyber tactical support, at the same time that Syria, a strategic regional ally to Iran, was increasingly threatened by western occupation makes a strong case for Iranian involvement. A similar case can be made for the YCA being used against Saudi Arabia during the 2015 Yemen Civil War.\(^{33}\) It is most likely that Iran is providing material and technical support to these groups, rather than being at the helm, in order to provide a degree of deniability that allows Iran-based cyber groups to focus on more advanced cyber operations.

With increased investment in cyber control at home and abroad comes greater risk of foreign interference. Despite its extraordinary advances, Tehran is aware it cannot go toe-to-toe


in an escalating cyber conflict with its most capable adversaries. Instead it has decided to reshape how its enemies think through deterrence by threat of retaliation in kind. Successful deterrence in Tehran’s situation relies on two components of cyber activity: ‘loud’ attacks to signal a willingness to act and constant, ‘quiet’ efforts to identify vulnerable high-cost targets, most likely critical infrastructure.\textsuperscript{34} The attacks on Saudi Aramco and the US financial system were meant to be overt and noticeable to make Iran’s adversaries take note that the Islamic Republic is capable of striking even highly defended targets. Unlike nuclear deterrence, where a new nuclear power can demonstrate its destructive capabilities by conducting a public, harmless test detonation, cyber demonstrations require that an enemy be negatively impacted. However, the impact of the cyber demonstration must not be as catastrophic as the threatened deterrent, as this would invite escalation and defeat the purpose of deterrence. By using front organizations to infiltrate highly defended targets to execute a costly, but not overwhelming, cyber-attack, Iran stays below its adversary’s escalation threshold while still signaling its intent to use more damaging attacks if necessary. Demonstrated intent through loud signals would be insufficient for a deterrent, however, unless Tehran was able to indicate that it had a fully stocked arsenal of costly cyber weapons. Again, diverging from standard nuclear deterrence, cyber weapons typically have an expiration date that occurs when the intended victim discovers and patches the targeted vulnerability. Iran overcomes this by using advanced, stealthy cyber operations in the style of Operation Cleaver to locate new, fresh vulnerabilities at a likely faster rate than previously found vulnerabilities ‘expire’.\textsuperscript{35} Furthermore, Operation Cleaver indicated that these operations seek out vulnerabilities in energy, airline, hospital, military, telecommunications, and other systems that represent a high cost if taken down.\textsuperscript{36} While the security researchers at Cylance were able to identify Operation Cleaver, it can be safely assumed that there are other operations being conducted by Tehran to fulfill a similar critical-infrastructure-oriented purpose in order to deter a repeat of Stuxnet.

**The Future of Cyber Iran**

Some have called Stuxnet the initial shot in “history’s first known cyber-war”.\textsuperscript{37} While this claim is debatable, there is little doubt that the attack’s demonstrated effect against valued critical infrastructure in Iran defined the country’s development of a cyber strategy. In response,


\textsuperscript{36} Ibid., 10.

Tehran leaned more heavily on developing critical infrastructure attacks. These attacks pose an asymmetrically higher threat to Iran’s adversaries and lend themselves to Tehran’s *modus operandi* of using the cyber domain to *react* to the actions of its adversaries, rather than striking first. This reactionary posture will result in Iran’s continued collection of critical infrastructure vulnerabilities. As it stockpiles these critical vulnerabilities, Iran will regularly execute costly, politically-motivated, reactive attacks that directly punish its perceived aggressor while indirectly deterring its many technically reliant adversaries who are, by their nature, asymmetrically more vulnerable to critical infrastructure attacks. However, if Iran continues on the path of economic openness allowed by reduced sanctions and President Rouhani’s progressive outlook on external investment, there may be opportunities to build communication channels with the Islamic Republic to prevent an escalation of cyber threats in the next political disagreement by raising Tehran’s threshold to react. The flip side is also true, and a situation in which conservative hardliners led by Supreme Leader Khamenei and the IRGC retake control could close the door to these negotiations and lead to a volatile cyber program that is more willing to use costly cyber-attacks as a regular tool of foreign policy. In any case, Iran has no desire to stop pursuing world-class cyber capabilities. With its nuclear weapons program limited by the Joint Comprehensive Plan of Action (JCPOA), Iran may very well reallocate some of these now unused resources towards advancing cyber initiatives instead. Already a formidable cyber power, the Iran of 2024 will be more technically advanced and able to conduct sophisticated cyber operations against perceived threats to itself or its sphere of influence.

*About the Author*

*Jack Rock Lucas is an M.A. candidate in the Georgetown University Security Studies Program, concentrating in technology and security. His research interests include assessing the cyber capabilities of state actors and the threat and feasibility of cyber attacks targeting critical infrastructure. Jack graduated from the University of Southern California’s Viterbi School of Engineering with a B.S. in Computer Science and has professional experience as a cybersecurity consultant, software engineer, and game developer.*
“Then Kill the Pagans Wherever You Find Them”: The Emerging Trend of Islamic State Networks Targeting Christians in Egypt

Sarah Gilkes

Since the rise of the Islamic State (IS) and the organization’s declaration of a caliphate in June 2014, much scholarship has been devoted to examining the group’s evolution, ideology, and expansion. Little attention, however, has been paid to the development and mobilization of IS’s affiliate in Egypt, Wilayat Sinai, and other IS-related networks across Egypt. This article seeks to fill this gap through a quantitative study of terrorist attacks attributed to and/or claimed by Egyptian IS-related entities and their predecessors, specifically Ansar Bayt al-Maqdis (ABM), between January 1, 2011, and June 30, 2017. In particular, this article focuses on the recent shift of IS strategy within Egypt embracing the targeting of Coptic Christians, the largest Christian community in the Middle East. Comprehensive examination of all ABM and IS-related terrorist attacks in Egypt during this period reveals that while attacks targeting Christians began in early 2014, only in the first six months of 2017 did IS-related networks—both in the Sinai and across mainland Egypt—begin to systematically target Copts. Analysis of official IS propaganda suggests that militants hope attacks will aggravate existing tensions between the Coptic minority and Muslim majority in Egypt, thereby sparking a larger civil and political conflict and enabling IS-related networks of militants to act as the defenders of the Sunni Muslim community.

Introduction

Since the rise of the Islamic State (IS) and the organization’s declaration of a caliphate in June 2014, much scholarship has been devoted to examining the group’s evolution, ideology, and expansion. Little attention, however, has been paid to the development and mobilization of IS’s affiliate in Egypt, Wilayat Sinai, and other IS-related networks across Egypt. This article seeks to fill this gap through a quantitative study of terrorist attacks attributed to and/or claimed by Egyptian IS-related entities and their predecessors, specifically Ansar Bayt al-Maqdis (ABM), between January 1, 2011—the origins of ABM’s ties to the Egyptian mainland—and June 30, 2017. In particular, this study focuses on the recent shift of IS strategy within Egypt embracing the targeting of Coptic Christians, the largest Christian community in the Middle East. Comprehensive examination of all ABM and IS-related terrorist attacks in Egypt during this period reveals that while attacks targeting Christians began in early 2014, only in the first six months of 2017 did IS-related networks—both in the Sinai and across mainland Egypt—begin
to systematically target Copts. Analysis of official IS propaganda suggests that militants hope attacks will aggravate existing tensions between the Coptic minority and Muslim majority in Egypt, thereby sparking a larger civil and political conflict and enabling IS-related networks of militants to act as the defenders of the Sunni Muslim community.

This article proceeds in four parts. The first section briefly discussed the evolution of Salafi jihadism in modern Egypt, placing particular emphasis on the rise and growth of ABM and developments following the leadership’s pledge of allegiance to IS in November 2014. In order to place the targeting of Christians within the Islamic State’s larger strategy, the second section examines the framing of Christians in IS’s official propaganda magazines, Dabiq and Rumiyah. The third section details the methodology and findings of the article, examining how the declaration of an IS affiliate in the Sinai Peninsula—Wilayat Sinai—impacted the frequency, target selection, modality, location, and lethality of IS-related terrorist attacks across the country, again placing particular emphasis on attacks targeting Christians. The final section provides an overview of the current status of the Egyptian Coptic community and offers predictions for the future of IS networks in the country.

I. Brief History of Salafi Jihadism in Egypt

From the Afghan Jihad to the Arab Spring

Militant Islamism has a long history in modern Egypt. Beginning in 1979 with the Soviet invasion of Afghanistan and continuing throughout most of the 1980s, a large number of Egyptians traveled to Afghanistan and Pakistan in the hopes of participating in the Afghan jihad. Arguably one of the most influential Egyptians to take part in the jihad was Ayman al-Zawahiri, the then-leader of Egyptian Islamic Jihad (EIJ) and the future leader of al-Qaeda (AQ). While al-Zawahiri was cultivating a relationship with Osama bin Laden in Peshawar, EIJ remained active back in Egypt: in 1981, members of EIJ assassinated Egyptian President Anwar Sadat.

Between 1990 and 1997, the Egyptian state was locked in a low-level war of attrition with militant Islamists who sought to overthrow the government of President Hosni Mubarak. After years of relative stalemate, a confluence of factors enabled the government to degrade and

---

contain the terrorist threat in 1997. The militant organizations’ failure to cultivate a strong base of support among the population and heavy reliance on “shock tactics,” combined with Egyptian security services increasingly successful targeting of militant leaders, severely diminished the militants’ capacity to wage an insurgency.\(^4\) The militants’ greatest strategic mistake, however, was the indiscriminate targeting of civilians.\(^5\) Perhaps no event captures the degree to which the decision to target civilians backfired than the November 1997 Luxor attack when an al-Jama’a al-Islamiyya cell attacked an ancient Egyptian temple and killed 68 civilians.\(^6\) After the attack, public opinion decidedly turned against the militants, and political, religious, and civil leaders called on the government to more aggressively pursue the jihadists.\(^7\) In the two decades that followed, the fallout of the Luxor massacre guided the targeting patterns of jihadist groups inside Egypt.

In the years after the Luxor massacre, a period of relative peace between jihadists and the Egyptian state took hold.\(^8\) However, this period of relative calm ended abruptly on October 7, 2004.\(^9\) On that evening, a group of four men conducted a series of three bombings targeting tourist destinations—the Taba Hilton Hotel and two campsites—just south of the Egyptian border with Israel. The attacks, which claimed 34 lives, marked the beginning of an almost two year period of unrest in the Sinai.\(^10\) During the period between late 2004 and mid-2006 a series of four large-scale terrorist attacks claimed over 120 lives. In three of the attacks, militants targeted locations frequented by tourists; one operation targeted a base belonging to Multinational Force and Observers, an international peacekeeping force charged with overseeing the terms of the Camp David Accords in the Sinai.

While it remains unclear who was behind the planning and execution of the attacks, “the target, type, planning, scope, and simultaneous attacks...all displayed the hallmarks of al-Qaeda operations.”\(^11\) Following each attack, a number of militant organizations claimed responsibility. Notably, one group in particular claimed responsibility on a number of occasions: the Abdullah Azzam Brigades of al-Qaeda in the Levant and Egypt.\(^12\) While al-Qaeda central (AQC) never publicly claimed responsibility for any of the operations in the Sinai, “the fact that these attacks threatened the interests of three of al-Qaeda’s main enemies and focused attention on one of the

---

\(^4\) Gerges, “The End of the Islamist Insurgency in Egypt?” 593.
\(^5\) Ibid, 593–594.
\(^6\) Ibid, 594.
\(^7\) Ibid, Awad, “Bay’a Remorse?” 2.
\(^8\) Gerges, “The End of the Islamist Insurgency in Egypt?” 595.
\(^9\) Ibid, 596.
\(^11\) Ibid, 485.
\(^12\) Ibid, 492.
foundations of al-Qaeda’s causes—the Palestinians—prompts the question whether the group was behind them.” Furthermore, it would be a mistake to read Osama bin Laden and al-Zawahiri’s failure to disclose a role in these attacks as proof that the attackers had no connection to AQC; in fact, AQ leadership never officially claimed a number of major assaults despite revelations related to the organization’s role.

From Ansar Bayt al-Maqdis to Wilayat Sinai

The political uprisings that took hold of Egypt in early 2011 and forced President Mubarak from power created space for the reinvigoration, expansion, and proliferation of jihadist mobilization networks across the country. One group that emerged out of this period was Ansar Bayt al-Maqdis (ABM), also known as Ansar Jerusalem. While researchers agree that ABM was founded in 2011 by Egyptian militants seeking refuge in the Sinai, the exact date of the organization’s founding remains unclear. From the beginning, “ABM’s unique strength was its coalition of operatives sympathetic to al-Qaeda, jihadis with local grievances, and radical Gazan elements still focused to a significant degree on Israel.” Yet, despite ABM’s affinity for AQ’s ideology, the organization never issued a statement pledging loyalty to AQ leaders Osama bin Laden or Ayman al-Zawahiri. Further, and perhaps more interestingly, AQ’s leadership has never claimed a formal affiliate inside Egypt despite the organization’s extensive connections to the Egyptian jihadist scene.

It wasn’t until 2013, following the military coup that ousted Muslim Brotherhood candidate and Egyptian President Mohamed Morsi, that ABM emerged as the most powerful jihadist actor in the country. In his book The New Arab Wars, Marc Lynch offers perhaps the most succinct explanation of the coup’s impact on the global jihadist movement: “The coup had

---

14 Ibid, 494. As the authors point out, “bin Laden never accepted responsibility for other strikes attributed to him, including the 1998 bombings of U.S. embassies in Kenya and Tanzania or the USS Cole in Yemen in 2000.”
made a mockery of the Brotherhood’s strategy of peaceful democratic participation, vindicating long-standing jihadist arguments for violent struggle. State failure...opened space for jihadist groups to reorganize, acquire weapons, and establish new strongholds.” 21 It is in this environment in which ABM began to grow and spread beyond the Sinai.

On November 11, 2014, ABM leadership pledged bay’a (allegiance) to Abu Bakr al-Baghdadi and the Islamic State, and shortly thereafter changed its name to Wilayat Sinai. 22 ABM’s decision grew out of a combination of ideological, strategic, and financial considerations. Over the course of 2014 many of ABM’s leaders were killed, leading to significant organizational disruption.23 The removal of these leaders, with whom the organization’s ideological affinity with AQ was centered, created the space necessary for the shift to IS. Only a month before pledging allegiance to Baghdadi, two ABM envoys traveled to Syria to meet with IS leaders, where ABM allegedly hoped to secure financial support in exchange for their bay’a. 24

The specifics of IS’s support and mobilization networks across Egypt remain unknown. ABM’s ties to the Egyptian mainland can be traced back to 2011, when a group of jihadists recently released from prison established “a number of compartmentalized cells” in the Nile Valley. 25 Within two years, cells were established in at least eight governorates across the country. Yet, while ABM’s support network was expanding, the organization also relied upon alliances with local militant groups across mainland Egypt to project power.26 The extent to which these cells were connected to other AQ–linked networks in Egypt during this period remains unclear.27 Regardless of ideological affinity, there are indications that IS has attempted to recruit, coopt, and consolidate existing jihadist groups in the Nile Valley under the black flag. 28 The first IS cell in mainland Egypt, based out of the province of Beni Suef, appears to have become operational in the summer of 2015 with the attempted attack on the Karnak Temple in Luxor. In the months that followed, IS jihadis lost momentum in the Nile Valley and “new cells made up of fresh Islamic State recruits whose loyalty is only to Abu Bakr al Baghdadi rose in their stead.”29 This wave of IS recruits chose Giza governorate, a historic Islamist

23 Gartenstein-Ross, “ISIL’s International Expansion.”
24 Kirkpatrick, “Militant Group in Egypt Vows Loyalty to ISIS.”
26 Ibid.
27 Ibid.
stronghold to the southwest of Cairo, as their staging ground. Some analysts speculate that these mainland IS networks are working directly with the group’s core leadership in Syria and Iraq instead of operating through Wilayat Sinai.

There are also indications that in the months before ABM pledged allegiance to IS, the group had started establishing networks in Egypt’s Western Desert, a largely uninhabited and arid area that extends to the border with Libya. Over the summer of 2014, ABM carried out several attacks in the Western Desert. This network appears to have survived ABM’s evolution to Wilayat Sinai, as IS issued a statement declaring its presence in the Western Desert in the fall of 2015. As Mokhtar Awad notes, “Egypt’s adjoining western desert remains an entry point for both al-Qaeda- and Islamic State-linked operatives as both groups have a strong presence in Libya.” Wilayat Sinai has also received material support from IS leadership through smuggling networks along the Mediterranean coast, where “a network of small fishing boats connects the Northern Sinai coast with Libya’s and allows for these transfers.” Further underscoring the likely connection between Egyptian and Libyan IS networks, in a statement released June 22, 2017, the Egyptian Interior Ministry said officials are “certain that a group of individuals had been stationed in some areas in the Western Desert, where they received military training on how to use weapons and assemble explosive devices in order to carry out more terrorist attacks.” Additionally, in 2015 United Nations Security Council expert panel concluded, “Libya is a pre-eminent [sic] source of arms used in criminal and terrorist activities in Egypt. Groups like Ansar Beit el Makdess [sic] receive support from some Libyan actors, including military material.” To date, however, there is little publicly available information explicitly linking IS networks in Egypt and Libya, let alone evidence tying Libyan-based IS militants to attacks inside Egypt claimed by local IS networks. This suggests that Egyptian IS-affiliated networks conduct attacks relatively independently of other IS-affiliated groups in the region.

II. Framing of Christians in Official IS Propaganda Magazines

Comprehensive examination of how IS frames Christians in official propaganda magazines Dabiq and Rumiyah sheds light on Egyptian IS networks’ recent shift toward

---

31 Awad, “Bay’a Remorse?” 7.
32 Awad, “The Islamic State’s Pyramid Scheme,” 34.
36 Nicholas Marsh, “Brothers Came Back with Weapons: The Effects of Arms Proliferation from Libya,” PRISM 6, no. 4 (2017), 86.
targeting Coptic Christians. The first discussion of the permissibility of targeting Christians appeared in the seventh issue of *Dabiq*, released in early 2015, in which the author writes: “[It] is important for Muslims everywhere to know that there is no doubt in the great reward to be found on Judgment Day for those who spill the blood of these Coptic crusaders wherever they may be found....”37 This statement characterizes Christians as legitimate targets, placing them alongside Shia Muslims, Jews, and members of other minority religions regarded as “pagans,” “idolaters,” or “apostates” by the Islamic State.

The organization offers a number of religious justifications for the strategy of targeting Christians. In the fifteenth issue of *Dabiq*, released in the summer of 2016, the author explains, “Allah has made our mission to wage war against disbelief until it ceases to exist, as he has ordered us to kill all pagans wherever they are found.’ He said, ‘Then kill the pagans wherever you find them.”38 An issue of *Rumiyah*, released in the spring of 2017, clarifies that those Christians who repent and convert to Islam, make a covenant of security, and give zakat (an obligatory religious tax) should be forgiven.39 In other words, so long as Christians agree to submit to living under the Islamic State’s interpretation of sharia they can theoretically avoid death. Those Christians who refuse to comply or break their covenant, however, are regarded as legitimate targets.40

There is a second set of restrictions limiting who among Christians can be targeted by IS militants. The ninth issue of *Rumiyah* explains

[It] is the fighters among them who are to be targeted, and they are those who are capable of carrying a weapon, even if they don’t actually do so, and likewise those of them who support the fighters with their opinion and counsel. As for those who don’t normally carry weapons, such as women, children, the elderly, and the infirm, the default with them is that they are to be taken as slaves, not that they are to be killed.41

The passage goes on to explain that the death of women, children, the elderly, or the infirm in IS attacks is not deliberate, but rather an unintended consequence of the militants’ inability to distinguish between “fighters” and “non-fighters.” However, individuals traditionally deemed non-combatants but seen carrying a weapon or taking part in the fight against IS—both

37 *Dabiq* 7 (2015), 32.
38 *Dabiq* 15 (2016), 63.
40 Ibid.
actively and by “offering his opinion and counsel”—are deemed legitimate targets.\textsuperscript{42} This particularly applies to monks and priests, as “they are in fact the leaders of \textit{kuf\MakeLowercase{r}} [infidel] and they are the \textit{tawaghit} [idolaters] who are worshiped besides Allah.”\textsuperscript{43} Similarly, churches and monasteries are deemed acceptable targets since they are the places in which idolatry is practiced.\textsuperscript{44} In fact, IS encourages assaults on symbols of Christianity, explaining that such acts permit the attacker to “attain closeness to Allah.”\textsuperscript{45} An interview with an individual identified as the “Amir of the Soldiers of the Khilafa in Misr [Egypt],” also featured in the ninth issue of \textit{Rumiyah}, calls upon Egyptian Muslims unable to reach the so-called caliphate to “plan operations against the Christians and the apostates. Cause them tremendous harm and detriment, and let them see from you the might of the believers, as well as your eagerness to attain \textit{shahadah} [martyrdom] for the cause of Allah.”\textsuperscript{46}

The same issue of \textit{Rumiyah} devotes a section to the state of Christians in Egypt, who IS characterizes as “belligerent kuffar.”\textsuperscript{47} The piece goes on to enumerate a number of ways in which Egyptian Christians are battling Muslims, stating

The Christians of Misr…are engaged in fighting the Muslims through their continuous transgressions against any Christian who embraces Islam, kidnapping them, killing them, and putting them through trial and tribulation in order to make them return to shirk [idolatry or polytheism]. And likewise through their membership in the taghut’s army, security and intelligence agencies, and police force, which wage war against the Muslims and guard the shari’ah of the taghut, and they are among the most sincere supporters of the taghut Sisi in Misr, and among his closest allies and most loyal partners in his war against Islam and the Muslims. Furthermore, they, their priests, and their monks are among the people most active in defaming the religion of Islam, the Noble Quran, and the Messenger.\textsuperscript{48}

The first video released by IS on behalf of what is referred to as the “Islamic State in Egypt” in February 2017 speaks directly to the recent increase in attacks targeting Christians across the country. Drawing from similar passages of the Quran and Hadith that were cited in \textit{Dabiq} and \textit{Rumiyah}, the video justifies the December 2016 suicide bombing at St. Mark’s Coptic Orthodox Cathedral in Cairo as a necessary response to the “Crusaders who fight the Muslims.”

\textsuperscript{42} Ibid.
\textsuperscript{43} Ibid, 8.
\textsuperscript{44} \textit{Rumiyah} 9 (2017), 9
\textsuperscript{45} Ibid, 8, 10.
\textsuperscript{46} Ibid, 52, 54.
\textsuperscript{47} Ibid, 6.
\textsuperscript{48} Ibid, 7.
An IS fighter, identified as Abu Zubair al-Masri, then speaks directly to Egyptian Muslims, saying, “Oh you, who seek martyrdom, oh you, who could not make it to the Islamic State, the marketplace of jihad is open. The enemies of Allah are in front of you. Turn their nights into hellfire and their days into destruction. Let their blood flow like rivers. Fill their hearts with fear and terror.”\textsuperscript{49} Finally, near the end of the video the narrator issues a warning to Copts, stating, “You are a target at the top of our priorities, our favorite prey.”\textsuperscript{50}

Unlike the leadership of AQ, who sought to foster deep and lasting ties with local communities in areas of active hostilities regardless of religious or ethnic identity, official IS propaganda demonizes Christians crusaders and apostates and explicitly calls for their elimination.\textsuperscript{51} This extreme position is not foreign to IS ideology. In fact, in the early 2000s the leader of al-Qaeda in Iraq (AQI), the predecessor to IS, Abu Musab al-Zarqawi, sought to spark a sectarian conflict in between the Sunni and Shi’a communities in Iraq. As Charles Lister explains, “Zarqawi believed his organization could take advantage of the resulting chaos to cast itself as the defender of the Sunni community and to usher in the establishment of an Islamic state.”\textsuperscript{52} Similarly, it appears that IS hopes attacks on Egyptian Copts—the largest religious minority in Egypt—will ignite a civil war between Christians and Muslims, thereby enabling IS-related networks of militants to act as the defenders of the Sunni Muslim community.

III. Case Study

Methodology

The data used in this piece is drawn from two existing databases: the Global Terrorism Database (GTD), created and maintained by researchers at the National Consortium for the Study of Terrorism and Responses to Terrorism (START) at the University of Maryland, and the Armed Conflict Location and Event Data (ACLED) Project’s Africa dataset.\textsuperscript{53} Since each dataset utilizes unique data collection methods and coding schemes, I selectively integrated the data points from each source to create a single dataset containing a comprehensive account of all armed incidents in Egypt between January 1, 2011, and June 30, 2017. I then isolated all incidents in which ABM or an IS-related group—either official IS affiliate Wilayat Sinai or an


\textsuperscript{50} MEMRI, “New ISIS Video Threatens to Increase Attacks on Copts and ‘Liberate’ Cairo”; MEMRI, “In New Video, ISIS Threatens to Increase Attacks on Copts,” February 20, 2017.


\textsuperscript{52} Charles Lister, “Profiling the Islamic State,” Brookings Doha Center Analysis Paper no. 3, November 2014, 7.

\textsuperscript{53} For more information on the GTD, see http://www.start.umd.edu/gtd/; for more information on ACLED’s Africa dataset, see http://www.acleddata.com/data/.
unofficial IS-related network in Egypt—either claimed responsibility or was identified as the perpetrators by an official government statement. The dataset includes all attempted and successful attacks; those attacks that were still in the planning stages—where militants had not begun to mobilize for the execution of the assault—however, are not included. Additionally, armed confrontations between security forces instigated by a raid are not included, as the militants were not on the offensive.

For each incident, data related to four categories was collected: target type, modus operandi, location, and fatalities. The analysis of each category is then broken down into three time periods: (1) general annual trends from 2011 to 2017; (2) before ABM pledged allegiance to IS vs. after the pledge; and (3) the final six months of 2016 (from July 1 to December 31) vs. the first six months of 2017 (from January 1 to June 30).

As with all quantitative studies of terrorism and political violence, the results of this study are limited by a number of factors. First, media reports of terrorist attacks in Egypt, particularly those in the Sinai Peninsula, are inconsistent and not always reliable. For much of the ongoing insurgency in the Sinai, the Egyptian government has attempted to enforce a media blackout in the area, severely limiting both the frequency and accuracy of media reports of armed incidents. Second, and related to the limitations of media coverage in conflict zones, terrorist organizations’ claims of responsibility—and lack thereof—are not always reliable. As discussed earlier, there is a range of strategic, operational, and practical reasons why terrorist groups do not claim attacks they helped plan, prepare, and execute. Similarly, terrorist organizations sometimes claim responsibility for attacks despite having no connection to the incident in the hopes of boosting recruitment, credibility, or public support. Further, it is sometimes politically and strategically expedient for governments and rival organizations to attribute attacks to a specific terrorist organization despite the absence of sufficient evidence linking the incident to the group in question. Both of these factors complicate the post-hoc attribution of terrorist attacks. Third, using data drawn from existing databases limited the variables examined in this study and, when reports of armed incidents were in Arabic, limited the capacity to independently verify that incidents met the basic criteria for inclusion in my integrated dataset.

54 Kirkpatrick, “Militant Group in Egypt Vows Loyalty to ISIS.”
IV. Results

Number of Attacks

Between January 2011 and June 2017, ABM and IS-related networks conducted a total of 366 attacks across Egypt. There are no recorded incidents in 2011 or 2012, likely a result of the chaos that characterized the Egyptian jihadist scene in the aftermath of President Mubarak's ouster and the fact that ABM did not emerge as the dominant jihadist entity in the Sinai Peninsula until mid-2013. The first recorded incident—a suicide bombing targeting Egypt’s Interior Minister in Cairo claimed by ABM—occurred on September 5, 2013. The greatest number of attacks attributed to IS-related networks occurred in 2015, with a total of 135 incidents. From 2013 to 2015, the number of attacks attributed to ABM and IS-related entities increased steadily (see Figure 1). In 2016, Egypt witnessed a relative decrease in IS-related attacks, with a total of 93. If the rate of attacks continues apace in 2017, however, this downward trend may reverse: the first six months of 2017 alone witnessed 63 IS-related terrorist attacks.

Before vs. After Pledge

Since ABM’s leadership pledged bay’a to Abu Bakr al-Baghdadi, IS networks in both the Sinai Peninsula and the Egyptian mainland have conducted terrorist attacks with much greater frequency. Only 16.4% of attacks attributed to ABM and IS networks occurred before November 10, 2014. Following ABM’s transition to IS’s orbit, on the other hand, IS-related militants have conducted 306 attacks across the country.

Figure 1: Yearly Number of ABM and IS-Related Attacks in Egypt, January 1, 2011 to June 30, 2017

*Data for 2017 only includes data from January 1 to June 30
2016 vs. 2017

Examination of attacks attributed to and/or claimed by IS-related networks in Egypt over the previous year reveals that the militants have carried out attacks with much greater frequency in the first six months of 2017 when compared to the previous six months. From July 1 to December 31, 2016, IS-related entities conducted 30 attacks; within the first six months of 2017 alone, the same networks have conducted a total of 63 attacks, more than double that of the previous six months. There are no indications that this trend will abate in the latter half of 2017.

Target of Attacks

Examination of the targeting patterns of ABM and IS-related attacks reveals a gradual targeting radicalization: while attacks in 2013 were largely limited to assaults on symbols and individuals associated with the government and security services, beginning in 2014—and escalating dramatically in 2015—militants widened the definition of legitimate targets to include civilians and minority groups, particularly Coptic Christians. In fact, attacks targeting Copts constitute 15.9% of all IS-related assaults from January 1 to June 30, 2017—compared to merely 3.3% of all attacks in the latter half of 2016. Additionally, between 2015 and 2017 militants increasingly targeted Israeli interests.

Table 1. Targets of ABM and IS-Related Attacks in Egypt

<table>
<thead>
<tr>
<th>TARGET TYPE</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government/security services</td>
<td>-</td>
<td>-</td>
<td>13</td>
<td>34</td>
<td>108</td>
<td>78</td>
<td>45</td>
</tr>
<tr>
<td>Civilians</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>20</td>
<td>18</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Utilities</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>5</td>
<td>-</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>Aircraft</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Christians</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Israel</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Other religious figures/institutions</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Other militant groups</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Unknown</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>2</td>
<td>-</td>
</tr>
</tbody>
</table>

Before vs. After Pledge

While little scholarship is dedicated to explaining and analyzing ABM’s ideology, experts agree that the organization “always presented itself as a defender of the local Sinai population.”55 It is clear from the data that ABM’s perception of itself as guardian of the local population

informed its target selection: prior to pledging allegiance to IS, 71.7% of ABM attacks targeted entities or individuals associated with the government and/or the state security services. The relatively discriminate nature of the group’s attacks was likely also informed by the lessons of the terrorist insurgency in the 1990s, namely that mass-casualty attacks targeting civilians were likely to backfire against the perpetrating organization. In this respect, ABM was closely aligned with AQ’s belief in the importance of cultivating popular support among the local population.56

The transition from ABM to Wilayat Sinai, however, dramatically altered the organization’s targeting patterns. As can be observed in Table 1, even while IS-related networks continued to target the government and security services, civilians and other minority religious groups emerged as major targets. In 2015, 20% of all IS-related attacks within Egypt were directed at non-government targets; thus far, 28.6% of attacks in 2017 targeted entities other than the government or the security services. Included among these non-government targets are members of the Coptic community. Aside from a single attack in February 2014, all recorded terrorist attacks on Copts occurred after ABM pledged allegiance to IS. This trend is discussed in greater detail below.

2016 vs. 2017

Comparison of the entities targeted by IS networks across Egypt in the final six months of 2016 and the first six months of 2017 illuminates that militants remained committed to targeting entities associated with the government and security services. During both periods, less than 30% of attacks were directed toward soft targets, entities not associated with the government. Interestingly, the 2017 period witnessed three IS attacks targeting Israel, compared to a single attack targeting Israelis in the latter half of 2016. It is not immediately clear what observers should make of this shift, but the apparent return to focusing attacks on Israel and Jewish targets is a notable development.

The major change, however, is that in the first six months of 2017 attacks targeting Christians occurred with greater frequency than any previous six-month time in the period under study. In the six months between January 1 and June 30, 2017, IS-related militants executed ten attacks targeting Egyptian Copts, twice as many assaults as ABM and IS networks conducted in the 36 months between 2014 and 2016 combined (see Table 2). Further, attacks targeting Copts constitute 15.9% of all IS-related assaults thus far in 2017—compared to merely 3.3% of all attacks in the latter half of 2016.

56 Lister, “Al-Qa’ida Plays a Long Game in Syria.”

148
ABM's only claimed attack targeting Christians occurred in February 2014 following a suicide bombing aboard a South Korean church’s tour bus at the Taba border crossing with Israel. The attack killed three South Koreans and the Egyptian driver. Despite targeting a Christian tour group, ABM’s post-attack statement framed the incident as falling “within our… economic war on this traitorous agent regime,” suggesting tourists were a higher priority target for ABM than Christians.\(^{57}\) While the group did not claim other attacks targeting Christians, Egypt expert Mokhtar Awad has written that ABM is “believed to have been quietly targeting Christians since 2013.”\(^{58}\) If proven true, this suspicion would call into question the notion that IS targeting of Copts is a novel strategic development. Nonetheless, even if ABM did conduct targeted attacks on Copts prior to pledging allegiance to IS, publicly claiming responsibility for these attacks is a novel development.

### Table 2. ABM and IS-Related Attacks Targeting Christians in Egypt

<table>
<thead>
<tr>
<th>Date</th>
<th>Target Type</th>
<th>MO</th>
<th>Location</th>
<th>Fatalities</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/16/14*</td>
<td>South Korean tourists</td>
<td>Suicide bombing</td>
<td>Sinai (south)</td>
<td>4</td>
</tr>
<tr>
<td>4/12/15</td>
<td>Evangelical church</td>
<td>Explosive</td>
<td>Sharqia</td>
<td>0</td>
</tr>
<tr>
<td>4/12/15</td>
<td>St. Joseph Church</td>
<td>Explosive</td>
<td>Sharqia</td>
<td>0</td>
</tr>
<tr>
<td>6/30/16</td>
<td>Rafael Moussa - priest</td>
<td>Armed assault</td>
<td>Sinai (north)</td>
<td>1</td>
</tr>
<tr>
<td>12/11/16</td>
<td>Coptic church</td>
<td>Suicide bombing</td>
<td>Cairo</td>
<td>28</td>
</tr>
<tr>
<td>1/30/17</td>
<td>Christian supermarket owner</td>
<td>Armed assault</td>
<td>Sinai (north)</td>
<td>1</td>
</tr>
<tr>
<td>2/12/17</td>
<td>Coptic vet</td>
<td>Armed assault</td>
<td>Sinai (north)</td>
<td>1</td>
</tr>
<tr>
<td>2/16/17</td>
<td>Coptic teacher</td>
<td>Armed assault</td>
<td>Sinai (north)</td>
<td>1</td>
</tr>
<tr>
<td>2/22/17</td>
<td>Coptic men</td>
<td>Armed assault/kidnapping</td>
<td>Sinai (north)</td>
<td>2</td>
</tr>
<tr>
<td>2/23/17</td>
<td>Coptic man</td>
<td>Armed assault</td>
<td>Sinai (north)</td>
<td>1</td>
</tr>
<tr>
<td>2/24/17</td>
<td>Coptic man</td>
<td>Armed assault</td>
<td>Sinai (north)</td>
<td>1</td>
</tr>
<tr>
<td>4/9/17</td>
<td>St. Mark Church (Coptic)</td>
<td>Suicide bombing</td>
<td>Alexandria</td>
<td>18</td>
</tr>
<tr>
<td>4/9/17</td>
<td>St. George Church (Coptic)</td>
<td>Suicide bombing</td>
<td>Gharbia</td>
<td>29</td>
</tr>
<tr>
<td>5/5/17</td>
<td>Christian man</td>
<td>Armed assault</td>
<td>Sinai (north)</td>
<td>1</td>
</tr>
<tr>
<td>5/26/17</td>
<td>Bus of Copts</td>
<td>Armed assault</td>
<td>Menia</td>
<td>29</td>
</tr>
</tbody>
</table>

Unlike ABM, official IS propaganda outlets *Dabiq* and *Rumiyah* have claimed a number of attacks in Egypt targeting Copts. The first claim of responsibility for an attack targeting Christians in Egypt is found in the July 2016 issue of *Dabiq*. The attack, attributed to members of Wilayat Sinai, is described as an armed assault targeting Musa ‘Azmi, a Coptic priest in North Sinai.\(^{59}\) Interestingly, only four of the attacks included in Table 2 that occurred after ABM’s

---


bay'a are claimed as IS-related operations in official IS propaganda releases: the December 11, 2016, suicide bombing at a Coptic church in Cairo; the April 9, 2017, twin suicide bombings at St. Mark's Cathedral in Alexandria and St. George's Church in Gharbia; and the May 26, 2017, assault on a bus of Copts in Menia. All four incidents were major attacks, suggesting that given IS's current momentum inside Egypt the organization may be less interested in claiming small-scale attacks unless the target is notable.

It is also important to place assaults of Christians within the larger historical context of incidents targeting Egyptian Copts at both the official and unofficial level. As Joe Stark, deputy director of Human Rights Watch's Middle East and North Africa division, writes, “Historically, in areas like Minya and Assuit, which have large Coptic populations, violence erupts when personal feuds get out of hand or Muslim crowds respond violently to Christian construction (or reconstruction) of churches.” This trend has continued against the backdrop of increasing terrorist attacks targeting Copts across Egypt. In addition to these personal feuds, Copts sometimes find themselves targeted by the very security services that are meant to protect them. As Nina Shea explains, “Security forces themselves sometimes become the persecutors. Police have been known to shoot down Coptic monks and their helpers from church and monastery roofs as they make repairs…. Security forces have even used their tanks to run over Copts peacefully protesting church burnings.” However, the research for this study suggests that, at least in the period under study, incidents of this nature described by Shea are exceedingly rare.

Between 2011 and June 30, 2017, there were at least 105 armed incidents targeting Christians across Egypt that were not associated with or claimed by IS-related networks (see Figure 2 below). The frequency of these attacks peaked in 2013, with 36 incidents recorded that year. A number of researchers partly attribute this dramatic increase to the July 2013 military coup. As Shea highlights, “After the 2013 military overthrow of the Muslim Brotherhood government, mobs scapegoated the Copts and destroyed scores of ancient churches.” Largely supportive of current Egyptian President Abdel Fattah el-Sisi, the Coptic community was an easy target of Morsi supporters’ rage. Interestingly, however, as the number of IS-related attacks

---

60 Rumiyyah 5 (2017), 40.
61 Rumiyyah 9 (2017), 43-44.
62 Rumiyyah 10 (2017), 34.
63 It is possible that Wilayat Sinai or other Egypt-based IS-related networks claimed responsibility for these attacks in their own propaganda, but examination of this material is beyond the scope of this study.
67 Shea, “Do Copts Have a Future in Egypt?”
targeting Christians increased, the number of armed incidents directed at Christians unattributed to IS decreased markedly. While continued study is required to confirm this trend, it suggests that IS’s goal of stoking sectarian divisions and aggravating tensions between Muslims and Christians within Egypt is not gaining traction among the Egyptian population unsympathetic to IS’s ideology.

Figure 2. Frequency of Armed Incidents Targeting Christians in Egypt

Modus Operandi

For the duration of the period under study, ABM and IS-related networks demonstrated a consistent preference for explosives, specifically improvised explosive devices (IEDs), and armed assaults, including the use of firearms and knives. Relative to the use of projectiles and kidnapping, attacks using IEDs, guns, and knives require little monetary investment and are relatively simple to conduct. Additionally, targeting government and security service convoys with IEDs and other remotely detonated explosives are much lower risk ways for terrorists to incur casualties than through armed confrontations. Further, following Libyan Prime Minister Muammar Gaddafi’s ousting in late 2011, there was an influx of guns into the Sinai, much of which ended up in the hands of AMB-affiliated militants.  

Before vs. After Pledge

Despite the abundance of scholarship on IS’s brutal tactics, militants’ preferred modality of attack before and after ABM pledged bay’a to IS remained largely constant. The one notable

---

68 Marsh, “Brothers Came Back with Weapons: The Effects of Arms Proliferation from Libya.”
though anecdotal, difference is in the frequency of attacks using explosives: explosives accounted for 30% of attacks prior to the pledge, but were the weapon of choice in a staggering 48.7% of attacks after ABM entered IS’s orbit. The rationale behind this marked increase in the proportion of attacks using explosives is beyond the scope of this study.

2016 vs. 2017

Similarly, there were no notable changes in modalities when comparing attacks in the latter half of 2016 and those in the first half of 2017. Anecdotally, three of the four large-scale attacks targeting Christians that were claimed in official IS propaganda were suicide bombings. This does not indicate, however, a preference for suicide bombings in attacks targeting Christians; in fact, most attacks targeting Copts were armed assaults.

Location

Between January 1, 2011, and June 30, 2017, ABM and IS-related militants gradually executed attacks beyond their traditional “launching pad” in the Sinai. While in 2013 ABM militants conducted only seven attacks in mainland Egypt, by 2015 IS-related militant networks conducted 15 attacks beyond the Sinai Peninsula.

Table 3. Location of ABM and IS-Related Attacks

<table>
<thead>
<tr>
<th>Governorate</th>
<th>Before bay’a</th>
<th>After bay’a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sinai Peninsula</td>
<td>37</td>
<td>275</td>
</tr>
<tr>
<td>Cairo</td>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>Sharqia</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Giza</td>
<td>4</td>
<td>9</td>
</tr>
<tr>
<td>Ismailia</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td>Alexandria</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Dakhalia</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>Menia</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Gharbia</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Qalyubia</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Suez</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Luxor</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Western Desert</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Red Sea</td>
<td>-</td>
<td>1</td>
</tr>
</tbody>
</table>

Awad, “The Islamic State’s Pyramid Scheme,” 32.
Before vs. After Pledge

As indicated in Table 3, militants carried out more attacks in mainland Egypt after ABM pledged allegiance to IS (30 attacks) than before the group’s affiliation with the IS (21 attacks). Analysis of the proportion of attacks executed outside the Sinai, however, tells a different story: while 35% of all attacks occurred in the mainland before ABM’s pledge of allegiance to IS, a mere 9.8% of IS-related networks’ attacks have occurred beyond the Peninsula since ABM moved into IS’s orbit. These findings call into question previous arguments claiming that prior to ABM’s bay’a militants remained largely contained to the northeastern corner of the Sinai Peninsula.\textsuperscript{70} Further analysis on the lethality of IS-related attacks in the Egyptian mainland could shed further light on this issue.

Table 4. Location of IS-Related Attacks

<table>
<thead>
<tr>
<th>Governorate</th>
<th>July-December 2016</th>
<th>January-June 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sinai Peninsula</td>
<td>29</td>
<td>59</td>
</tr>
<tr>
<td>Cairo</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>Sharqia</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Giza</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Ismailia</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Alexandria</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Dakhalia</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Menia</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Gharbia</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Qalyubia</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Suez</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Luxor</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Western Desert</td>
<td>-</td>
<td>1</td>
</tr>
<tr>
<td>Red Sea</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

2016 vs. 2017

Interestingly, very few IS-related attacks occurred outside the Sinai Peninsula between July 1, 2016, and June 30, 2017: Cairo saw only one attack in in the latter half of 2016, and only four attacks occurred in various governorates in the first half of 2017. However, all but one of these five attacks were mass-casualty assaults targeting Copts. It is not immediately clear why IS-related networks did not execute attacks targeting other entities during this 12 months period, as both ABM and IS-affiliated militants had in the past. What is clear, however, is that a dramatic

\textsuperscript{70} Gold, “Wilayat Sinai,” 197.
shift has occurred: unlike the “economic war” rationale for ABM’s February 2014 attack targeting Christian tourists, the fact that all but one IS attack outside the Sinai targeted Christians suggests that Copts are now regarded by IS-affiliated militants as a primary target.

Fatalities

Between January 2011 and December 2015 the total number of fatalities from ABM and IS–related attacks gradually increased, after which point fatalities decreased (see Table 5). Whereas ABM was responsible for only 45 deaths in 2013, successor IS–related networks were responsible for a total of 446 fatalities in 2015. Even when Wilayat Sinai’s October 2015 attack on a Russian airliner—responsible for 224 deaths—is removed from the sample, fatalities from IS–related attacks still peaked in 2015, at 222 deaths. While the total number of fatalities decreased to 208 in 2016, if current trends continue the total number of fatalities will increase again in 2017.

Before vs. After Pledge

After pledging allegiance to Baghdadi, IS–related networks were responsible for over four times as many fatalities than their ABM predecessors (see Table 6). The lethality of IS–related attacks, however, decreased after ABM’s bay’a: before the pledge ABM attacks resulted in an average of 2.98 fatalities per attack, whereas after the pledge IS attacks resulted in an average of 2.75 fatalities per attack.

<table>
<thead>
<tr>
<th>Fatalities</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fatalities</td>
<td>-</td>
<td>-</td>
<td>45</td>
<td>153</td>
<td>446</td>
<td>208</td>
<td>171</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fatalities</th>
<th>Before bay’a</th>
<th>After bay’a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fatalities</td>
<td>179</td>
<td>844</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fatalities</th>
<th>July-December 2016</th>
<th>January-June 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fatalities</td>
<td>90</td>
<td>171</td>
</tr>
</tbody>
</table>
Similarly, IS-related networks were responsible for 171 fatalities in the first half of 2017, almost double the 90 fatalities in the latter half of 2016. Attacks in the final six months of 2016, however, had an average lethality greater than those in the first half of 2017. In the first half of 2017, attacks targeting Egyptian Christians have become more fatal than those in the preceding six months. In the latter half of 2016, IS networks were responsible for the death of 28 Christians—all of which occurred in a single attack; these deaths account for 31.1% of all fatalities from IS-related attacks in the second half of 2016. In the first six months of 2017, on the other hand, IS-related networks were responsible for the death of 112 Christians—eight in armed assaults and 104 in large-scale attacks. In sum, these deaths account for 42.9% of fatalities from IS-related attacks in this period.

IV. Summary and Implications for the Future

Between January 1, 2011, and June 30, 2017, patterns in the frequency, location, target(s), and lethality of attacks claimed by or attributed to ABM or an Egyptian IS-related group underwent substantial change, while the attacks’ modus operandi remained largely consistent over time. Since ABM’s leadership pledged bay’a to IS leader al-Baghdadi, the frequency of attacks conducted by IS networks across Egypt has increased substantially. Further, attacks attributed to and/or claimed by IS-related networks in Egypt over the previous year reveals that the militants have carried out attacks with much greater frequency in the first six months of 2017 when compared to the previous six months. Concurrent with an increase in the frequency of attacks, over the period of study ABM and IS-related attacks underwent a gradual targeting radicalization, increasingly targeting civilians and minority groups, particularly Coptic Christians. Attacks targeting Copts constitute 15.9% of all IS-related assaults thus far in 2017—compared to merely 3.3% of all attacks in the latter half of 2016. Further, unlike ABM, which claimed only a single attack targeting Christians, official IS propaganda outlets Dabiq and Rumiyah have claimed a number of attacks in Egypt targeting Copts. After pledging allegiance to Baghdadi, IS-related networks were responsible for over four times as many fatalities than their ABM predecessors. Similarly, IS-related networks were responsible for 171 fatalities in the first half of 2017, almost double the 90 fatalities in the latter half of 2016.

There are some indications that IS may be succeeding in fostering tensions between the Muslim majority and Christian minority within Egypt. Following a series of IS-claimed attacks in the Sinai left at least seven Christians dead, Coptic families and students, fearing for their
lives, began to flee the peninsula.\textsuperscript{71} Within a single month “the internal displacement [had] reached a scale rarely seen in Egypt outside natural disasters.”\textsuperscript{72} Despite Sisi’s condemnation of the terrorist attacks and call for security forces to “completely eradicate terrorism in northern Sinai,” some Copts have begun to question the government’s capacity and willingness to protect its civilians.\textsuperscript{73} After IS claimed responsibility for a suicide bombing at the seat of the Egyptian Coptic Church in December 2016, President Sisi faced public criticism from both victims’ families and Coptic activists.\textsuperscript{74} As attacks continue, it is likely that Sisi’s relationship with Egyptian Copts will continue to deteriorate.

Increased pressure from Egyptian security services and rising opposition among local populations has threatened Wilayat Sinai’s launching pad in the Sinai, forcing the group to seek out alternative operational bases.\textsuperscript{75} Yet, the geographic dispersion of attacks claimed by IS-related cells over the previous six months—reaching as far as Alexandria, Menia, and the Western Desert—and the lethality of attacks outside the Sinai Peninsula suggests that the IS network within Egypt is alive and well. There are no indications to suggest IS networks within Egypt will execute attacks less frequently, stop targeting Christians, curb their westward expansion into mainland Egypt, or seek to conduct less lethal attacks. In fact, if the previous six and a half years serve as a guide, IS-related networks may begin more aggressively and explicitly targeting other religious and ethnic minorities within Egypt in the hopes of exploiting any potential fault line.

\begin{footnotesize}
\begin{itemize}
  \item \textsuperscript{72} Tamer El-Ghobashy and Dahlia Kholaif, “Egyptian Christians Fearing Terror Flee Sinai,” \textit{The Wall Street Journal}, February 26, 2017.
  \item \textsuperscript{73} Aboulenein, “Egypt’s Christians Flee Sinai Amid Islamic State Killing Spree.”
  \item \textsuperscript{74} El-Ghobashy and Kholaif, “Egyptian Christians Fearing Terror Flee Sinai.”
  \item \textsuperscript{75} Abdullah, “IS Loses Ground in Sinai, Searches for Other Foothold in Egypt.”
\end{itemize}
\end{footnotesize}
Sarah Gilkes is an M.A. candidate in the Security Studies Program at Georgetown University, concentrating in terrorism and sub-state violence. Her research interests include domestic terrorism and homegrown violent extremism; radicalization processes; deradicalization methods, programs, and initiatives; and the intersection of counterterrorism policy and law at the national and international levels. Sarah has previously held positions as a political-military analyst for OSD Policy and as a Research Associate for the Program on Extremism (POE) at George Washington University. While at Georgetown, she has worked as Dr. Daniel Byman’s research assistant and served as a teaching assistant for an undergraduate course in International Law. Her work has been published by The Washington Post, POE, American Security Project, and GSSR. Sarah graduated with honors from Colgate University with a B.A. in Religion.
Individual Choice, National Consciousness: Cyber Hygiene

Christen Soden

Individuals must practice cyber hygiene, not only for their personal protection but for the greater national security. Malicious actors can use individual lapses in cyber hygiene to access restricted networks and weaponize devices, exposing state secrets and disabling critical infrastructure. However, cyber hygiene presents a collective action problem and requires a government campaign or incentive structure to mobilize compliance. Academics and practitioners have looked to the public health model for answers. However, the public health model has several shortcomings for application to cyber, including the need for a new federal regulatory authority, enforcement of individual compliance, the importance of mission-oriented non-governmental and quasi-governmental organizations, and the stronger tie to self-interest.

This article suggests an alternative model for consideration: the Federal Civil Defense Administration (FCDA), and the post-World War II devolution of civilian defense to the state and local levels. This structure depended less upon regulations and compliance enforcement, and more upon local civilian defense units to provide functional adaptability and local surge capacity.

Cyber hygiene’s importance transcends the potential negative individual effects of neglect, and impacts the entire online ecosystem—and even national security. Cyber hygiene describes the basic steps that individuals take to ensure that malicious actors do not compromise or use their digital data or computer systems. Unfortunately, the irregularity of public adherence to cyber hygiene recommendations has forced the cybersecurity community to look to other fields for models to promote cyber hygiene. Much of the literature cites the public health system as a useful model, given its focus on information sharing and public awareness campaigns. However, the government regulates individual compliance with many of the mandates that enable the public health system to function. In this article, I examine whether governments must similarly regulate the communal responsibility for cyber hygiene, and if the current legislative environment will even permit those types of regulations. Alternatively, I explore whether the incorporation of lessons from other public responses to national security threats and technological changes—such as the threat of nuclear war—adequately supplement the non-regulatory sides of the public health model, and thereby avert the need for cyber hygiene regulation.

I begin this article by discussing the importance of cyber hygiene and then review the extent and severity of the threat from poor cyber hygiene habits amongst the broader populace.
Then I introduce the public health model and assess its applicability to cyber hygiene. Finally, I introduce a different model for affecting public behavior—the Federal Civil Defense Administration (FCDA) model—and demonstrate how this model may provide the most viable option for tackling the cyber hygiene issue either singularly, or in conjunction with relevant elements of the public health model.

**Why is Cyber Hygiene Important?**

Standard cyber hygiene practices include prompt and consistent installation of software updates, use of different, strong passwords that are regularly changed, disengagement from risky online behavior such as downloading or visiting unsecure websites, and vigilance against spear-phishing attempts. Cyber hygiene protects individual computer users by, for example, preventing viruses from entering their systems via vulnerabilities in software that users have not updated or by ensuring that, by the time a cyber-criminal tries to use their stolen credentials, the user has already completed a routine password change. Individual cyber hygiene also protects the broader cyber community. Once a virus or attacker compromises a computer system, they can turn that computer system against other computers in the cyber domain by spreading viruses or worms, or using the computer as a botnet to attack and overwhelm other websites, systems, etc. This communal threat can escalate to a national security threat when these malicious activities target the nodes and systems considered critical to national security, such as electric grids or financial system infrastructure. In addition, the US national security infrastructure and government are staffed by employees from a populace whose acceptance of cyber hygiene practices is neither consistent nor normalized, and this increases the likelihood of mistakes from those who should arguably “know better.” Ultimately, the best defense is, simply, strong defensive practices: “regardless of which side has the advantage, any steps that raise the capabilities of the defense make life harder on the offense and limit the incentives for attacks in the first place.”

Thus, even when specialized and complex threats to cybersecurity such as previously undiscovered security flaws in software—known as zero days—exist, the average computer user’s actions are critical. In fact, exploits of zero days are quite rare, and Curtis Dukes of NSA said in September 2016 that of the “high-profile [cyber] incidents” of the past two years, none of them were related to zero days. Most exploits take advantage of previously identified vulnerabilities.

---


under the assumption that many users have not upgraded their software (in fact, the release of the software upgrades often reveal vulnerabilities to cyber criminals and “bad actors”).

How Bad is the Cyber Hygiene Problem?

A February 2015 survey recorded that 20% of Internet Explorer users still use Internet Explorer 8 (released in 2009), and 20% of all desktop-computer users employ Windows XP (released in 2001, and for which Microsoft no longer issues security updates). Meanwhile, even though cyber hygiene advocates have actively promoted secure password habits for years, a Pew survey recently revealed that only “39 percent of Internet users ever changed their passwords.” Neglect of “minor” cyber hygiene fixes can have major real world consequences, by establishing the baseline conditions for common attack techniques. For example, a successful phishing campaign that sent Word documents with embedded macros to the emails of Ukrainian utility workers, led to the December 2015 Russian hack of the Ukrainian power-grid. When the macros were enabled, they installed a program that acted as a backdoor for the hackers into the utility IT system. Once there, the hackers mapped the system to find the virtual private network (VPN) credentials that the utility workers used to remotely access the supposedly segregated—by firewall—Supervisory Control and Data Acquisition (SCADA) network that ran the grid.

The cyber hygiene problem originates from a variety of behavioral and awareness weaknesses, which can only be addressed through a massive shift in how these issues are communicated to and conceptualized by the broader public. First, computer users feel powerless amidst a mind-boggling level of complexity, and therefore will not take the initiative to improve their cyber hygiene even if they are told it is important for the public good. As Quinn Norton outlines in her article “Everything is Broken,” “your average piece-of-shit Windows desktop is so complex that no one person on Earth really knows what all of it is doing, or how. Now imagine billions of little unknowable boxes within boxes constantly trying to talk and coordinate tasks at around the same time, sharing bits of data and passing commands around from the smallest little program to something huge, like a browser — that’s the internet... Because of all this, security is terrible.” Even informed members of the cyber community find these issues complex. It is unreasonable to expect the average user to embrace cyber hygiene rituals with the sense of

---

ownership that ensures lasting and consistent change, without the massive shift in public messaging advocated above.

Beyond the technical complexity of the issue, there are several pervasive societal behaviors that increase the population’s susceptibility to cyber hygiene deficiencies. For example, in Arun Vishwanath’s research, he found that most people “pay limited attention to email content, focusing instead on quick clues that help expedite judgment.” Our “ritualized media habits that our always-on and accessible smartphones and tablets enable” exacerbate this tendency, ensuring that we automatically process email without thoughtful consideration or assessment of potential threat indicators. Vishwanath argues that this pattern of processing amounts to a societal habit—i.e. “our brain’s way of automating repeatedly enacted, predictable behaviors”—and that this broad absence of cognitive processing leads to the same susceptibility levels to spear-phishing across technological sophistication levels.

As such, “the current approach of training people to be vigilant about suspicious emails remains largely ineffective” because “vigilance is a short term strategy and it is difficult to maintain a high state of alert at all times.” Instead, Vishwanath advocates for the replacement of poor cyber habits—such as habitual media use—that expose users to threats, with “safer rituals” that “might be sustainable over the long term,” such as designating set times of day to sort through and focus on email, or the use of multiple email accounts for specific purposes—i.e. banking, business, personal, etc. However, building a framework for long-term mass ritual substitution is an imposing task.

The individual explainers for bad cyber hygiene aggregate to impact organizations and organizational culture more broadly. In particular, senior employees, “the leaders who define and shape the organization’s culture” have an outsized impact on the prioritization of security, and often embody and promulgate the most dangerous organizational traits for cyber security: lack of tolerance for inconvenience, desire for collaboration across business units, and mission-driven environments. In the same way the broader public needs an aggressive campaign for cyber

---

8 Ibid.
12 Vishwanath et al., “Why do people get phished?,” 585.
hygiene, companies and bureaucracies must “infuse… into the organizational DNA” a cyber hygiene culture without “destroying the existing culture.” A culture of cyber hygiene differs from the aforementioned cyber hygiene vigilance, in that a culture ritualizes cyber hygiene to such a point that the public complies with its requirements automatically, as opposed to the forced heightened awareness and attention of vigilance.

To be sure, several government and private sector initiatives exist to overcome cyber hygiene weaknesses and increase literacy and awareness. For example, the National Initiative for Cybersecurity Education conducts Federal Cybersecurity Training Events. On the private sector side, the Center for Internet Security (CIS) and the Council on Cyber Security jointly sponsor the Cyber Hygiene Campaign. These initiatives are vital, but without a place in a comprehensive national framework they are not enough to match the scope of the problem.

Application of the Public Health Model to Cyber

Several different cybersecurity experts focus on the public health model as an improved approach to national cybersecurity generally—with cyber hygiene awareness and promotion a component of this. However, the experts vary in their degrees of commitment to the model, the scope of their parallelism, and the ambitions of their plans. For example, in their book Cybersecurity and Cyberwar, P.W. Singer and Allan Friedman focus specifically on the implementation of a Cyber Centers for Disease Control (CDC). Cyber CDC would act as a “hub for cooperation” focused on research and information-sharing, thereby standing apart from CYBERCOM (with its Department of Defense focus on specifics of offense and the defense of their own network) and private firms, which may perform the same functions, but do so for profit.

In a similar segmentation and extraction of the public health model, Scott Charney (vice president of Trustworthy Computing at Microsoft) issued a paper in 2010 also advocating for a Cyber CDC, but with a particular focus on the quarantine aspect of the typical CDC responsibility set. Charney advocated implementing a system which would quarantine an infected device until the infection was remedied and the owner notified. Around the same time...

---

14 Ibid.
15 Davis, “Poor cyber hygiene - not zero days.”
17 Singer and Friedman, Cybersecurity and Cyberwar, 174.
19 Ragan, “Microsoft proposes a cyber CDC.”
this paper was published, Comcast released a service that—while not compulsory as Charney envisioned—would notify subscribers if their machine was part of a botnet.\textsuperscript{20}

Given his research on the behavior behind cyber hygiene compliance, Arun Vishwanath takes a much broader look at this paradigm, searching for the system that will change public habits permanently. In his article, “Everything is Broken” Vishwanath outlines multiple health-behavioral models which he believes experts could integrate into a codified cybersecurity ecosystem.\textsuperscript{21}

The missing element in Singer and Friedman and Charney’s representations of a potential Cyber CDC (and even in Vishwanath’s approach to public health models) is the regulatory authority that would need to be vested in such an organization to parallel the CDC’s capabilities and to execute the goals they envision. While Steven Hofmeyr, a computer scientist in the Computational Research Division at Lawrence Berkeley National Laboratory, believes a Cyber CDC is technologically possible, he doubts its political and organizational feasibility.\textsuperscript{22}

For instance, while the US Computer Emergency Readiness Team (US-CERT)—an organization within the Department of Homeland Security tasked with threat analysis, information sharing, and incident response—collects reports of cyber incidents and disseminates this information, there is no legal requirement for industry and the government to report incidents, as there is with the health-based CDC.\textsuperscript{23} In terms of individual actions, equivalent to “cyber hygiene,” the health-based CDC has the power to force quarantines and vaccine distribution.\textsuperscript{24} However, unlike health-based quarantines and vaccinations that focus on individuals who are or may become infected, implementing similar regulatory actions in the cyber domain presents complicated issues of liability, even if those actions similarly target individual nodes.\textsuperscript{25} While cyber “quarantines” and “vaccinations” may target individual devices, these devices comprise interconnected networks, with diffuse levels of responsibility (individual, network administrators, ISPs, etc.).\textsuperscript{26}

The Rice et al. article “Applying Public Health Strategies to the Protection of Cyberspace” addresses the muscle of government involvement more directly. The article begins by proposing a public health framework for cyber modeled from five strategies of public health developed in 1920 by Charles-Edward A. Winslow—a prominent Yale public health

\begin{flushleft}
\textsuperscript{20} Ibid.  \\
\textsuperscript{21} Vishwanath et al., “Why do people get phished?,” 585.  \\
\textsuperscript{22} Ibid.  \\
\textsuperscript{23} Ibid.  \\
\textsuperscript{24} Vishwanath et al., “Why do people get phished?,” 585.  \\
\textsuperscript{25} Ibid.  \\
\textsuperscript{26} Ibid.
\end{flushleft}
theoretician—which includes: (i) sanitizing the environment; (ii) controlling community infections; (iii) educating the actors; (iv) organizing detection and prevention services; and (v) creating the social machinery for cyberspace health. Rice et al. then proceed to aggressively advocate for the involvement of government to “use incentives and regulations to influence individuals, communities, vendors and service providers” and to “sponsor large-scale awareness campaigns and other public education initiatives,” as well as “enforce quarantines” if necessary. Rice et al. particularly focus on efforts to improve public consciousness of cyber hygiene issues and the role that government can play in that process. For example, the authors stress the importance of cyberspace education in childhood and argue that cyber vendors should disclose proper use procedures, vulnerabilities, and risks at the same level as pharmaceutical companies.

However, Rice et al. advocate for some public health ecosystem parallels which would be immensely difficult to implement in the cyber domain and which emphasize the greater difficulty of public buy-in for cyber hygiene consciousness. For example, the article highlights the importance of non-governmental and quasi-governmental organizations in promoting education and outreach in the cyber domain, citing—amongst other organizations like the World Health Organization (WHO)—charities such as the American Red Cross and the March of Dimes. However, these independent organizations raise their funds and operate as charitable institutions that save lives and help sick people. While professional and private-sector organizations may fill the non-governmental organization niche to a certain extent, the same ecosystem of mission-oriented support organizations will simply never exist for cyber. The public health organizations derive their broad-based support from the public’s commitment to saving lives and alleviating human suffering—visceral motivators that cyber hygiene cannot match.

Meanwhile, although the Rice et al. article places most of the responsibility for this new cybersecurity paradigm with the government, it also issues a call to individuals to, “as in the public health domain…embrace, participate in and seek to improve the social machinery for cyberspace health.” Overall, this sentiment may be unrealistic. The obvious worst-case outcome of a public health disaster is death, and thus an instinctual sense of personal fear will always support the building of public health consciousness. Studies on compliance with vaccination regulations reinforce this conclusion that personal incentives motivate participation in public health activities. Vaccines rely on “herd immunity” which requires a critical mass of vaccinated

28 Ibid.
29 Rice et al., “Applying public health strategies to the protection of cyberspace,” 123.
30 Ibid.
31 Ibid., 125.
patients within a group; thus, not too many members of the community can choose to forgo vaccination and rely on the vaccinations of their neighbors for safety.\textsuperscript{32} In the United States, state-by-state regulations require a series of vaccinations before children can attend public school; however, states have different rules on exemptions for medical reasons, religious beliefs, and philosophical/personal beliefs.\textsuperscript{33} Recent trends indicate that more people choose not to vaccinate their children for philosophical and personal reasons, and that these trends tend to geographically cluster, further increasing the risk of outbreak.\textsuperscript{34} A decrease in vaccine coverage especially endangers children who cannot be vaccinated, either for medical reasons or because they are too young.\textsuperscript{35} Despite these important community obligations (protecting the young and the sick), parents choose not to vaccinate their children largely because of how they believe those vaccines will affect their children specifically. For example, parents of unvaccinated children thought their children had a low susceptibility to the disease, that the disease was not severe, and that “the efficacy and safety of the vaccines was low.”\textsuperscript{36} Not only do parents of unvaccinated children disregard the danger this poses to at-risk children within the community, but they also invest the time to navigate the process of obtaining an exemption to legislation. Thus, the public health model not only presents an imprecise corollary to cyber hygiene, but faces its own serious weaknesses. Since cyber hygiene has even less dramatic personal and empathetic pressures to motivate compliance than sick and dying children, application of the public health model to cyber hygiene would further accentuate the public health model’s weaknesses.

An Alternative Approach

If public health and vaccines offer an imperfect model for cybersecurity and cyber hygiene, other public initiatives may provide alternative or supplemental lessons and structures. The rise of civil defense groups in the US—beginning in World War I and through World War II and the Cold War—presents a comparative example. Federal government coordinating agencies like the Office of Civilian Defense in World War II and the Federal Civil Defense Administration (FCDA) from the beginning of the Cold War harnessed the efficiencies of such local groups.\textsuperscript{37} In particular, the FCDA consolidated wartime agencies and new programs to

\textsuperscript{34} \textit{Ibid.}, 1283.
\textsuperscript{35} \textit{Ibid.}, 1985.
\textsuperscript{36} \textit{Ibid.}, 1985.
provide physical protection against a nuclear attack (i.e. bomb shelters) as well as propaganda against Communism and the “Soviet military threat.”Interestingly, the local civil defense programs maintained their vitality and longevity largely because they also adopted local disaster management responsibilities. While the federal government still imposed their priorities over the local civil defense, these disaster management allowances marked what Patrick S. Roberts calls “a flexibility in the cooperative federalism of the era.” Much of the initiative and even the strategic vision of civil defense devolved to the state and local level, with state civil defense offices pursuing ties with a variety of federal agencies such as the Department of Agriculture. Essentially, the strength of the civil defense groups came not from their topical focus but from their functional adaptability, as well as their local surge capacity. Individual citizens, and not the federal government, carried out the key functions of the civil defense groups (building shelters, conducting air-raid watches, etc.), and the civil defense ecosystem organized and promoted “lasting peacetime programs to spur citizen involvement.”

The power of the FCDA as a tool for public education and the framing of the national consciousness cannot be overstated. A 2003 Slate article refers to the FCDA as a “pedagogical propaganda agency.” The FCDA issued curriculum advice to schools, produced advertisements and brochures, encouraged bomb shelter preparation campaigns, enlisted celebrities for public awareness, etc. As Roberts notes, the FDCA essentially ran an “ineffectual” shelter building program. However, the shelter program’s public relations campaign (epitomized by a cartoon turtle) was immensely successful, “spawning organizational routines, such as evacuation and warning procedures and… connections between national and state programs…” as well as the “wide adoption of civil defense at the state and local levels in the 1950s and the 1960s and the durability of these organizations, which persist in new forms to the present day.” Roberts argues that the broader Homeland Security apparatus today misses the local level civilian engagement promoted by the FCDA, to the detriment of all the programs DHS manages. He claims that, in the 1950s and 60s, state and local agencies engaged the public much more effectively than they do today, at least partially due to the movement and segregation of

38 Ibid.
39 Ibid., 366.
40 Ibid., 369.
42 Ibid., 368.
44 Ibid.
46 Ibid., 369.
homeland security programs to the law enforcement and intelligence domain. These lessons particularly apply in the realm of cybersecurity, where the complexity of the problem set and the oftentimes abstract nature of the threat (at least at the community and national security conceptual level), requires a more engaged grassroots mobilization.

The Way Forward

Cyber hygiene does not evoke the same individual immediacy and risk quotient as public health. However the public health model for cyber hygiene and cybersecurity management offers many useful frameworks for information-sharing and public education. Despite these useful frameworks, much of the literature on the public health model neglects the role of legislation and the strong regulatory authorities exercised by organizations like the CDC, as well as the current difficulty of establishing such regulatory structures for cyber at the federal level. In addition, many versions of the public health model rely upon a network of non-governmental and quasi-governmental organizations that advocates likely cannot replicate in the cyber domain. Likewise, the public health model works effectively through the network of providers of health services at the local community level, and this type of network currently does not exist for cyber. The critical impact of non-governmental and quasi-governmental organizations, as well as the integration of ground-level service providers, is less likely in cyber space due to profit and liability concerns. Therefore, in establishing any national-level structure to target individuals for cyber hygiene improvement, the government should look for innovative approaches towards grassroots and state-level engagement and consciousness-building around emerging issues. In the 1950s, the universal fear of nuclear weapons captured the public imagination. However, channeling the fear and wonder at this technological change into useful procedures and protocols required programs for individual engagement which built a sense of communal responsibility and actual community mobilization. Individual fear and public awareness campaigns alone will not lead to permanent cyber hygiene ritual replacement—local initiative and community organizations must supplement or replace these public health remedies to ensure broader cyber hygiene change.

48 Ibid., 372.
Christen Soden is an M.A. Candidate in the Security Studies Program at Georgetown University, concentrating in terrorism and sub-state violence. Her research interests include non-state actors in the Middle East and Africa, geopolitics of the Gulf and the Levant, and U.S. military and intelligence community adaptation to irregular warfare. Christen currently works as a business development intern at Northrop Grumman, and previously worked as an intern to the Deputy Assistant Secretary for Plans—Office of Policy at the Department of Homeland Security, and as the Senior Financial Analyst for the Office of Global Centers at Columbia University. She graduated from Columbia University with a B.A. in Political Science.