Celeste A. Wallander
House Committee on Foreign Affairs
Hearing on "Russian Bounties on U.S. Troops: Why Hasn't the Administration Responded?"
July 9, 2020 at 1pm

I thank the committee members for the invitation to contribute to your work. I hope to inform your understanding of what Russia has done and why it has done it. I want to explain how Russia's actions have threatened American national security and undermined the defense of our interests. I speak in my personal capacity as an analyst of Russian security affairs for 35 years and not as the representative of any organization for which I work or have worked.

I will limit the scope of my testimony to Russia, leaving issues of intelligence and Afghanistan to my able panel colleagues. I will not attempt to address questions regarding confidence levels and completeness of the reported intelligence assessment. For the purposes of today's discussion, I will assume that the publicly reported details are accurate.

To summarize my analysis: these recently reported operations are embedded in a nearly decade-long Russian campaign of strategic competition that aims to weaken the United States and advance Russian security. This campaign is focused on the "Phase Zero" end of the conflict spectrum and seeks to exploit Russia's asymmetric advantages in sub-conventional military spheres, including covert and not-so-covert operations in Eurasia, Europe, and the United States. The Afghanistan bounty operation fits this campaign, but it also is an escalation within it that suggests Russia's leadership is choosing increasingly risky actions in the belief it can continue to operate with impunity. The U.S. response must encompass improving our capabilities and defenses, eliminating vulnerabilities, closely working with NATO allies, and holding the Russian leadership accountable for its choices and actions.

## Russian security strategy, threat assessment, and risk-taking

For nearly a decade – since Vladimir Putin regained the position of President in 2012 -- Russian foreign policy has been driven by the assessment that the United States seeks to weaken, constrain, encircle, and coerce the Russian Federation -- and ultimately to dictate Russian foreign and domestic affairs. Russia's security priority is the perceived American threat to Putin's Russia, and Russia has been engaged in a broad-spectrum strategic competition to weaken the U.S. and strengthen Russia, at home and abroad.

While building its conventional and nuclear military capabilities – strategic, regional, and theater -- the Russian Federation has also developed and refined non-military tools in its security strategy, notably cyber, informational, and economic-political influence instruments. The Russian security leadership recognizes that while it is a peer to the United States in strategic nuclear capabilities (notwithstanding its fears that missile defenses and new technologies may undermine the credibility of its secure second-strike capability), it does not match the United States in global power projection and conventional military capabilities. Russia's economy has also underperformed for nearly a decade and has not met the leadership's goals for higher growth to put Russia among the top global economies, which complicates defense spending.

As a result of its disadvantages, Russia has sought to exploit relative American vulnerabilities and has preferred to compete with the United States in asymmetric terrains, on four dimensions. First, the Russian leadership is unalterably convinced that the United States is engaged in a fully integrated political, economic, informational, and technology-enhanced strategy to constrain Russia and effect regime change. To compete in this space, Russia has invested in tools and methods to asymmetrically counter perceived American advantages. Anything is fair game when Russia's survival is at stake, whether that is

collecting embarrassing information on foreign officials or creating extremist lies on social media. Second, Russia seeks to compete where it has advantages in the asymmetric terrain, and to avoid competition that could lead to costly escalation, in the modern conventional military sphere against the United States military. Third, in order to hold the diplomatic high ground while avoiding an open military conflict with the United States, Russia has deployed asymmetric tools to protect the deniability of its actions to international (and domestic) audiences, however implausible that deniability has proven. And fourth, the Russian Federation has sought to escape the constraints of international law, customs, and norms of conduct, while claiming that the U.S., Europe, and others in the international community must be bound by them. When the U.S. and other countries play by the rules, cheating provides Russia with asymmetric advantages.

Russia's strategic competition therefore takes places primarily in the "Phase Zero" end of the conflict spectrum. "Phase Zero" refers to the sub-military conflict strategic environment in which diplomatic, informational, political, and economic conditions shape a country's capacity to secure its interests and prevent conflict from escalating to active military confrontation. The concept is not unique to Russian security doctrine (and indeed the concept plays a role in U.S. defense strategy) but its centrality and asymmetric nature is distinctive in Russian doctrine and operations. Since 2012 Russia has been engaged in active "Phase Zero" operations to compete with the United States and prevail without having to face the U.S. in a conventional military confrontation that Russian analysts assess it would be likely to lose.

In Russian military doctrine, competition with the United States in Phase Zero may be non-kinetic, but it is **not** strictly non-military. First, limited Russian military interventions in Ukraine (both Crimea and the Donbas in 2014) and Syria 2015-2016 were primarily military, with the goal of preventing the loss of Ukraine to Europe (and thus to the U.S., in Russian threat assessment) and the fall of the Assad regime to U.S. demands. Both operations were non-military with respect to the United

States directly, but both military operations were undertaken to counter and weaken the U.S. and sustain Russian power and influence – against the United States. And it continues: Russia now conducts the same type of limited military intervention in Libya against the government that has been recognized and supported by the United Nations.

Second, Russian Phase Zero operations against the United States entail actions by elements of the Russian military – primarily Russian military intelligence (the GRU[1]) and quasi-private actors such as the Wagner group. For example, the earliest stages of operations in the Donbas in March/April 2014 were managed by GRU agents, followed only in summer 2014 by the supply of regular Russian conventional military equipment, thinly veiled "volunteers," and eventually regular Russian military forces (covert and unacknowledged). The Russian operation to influence the U.S. 2016 presidential election in order to achieve an outcome favorable to Russia was a classic Phase Zero shaping operation: a mix of friendly foreign (Wikileaks), quasi-private (the Internet Research Agency), non-military (FSB/SVR[2]), and Russian military (GRU) actors.

In short, while Russian Phase Zero operations are non-military in that they avoid direct conventional military conflict with the United States, military instruments and actors nonetheless play a role in ostensibly political, economic, and informational Russian operations to

---

[1] GRU is the acronym for *Glavnoye razvedyvatelnoye upravleniye*, the Main Intelligence Directorate of the Russian Ministry of Defense. It is Russia's military intelligence service.

[2] FSB is the acronym for *Federalnaya sluzhba bezopasnosti*, the Federal Intelligence Service. It is Russia's core intelligence service, primarily but not exclusively focused on counterintelligence and domestic intelligence. SVR is the acronym for *Sluzhba vneshney razvedki*, the Foreign Intelligence Service. As the name makes clear, its mission is foreign intelligence and operations.

compete with the United States, weaken us, and enhance Russia's relative power and influence.

Since 2013, Russia has launched a growing number of high-risk Phase Zero operations. Russia has come to adopt a much more risk-acceptant posture in its Phase Zero operations for two reasons. First, Russia has heightened its assessment of the threat that the U.S. poses to the Putin system and Russia's freedom of action in the global sphere. Higher threat perception leads to a willingness to accept greater risk. Second, Russian leadership frames the issues at stake in terms of loss: loss of its sphere of influence in Ukraine, loss of a buffer zone in Central and South Asia, loss of a client regime in Syria, loss of internal sovereignty. When people believe that they are in a realm of loss (even if such a perception is self-serving and based in misperception or falsities), they are more willing to accept higher levels of risk in their actions to prevent further loss.

**Russian ambivalence and pivot on Afghanistan**

A decade ago, we told ourselves that the United States and Russia shared the same interests in Afghanistan in the fight against al-Qaeda, and terrorist extremism more generally. Russia's interest in the defeat of al-Qaeda and its fear of extremist threats led Russia in 2009 to support the International Security Assistance Force and the Northern Distribution Network supply system by allowing ground- and air-transit of Russia territory. In the years that followed, Russia participated in numerous international and regional talks to bring a diplomatic end to the conflict in Afghanistan.

However, even during this positive period of the "reset," Russian government officials constantly pushed the United States to wrap up its military operations and go home. The Russian leadership was at best ambivalent about U.S. (and NATO) military presence in Afghanistan: it see-sawed between concern about extremism and growing alarm at (in

the Kremlin frame) NATO military encirclement of Russia from an arc starting in the Baltics, through the Black Sea and Caucasus, and into Central Asia and Afghanistan.

With the decisive break in U.S.-Russia relations in 2014 and America's shift to an active strategy of imposing costs and pressure on Russia for its invasion of Ukraine, Russia's concern about instability and extremism in its Eurasian borderlands moved down the priority list. The overwhelming priority became countering U.S. presence and influence throughout Europe, the Middle East and Central/South Asia. Russia continued to participate in multilateral efforts to end the conflict in Afghanistan, but it also began to develop separate ties to the Taliban, providing it financial and military resources to challenge U.S.-led coalition training and support for the Afghan government's security operations. Russia has sought to hasten the departure of U.S. and coalition forces for years, and to develop ties with actors in Afghanistan in anticipation of that day.

That Russia seeks the end of U.S. and NATO military presence in Afghanistan and has been investing in a relationship with the Taliban to influence Afghanistan in the future does not fully explain why it would take the risky, escalatory, and distasteful (in terms of professional military ethics) step of offering bounties for soldiers killed. It may be that Russia assessed that the Taliban was insufficiently active in striking coalition forces and needed incentives in order to hasten U.S. failure and withdrawal. It might be that Russia sought to complicate the U.S.-Taliban relationship to ensure that Russia would emerge with the stronger relationship with the beneficiary (the Taliban) of the coalition withdrawal. Many of the GRU's operations have been strange in intended effects and have backfired: in the end, Russia's reasoning may not make any sense to us.

Yet, while Russian meddling in Afghanistan and efforts to push the U.S. out are not new, the operation to conspire with criminal actors and Taliban fighters to target and kill American and coalition soldiers for

Russian payments crosses a threshold on risk and threat, seeking to exploit asymmetric operations to not only weaken the U.S. but kill our citizens with impunity. The GRU bounty operation reportedly dates back to 2019, before the February 2020 agreement for withdrawal of coalition forces and the Taliban's commitment not to attack U.S. or coalition forces. One would hope that this means the operation has been abandoned or is otherwise inoperative. Yet, if the reports are true, we have to take seriously what this escalation means for Russia's intentions and willingness to prosecute strategic competition.

**Implausible Deniability and the Role of the GRU**

The asymmetric Phase Zero framework helps to explain why the GRU has surfaced in a number of operations in Europe, the U.S., and now in Afghanistan. As an instrument of Russian security, defense, and military policy, the GRU's role goes beyond standard military intelligence collection and battlefield support operations to active measures in Phase Zero competition to weaken adversaries and advance Russian power and interests. These operations have encompassed successful and attempted assassinations in Europe, political interference in Europe and the United States, and commissioning bounty-hunting to kill American and coalition soldiers in Afghanistan.

Across all of these cases, GRU operations are bold, and sloppy. The failures of operational security and professionalism suggests that the Russian leadership's elevated threat perception and risk-taking has resulted in approving a broader, bolder, and more active set of operations to achieve the leadership's objectives. Over the years, the GRU's operations (both botched and successful) have been repeatedly exposed, yet the GRU has nonetheless continued to engage in them. Americans often over-estimate President Putin's role in dictating and micro-managing affairs in Russia: Russia is a large country, has a huge government bureaucracy, and faces a host of problems and challenges. It is unlikely that Putin orders each GRU operation directly.

But the fact that the GRU has not been restrained or punished and operates over multiple years with impunity despite being exposed, means that there is no question that the GRU operates with political cover and approval at the highest levels of the Russian leadership. Whether that is Minister of Defense Shoigu (to whom the GRU technically reports), or Russian Security Council head Nikolai Patrushev (a Kremlin hard-liner who speaks most alarmingly about the U.S. threat, who served in the Soviet KGB, and directed the Russian FSB), or President Vladimir Putin himself, the Russian leadership has authorized and is therefore responsible for these operations.

Why would the Russian leadership allow the GRU to play such a dangerous game? Russia has for years successfully managed asymmetric operations to keep the competition in spheres where it has operational advantages. Unlike the United States or other democracies, the Russian government is not constrained in its dangerous overseas operations by an empowered Russian public or co-equal branch of government. It can act with virtually unconstrained domestic impunity.

More disturbing is how successfully Russia has prosecuted asymmetric competition with international impunity. We still refer to Ukrainian "separatists" as if national self-determination is at stake in Ukraine. Syria is nearly fully under the Assad regime's control after Russia patiently exploited ceasefire agreements to successfully destroy opposition forces and prosecute the war. GRU officers travel freely throughout Europe conducting Phase Zero political de-stabilization, and assassination attempts against EU citizens. And Russia has now crept over the line from asymmetric political operations to attacks against American military forces, through a dishonorable proxy military operation.

**Steps to Right the Balance**

The Russian government has gotten away with its Phase Zero operations in part because we are not well-equipped to compete in that asymmetric space. Russia has also gotten away with them because U.S. and European leaders tend to view these operations as political, not part of the national security spectrum. That framework is mistaken. And most importantly, the Russian leadership has gotten away with them because we have all allowed the Implausibly Deniable to pass as deniable, murky, ambiguous, or "gray zone."

The result has been a creeping escalation and exploitation of asymmetric operations that are meant to complicate an effective U.S. response. American caution is warranted: the other end of the conflict spectrum is mutually assured destruction. Caution, however, does not require paralysis, nor implausible denial.

*Step One: Defense*

Policy discussions on Russia tend immediately to go to imposing costs and deterrence. But the first step needs to be building defenses against Russian asymmetric competition. The U.S. (and allies) must invest in better monitoring, tracking, and defense capabilities against Russia's implausibly deniable actors and agents. The effectiveness of these operations erodes when they are publicized. When Russia's delivery of the SA-11 and its use to destroy MH-17 along with its 298 passengers in Ukraine in 2014 was publicly exposed, Russia immediately withdrew the system and halted delivery of high-altitude surface-to-air weapons systems to its proxy forces in the Donbas. Public exposure erodes Russia's operational capabilities.

The U.S. and its allies could also do much better in constraining and complicating the operational freedom that Russia's asymmetric agents and actors enjoy. Expulsion of Russian agents from the United States and Europe following election interference and assassination operations eroded, for a time, Russia's capabilities. Combined with better monitoring and information sharing, the U.S. and Europe could

shut down or at least limit the effectiveness of gray zone exploiters and operators.

More broadly, Russia's asymmetric campaign has struck at Europe as well as the U.S., so coordination and a common approach with NATO allies should be at the core of the U.S. response strategy. A unified response prevents Russia from being able to find seams and vulnerabilities in our strategy. It allows the U.S. and European countries to pool information and resources, enhancing our capabilities to protect ourselves from Phase Zero exploitation operations.

*Step Two: Eliminate Vulnerabilities*

The next step is to mitigate our own weaknesses and the vulnerabilities Russian asymmetric operations have exploited in order to thwart or at least limit their effectiveness. Private sector social media companies have begun to take these steps, so we know that it can be effective. Russian asymmetric operations require financing, so governments should look at regulations to prevent the use of financial organizations in facilitating monetary flows that support Russian intelligence operations.

*Step Three: Hold Russia accountable*

The Secretary of Defense and Chairman of the Joint Chiefs of Staff should communicate this to the Russian Minister of Defense and Chief of the General Staff: you are held accountable for the actions of those who serve in the Russian military under your command, and this incident is unprofessional and not worthy of a peer relationship, however competitive. Insofar as possible, the U.S. should lay out the evidence and not take this issue off the table until there is an acceptable answer, and acknowledgement that this is beyond the bounds, and will not recur. The Russian military sees itself as a peer competitor to the U.S. military, and constantly demands to be treated as such. The Russian military

pushed to go beyond de-confliction in Syria to intelligence sharing and cooperation against common threats. Instead, the Russian military has engaged in the dirty business of paying a bounty to strike at the U.S. military. The U.S. military has something the Russian military values and seeks: mutual professional respect. The U.S. defense leadership must make clear how the Russian military must conduct itself to earn that respect.

If the Russian security/military leadership is willing to acknowledge the need for a code of conduct based upon professionalism – not cooperation, but communication in order to end the implausible deniability game – Congress should support the communication channel with an explicit carve-out from its prohibition on military-to-military cooperation. Communication is not cooperation (which is working together to achieve common objectives, which are few and far between in current circumstances, and therefore unlikely even without Congressional prohibitions): its purpose would be to restrain Russian exploitation of its asymmetric advantages, and thus be in American self-interest.

*Step Four: Impose targeted, effective, and removeable costs*

If the Russian government refuses to take responsibility, or refuses to agree to a code of conduct that pulls back from the more egregious violations of international law, diplomatic norms, and military professionalism, the U.S. then must look at imposing costs that would negatively impact the cost-benefit calculation of Russian leaders with the power and responsibility for dangerous activities. Those costs could be sanctions and restrictions on officials or organizations, but they should be targeted to be effective. The targets should be officials and institutions in the security sector, or serious systemic financial sanctions tied to precise and specific behavioral changes by the Russian leadership. Scattershot sanctions against Russian business will not provide leverage for behavioral change in the security and military

sphere, and should be avoided. The message needs to be clear, precise, credible, and targeted on the source of the threat to U.S. security.

Thank you for allowing me to contribute to your work on this issue, and I look forward to your questions and insights on this challenge we face together.