Senate Armed Services Committee
Subcommittee on Emerging Threats and Capabilities

March 29, 2017

‘Fighting in the “Grey Zone”: Lessons from Russian Influence Operations in Ukraine’

Testimony by
Dr. Michael Carpenter
Senior Director
Biden Center for Diplomacy and Global Engagement
University of Pennsylvania

PennBidenCenter
for Diplomacy & Global Engagement

Note: The statements, views, and policy recommendations expressed in this testimony reflect the opinions of the author alone, and do not necessarily reflect the positions of the Biden Center for Diplomacy and Global Engagement or the University of Pennsylvania.

Chairman Ernst, Ranking Member Heinrich, members of the Subcommittee on Emerging Threats and Capabilities, thank you for the opportunity to speak about the lessons learned from Russian influence operations in Ukraine.

Russia's unconventional war against Ukraine has revealed a formidable toolkit of measures for fighting in the so-called "grey zone," from world-class cyber and electronic warfare capabilities to sophisticated covert action and disinformation operations. Russia has used propaganda, sabotage, assassination, bribery, proxy fronts, and false-flag operations to supplement its considerable conventional force posture in eastern Ukraine, where several thousand Russian military intelligence advisors, unit commanders, and flag officers exercise command and control over a separatist force consisting of roughly 30,000-40,000 troops.

Moscow has been doing its homework. Recognizing that Russia's conventional military capabilities lag behind those of NATO, Russian Chief of the General Staff Valeriy Gerasimov called in 2013 for investing in asymmetric capabilities to enable Russia to fight and win against conventionally superior Western militaries. Gerasimov's call for more emphasis on unconventional warfare also coincided with a subtle but important shift in Russian foreign policy. After Mr. Putin's return to the Kremlin in 2012, Moscow dispensed with its post-Cold War foreign policy of cooperating with the West where possible and competing where necessary. Instead, the Kremlin now actively seeks to corrode the institutions of Western democracy, undermine the transatlantic alliance, and delegitimize the liberal international order through a continuous and sustained competition short of conflict that takes place across all domains.

However, even with Russia's well-honed unconventional warfare capabilities, the United States and its NATO Allies can prevail in this competition if we recognize the Kremlin's goals for what they are, develop smart strategies to counter them, properly align our institutional structures, and invest in the right capabilities.

I will briefly discuss six areas where Russia has invested in significant unconventional or "new generation warfare" capabilities, and suggest some responses the United States should consider. All of the capabilities I will highlight were used during Russia's invasion of Ukraine in 2014 and remain on display as Russia continues to wage its unconventional war against the government in Kyiv.

Information Warfare

First, Russia has demonstrated a mastery of the tools of information warfare. Russia's intelligence services understood through their "operational preparation of the environment" (OPE) how to tailor messages that would resonate with the population of eastern Ukraine. Such efforts began long before the Maidan protests as networks of influence were established across virtually all of Ukraine's government and military institutions, allowing for rapid activation once the conflict began. Immediately after President Yanukovych's ouster, Russian media outlets and government officials began to disseminate a narrative that Yanukovych had been forced out of power by Ukrainian fascists supported by the West. This propaganda was so insidious that even an 86-year-old Ukrainian-American living in the United States whose sole source of news is Russian TV could believe that a fascist government had come to power in Kyiv.

It is not just the message that matters, but also Russia's virtual monopoly of the medium. To guarantee its control of information, one of the first operations Russian special services carried out inside Ukraine in the spring of 2014 was to seize key television transmission towers. This monopoly on broadcast television lasted until only recently. In December 2016, Ukraine inaugurated a new television tower near Slovyansk to broadcast its own public programming into occupied eastern Ukraine, while Ukrainian public radio only began broadcasting into the Donbas in January 2017.

To counteract Russian propaganda, the United States needs to take a more pro-active approach. U.S. European Command led the way during the Ukraine crisis by revealing de-classified images of Russian tanks and equipment, and NGOs like Bellingcat followed suit with further proof of Russia's involvement, including evidence of Russia's role in the shoot-down of MH-17. However, more is needed beyond simply publicizing evidence of Russian aggression. The United States should consider making greater use of regulatory tools to label Russian propaganda for what it is, for example by mandating a screen banner warning viewers of *RT* or *Sputnik* that they are watching Russian government programming. An independent commission should also be established to identify and take action against Russian misinformation. In parallel, the 2016 Countering Disinformation and Propaganda Act should be used to spur the development of a robust whole-of-government toolbox for exposing and countering Russian propaganda, ideally drawing on expertise outside of government.

Counter-disinformation strategies will also be more effective when coordinated across the NATO Alliance, particularly since Russian disinformation has found fertile ground in many European societies. Expanding the funding and mandate of the NATO Center of Excellence on Strategic Communications in Latvia would help share best practices on counter-messaging. The Center should also explore how to use big data analytics and other social media tools to counteract Russia's well-financed army of internet bots and trolls. For example, technological solutions should be explored, including "spam filters" for content generated by programmed bots.

Finally, the United States should not limit itself to refuting lies in the Western media space but should take a more active role in exposing lies and corruption within Russia. Those who claim Russian citizens are inured to revelations of high-level corruption or Russian military involvement in the war on Ukraine do not understand what the Kremlin knows well. Russian opposition politician Boris Nemtsov was murdered only a few hundred yards from the Kremlin in part because he had revealed information about the Russian military's direct involvement in the war in Ukraine. Exiled Duma lawmaker Denis Voronenkov was murdered last week in Kyiv because he was ready to speak about Russia's ties to Yanukovych and the war in Ukraine. The

Russian NGO Soldiers' Mothers was declared an "undesirable foreign agent" by the Russian government after its members exposed the cover-up of Russian service-members' deaths in Ukraine. Clearly, the Kremlin does not want this information to be disseminated within Russia and is willing to go to extreme lengths to silence these voices. Protests across Russia just within the last few days also provide ample proof that Russian citizens do not accept corruption as a way of life.

To speak directly to Russian citizens and Russian speakers, the United States should devote more resources to projects like *Current Time*, the Broadcasting Board of Governors' new 24/7 Russian-language digital network, which provides information to Russians and Russian-speaking audiences on Russia's periphery. The U.S. should also consider supporting efforts like Estonia's Russian-language public television station, which has filled an important vacuum in the Baltic region's information space.

Cyber Operations

A second unconventional tool Russia is using to great effect in Ukraine is cyber-attacks, which range from "hacking" Ukrainian networks to steal information for intelligence or propaganda purposes to crippling denial of service attacks on critical infrastructure. At the start of the conflict, the deployment of Russian special forces to Crimea was accompanied by cyber-attacks on cellular and internet connections to disrupt the government's ability communicate with its citizens. Similar operations were launched in Georgia during Russia's invasion in August 2008. Cyber operations were also augmented by the use of electronic warfare equipment to block cellular and radio signals used by the Ukrainian Armed Forces as well as civilians.

Cyber-attacks against Ukraine have escalated since the conflict began. In December 2015, evidence shows Russia hacked into the Supervisory Control and Data Acquisition (SCADA) networks of two Ukrainian energy companies, shutting off electricity and heat for a brief period before Ukraine was able to restore power. The attacks on the SCADA systems were accompanied by distributed denial of service (DDOS) attacks on telephone-operated customer call centers so complaints of a power outage would not get through to company operators. However, even when Russia was identified as the perpetrator of this attack, it was not deterred. In December 2016, Ukraine's power grid suffered another cyber-attack, and Russian cyber actors separately targeted Ukraine's payments system for government salaries and pensions. These attacks should serve as a wake-up call for the West, particularly since many Western power companies lack the backup manual functionality that helped Ukraine avert what could have otherwise been a crippling power shutoff. The potential for disruptive cyber action is enormous and deterrence is complicated by the difficulty of attribution. While recent discussions of Russia's cyber-attacks in the United States have focused on hacking and disclosure of information, we must not overlook the fact that Russia's cyber weapons have a potential lethality and scope that is matched only by strategic nuclear weapons.

The Defense Department must therefore invest more in U.S. Cyber Command's capabilities, and the United States should also continue to help build our Allies' and partners' cyber-defenses, which in many cases are more vulnerable than our own. Election-day attacks in Montenegro in October 2016 not only spread disinformation about the election on social media platforms such as Viber and WhatsApp, but also targeted the Ministry of Defense's network. At a December meeting of the U.S.-Adriatic Charter, defense ministers from across the Balkans noted their cyber defenses needed to be urgently upgraded in the face of increased Russian cyber activity.

U.S.-based efforts should also include stronger regulatory oversight to ensure standards are met for hardening critical infrastructure against cyber intrusions and attacks since much of this effort is currently left at the discretion of the private corporations that manage this infrastructure. Admiral Stavridis' suggestion to establish a National Cyber Academy is also worth considering, and the Defense Department's public-private partnerships with the information technology sector, like the Defense Innovation Unit Experimental (DIUx) launched by former Secretary of Defense Carter, should be expanded.

Finally, in cases where NATO or the United States are able to attribute a specific attack, the response must be timely and proportionate to deter future attacks. In the case of the cyber-attack against the United States during the presidential election, the declaration of Russian intelligence officials as *persona non grata* (PNG) is unfortunately a largely symbolic action with few lasting consequences given that these positions will soon be backfilled with other operatives. As long as Russian cyber actors encounter weak resistance, the Kremlin will continue to leverage its cyber capabilities against the West.

Clandestine and Covert Operations

Third, Russia's intervention in Ukraine demonstrates a mastery of the art of clandestine and covert operations. During its armed takeover of government buildings and military installations in Crimea in 2014, Russia deliberately chose to deploy what are now known as "little green men," or special forces in uniforms without insignias. The deployment of these semi-overt, semi-covert forces allowed Russia to maintain the fiction on the international stage that the conflict involved only local actors. At the same time, it made perfectly clear to those on the ground that the troops were in fact highly capable Russian special forces. Through this "asymmetric ambiguity" Russia was able to stave off the international community's immediate condemnation while simultaneously deterring Ukraine's interim government from fighting back. In essence, the Russian General Staff set the same trap it used in Georgia in 2008 when it covertly deploy special forces to create unrest: if the host government fights back and there are casualties, then the Kremlin is handed a pretext for launching a war to protect Russian compatriots; if the host government chooses not to fight, Russian forces have a free hand. In either case, Russia wins.

In addition to its semi-overt "little green men," Russia also deployed true covert operators to the Donbas. These "little grey men" organized and sometimes even led demonstrations and seizures of government buildings and police stations across eastern Ukraine in the spring of 2014. In April 2014, for example, Russian covert actors organized the seizure of the Kharkiv Opera House, which they mistakenly believed was City Hall, using paid protestors who had been bussed in from outside the city. A deadlier and more tragic incident occurred in May 2014 when pro-Kremlin protestors barricaded themselves inside a building in the port city of Odessa, which was then set on fire.

Importantly, Russia's covert agents were far less successful in stoking separatist sentiments in other parts of southern and eastern Ukraine than they were in Crimea. Thanks to the social resilience of the local population and more effective local law enforcement operations, Russian-directed efforts to foment anti-government insurgencies failed in major cities like Kharkiv, Odessa, Dnipro, and Mariupol. Russia's recent attempted coup d'état in Montenegro is also illustrative of how effective collaboration between intelligence and law enforcement agencies can thwart such covert operations. In the Montenegrin case, Russian military intelligence officers recruited mercenaries among far-right nationalist groups in Serbia and local criminal elements and hatched a plan for them to fire on anti-government protestors on election day while wearing stolen Montenegrin police uniforms. Fortunately, a tip-off and good intelligence work prevented the plot from moving forward as planned.

More broadly, defeating or neutralizing influence operations requires strengthening societal resilience through government programs that build stronger ties to disaffected ethnic groups or communities that are less well integrated into a country's social fabric. This requires a "whole-of-government" approach that coordinates among ministries of defense, internal affairs, and intelligence bodies, as well as health, social, and economic agencies. Finally, awareness of the threat is critical. In the Ukrainian case, Russia's operation in Crimea was successful in part (though there were other reasons) because it occurred first. Once Ukrainian citizens became aware that Russian forces were intervening militarily in their country, subsequent operations proved much more difficult even in areas where there were historically high levels of distrust in the central government. Within NATO it is vital for the Alliance to develop Indicators and Warnings (I&W) that rely not only on military factors, but also on social trends and dynamics.

Proxy Forces

Fourth, Russia relies on a range of proxy groups to carry out subversive actions and fight as irregular forces. In Ukraine, these groups include local organized criminal groups, Yanukovych-regime thugs known as *tytushki*, former Berkut riot police, Cossacks and Chechen fighters who came from Russia, members of the infamous Russian "Night Wolves" motorcycle gang, and a smattering of Russian and East European neo-Nazi volunteers. This medley of proxy groups proved to be little match initially for Ukraine's conventional military in the summer of 2014, during which Ukrainian forces succeeded in retaking significant territory. However, when it appeared that Ukraine might actually defeat the separatist forces, Russia intervened with a large number of conventional brigade combat teams that were ready and waiting in staging areas near the Ukrainian border.

Even after the tragic defeat of Ukrainian forces in Ilovaysk in August 2014, the Russian military encountered considerable difficulties with command and control of its proxies. Rampant criminality also prevailed as the various proxy groups organized themselves into mini-fiefdoms. This led the Kremlin to send high-level emissaries to reign in the various warlords, and when that failed special forces even resorted to assassination and forced extraction from the battlefield. The leader of the Cossack Great Don Army, Nikolai Kozitsyn, was for example forced out of the Donbas by Russian services. Another prominent Russian commander, Igor Strelkov (aka Igor Girkin), was also removed. To instill greater professionalism among its proxy forces, therefore, Moscow has increasingly turned in both Ukraine and Syria to private military companies.

I would contend that Moscow's greatest success with proxy groups has not been on the battlefield but on the diplomatic stage. Using the Geneva International Discussions on Georgia as a model, the Kremlin has insisted that no negotiations take place without the involvement of proxy leaders. One of the biggest mistakes made by the Western leaders of the "Normandy Group" (France, Germany, Ukraine, Russia) was to agree to Russia's demands and elevate the role of Russian proxies in the February 2015 Minsk Protocol. By establishing a parallel negotiation process involving proxies, Russia has largely been able to evade blame for its failure to implement even the most basic elements of the Minsk agreement: ceasefire, withdrawal of heavy weapons, and unlimited access for OSCE monitors to the territory of the Donbas. The result is a kabuki negotiation led by the OSCE in which the proxies stonewall any meaningful progress on implementing the agreement. So long as this dynamic is maintained and Moscow is able to hide behind the claim that local leaders are to blame for the impasse, the conflict will almost certainly continue unabated. Conversely, the sooner the international community cuts through the fiction that local actors call all the shots and applies pressure on Moscow, the closer we will be to a real negotiation aimed at resolving the conflict.

Sabotage and Terrorism

Sabotage and acts of terrorism have also been used in the Ukraine conflict. On the same day that former Duma member Denis Voronenkov was assassinated in Kyiv, an act of sabotage destroyed a large munition depot in Balaklia, forcing the evacuation of 20,000 civilians form nearby areas. Earlier in the conflict, Ukraine's security service, the SBU, accused Russia of having orchestrated a bombing attack on a rally in Kharkiv in February 2015 that killed a policeman and a civilian as well as bombing attacks on railroads, a courtroom, a pub frequented by pro-Maidan supporters, and the offices of a pro-Maidan NGO. Given the long border between Russia and Ukraine and extensive societal and family ties between the two countries, preventing acts of terrorism and sabotage remains difficult and relies heavily on good intelligence and societal resilience.

Political and Economic Subversion

Finally, political and economic subversion have increasingly become Russia's favored method of seeking to exert control over the government in Kyiv. Indeed, Russia has increased its political influence operations not just in Ukraine but throughout Europe and the United States, seeing them as a cheaper and more effective way to achieve its aims in the grey zone. Unconventional military operations carry a significant degree of risk, while political influence operations are easier to carry out and are camouflaged behind an often convoluted façade of corrupt business and political ties.

As part of this subversive campaign, Russia's intelligence services and Kremlin-linked oligarchs have targeted Western political parties, businessmen, politicians, media organizations, and NGOs. The goal is not always to influence a near-term political outcome, but sometimes simply to burrow into a country's political and economic fabric. In this way, corrupt ties and *kompromat* (material for blackmail) can be built up in reserve and deployed at the opportune moment. The primary tool used in these influence operations is Russia's vast network of corrupt patron-client relations, which extend not only to the former Soviet space but also to Europe and the United States. Russian businessmen who have professional ties in a particular country can be "encouraged" to donate money to select NGOs, offshore companies can be used to funnel money to political parties, and Russian cultural organizations such as state-run *Rossotrudnichestvo* can be used to forge ties with pro-Kremlin diaspora groups. Money laundering schemes using shell companies or "one-day firms" help to channel the flow of licit and illicit money from these various actors to favored politicians, NGOs, and media organizations.

To counteract this rising tide of Russian political subversion, Western states need to build more transparent institutions, particularly with regards to political party financing, and empower anti-corruption organizations, financial investigation units, and law enforcement bodies to coordinate with intelligence organizations to root out entrenched and corrosive Russian patronage networks. The United States should seriously consider establishing a standing interagency operational body dedicated solely to interdicting illicit Russian influence operations. Current interagency efforts to track Russian malign influence are not sufficient because of the firewall between policy agencies like the State Department and National Security Council on the one hand, and law enforcement bodies on the other.

On the policy side, the United States must also make better use of the tools already at its disposal. Financial sanctions against Russia remain vastly under-utilized given the scope of financial leverage the United States has over Russia. To date, the United States has only applied full blocking sanctions on one Russian bank, and that bank is not even among the 20 largest Russian financial institutions. Furthermore, personal sanctions against corrupt individuals such as those mandated by the Magnitsky Act have barely been utilized at all, with less than 30 individuals designated since 2012.

Finally, in the United States it is vital that an independent Special Prosecutor be empowered to investigate allegations of ties between the Russian government and U.S. political actors. Of all the lessons from Russia's influence operations in Ukraine and elsewhere in Europe, this one impinges most directly on our national security. It is frankly impossible to understand how one could point to vulnerabilities among our Allies and partners while neglecting to thoroughly and impartially investigate Russia's influence operation right here in the United States.

Conclusion

The effort to counter Russia's operations in the grey zone should start in Ukraine, where Moscow continues to fight an unconventional war against Kyiv. To check Russian influence in Ukraine, the U.S. must dedicate more resources to bolster military training programs for Ukraine's conventional and special operations forces. It should provide Ukraine with defensive weapons such as anti-tank missiles and equipment such as counter-battery radars with advanced fire control systems and more effective Intelligence, Surveillance, and Reconnaissance (ISR) platforms. On the diplomatic front, the United States cannot afford to remain a spectator as the Normandy Group engages in endless negotiations. The United States must get involved in these negotiations and help the parties develop a concrete roadmap of actions to implement the two Minsk agreements of September 2014 and February 2015. Crucially, this roadmap must specify specific dates by which actions must be completed and consequences for failing to meet required deadlines. To sharpen U.S. leverage, the United States should consider unilaterally tightening current debt and equity restrictions on Russian financial institutions, and if necessary incrementally apply blocking sanctions to signal resolve. Positive incentives should also be offered for compliance with the Minsk roadmap. Lastly, the United States needs to continue to support Ukraine's reforms, in part by applying strict conditionality to U.S. assistance and insisting on Ukrainian follow-through, but also by encouraging our European partners to play a more active role in supporting reform.

As we consider more robust measures to push back on Russian influence operations in Ukraine and elsewhere in Europe, we cannot blind ourselves to the painful fact that these operations have been targeted at the United States as well. I have argued before that if Russian aggression in places like Georgia and Ukraine is not checked, Russian malign influence will continue to spread to our allies in Europe as well as here in the United States. Now it is a fact that Russia has sought to corrode one of the most sacred institutions in this country: our democratic process. We must be prepared to respond with the sense of seriousness and urgency that is required.