Counterintelligence vs. the Russian Hybrid Warfare Model: An Arcane Tool against a Serious New Threat

By An Allied Command Operations NCO

Introduction

Russia has embarked on a new era of diplomatic assertion, using all means of influence within its available arsenal to assert its diplomatic will on those nation-states near its borders and sphere of influence. In some cases, these means have included diplomatic pressure – a normal state function – while in others, covert means have been employed such as disinformation campaigns, espionage, subversion, and strong-arm influence techniques via politically-connected gangs, and further coupled with special operations-style activities of sabotage, assassinations, deep area reconnaissance, and direct action to achieve results that were in line with Russian political will. These measures have been termed "hybrid warfare" by the academic community, and have been specifically designed so as to circumvent the NATO military collective defense response mechanism since they remain just below the threshold of an overt military attack. Russia loves to exploit legal loopholes. They've been doing it quite successfully for centuries. With a shadow of plausible deniability, Russian government-sanctioned covert actions seem designed to cause an effect that on the surface has the appearance of originating from within the affected country/region. Engaged by such tangible threats, the best and perhaps only course of action left to the affected country is to increase its national capabilities and capacity to respond through standing counterintelligence and security mechanisms – to counter the espionage, subversion, sabotage, and organized crime threats generated by Russian intelligence and Spetsnaz activities.

North Atlantic Treaty Organization

In an interview with Alfred Werner in the late 1940s, Albert Einstein famously forecast that World War IV would be fought with sticks and stones, implying that WW III would be so devastating given the development of nuclear weapons that the world would be destroyed as we know it should it be fought, with society returned to the Stone Age.[1] Indeed it has been the objective of the world's most powerful nations to avoid WW III through both peaceful measures and the development of standing alliances that dissuade would-be protractors from instigating hostilities against fellow members of the alliance.

One of the most successful of these alliances is based on the North Atlantic Treaty, signed in Washington, DC, on 4 April 1949. The North Atlantic Treaty Organization (NATO) is a political-military organization that lends its members increased strength based on the concept of mutual collective defense, articulated best in Article 5, which states that an armed attack against one or more of the parties of the treaty shall be considered an attack against all the parties, and will be responded to by the collective strength of the Alliance. Article 5 would have to be a major planning consideration for any nation contemplating hostile actions against any party to the North Atlantic Treaty, and indeed has helped ensure the peace held true throughout the Cold War, but how well it can secure the peace in the 21st century remains to be seen given the latest Russian warfare mechanism specifically designed to evade the NATO Article 5 clause.

Hybrid Warfare

National militaries are employed to impose the political will of their state but they are not the only tools at the disposal of governments. The US Government often refers to these 'tools' as DIME, consisting of Diplomatic, Information, Military, and Economic instruments of national power, though an argument could also be made that Cyber needs to be added to the mix, and some nations like Russia and Iran even employ extra-state proxy groups on the government's behalf; what is generally referred to in America as State-sponsored terrorism, though in the case of Russia one might also add State-sponsored organized crime. When faced with the threat of an Article 5 declaration and unified response, non-NATO states like Russia employ their DIME instruments in ways that ensure any engagement occurs just below the threshold of an 'Article 5' attack. These engagements may often look like intelligence preparation of the battlefield – deep reconnaissance, for example or cyber probing an enemy's computer networks – and information operations, which is selling a message in the public arena that puts a negative or false light on the enemy, or provides false 'news' as if it were true in order to create confusion and delay decision-making processes. These sub-Article 5 engagements may also look like sabotage, terrorism, espionage, and subversion: getting the enemy to come over to your side, thereby causing a change from within. The latter of which is the end-state goal of hybrid warfare: If you can cause a nation's government to change through surreptitious means without having to launch military operations, then the Article 5 collective defensive mechanism can be negated as it is never launched. The war would be over before it had even begun.

These types of attacks are not theoretical, though they are based on a new theory of warfare, the Russian Hybrid Warfare Model (RHWM). Each of Russia's major engagements on the periphery of NATO since at least 2007 have included some components of RHWM: Estonia in 2007; Georgia in 2008; Crimea and Ukraine beginning in 2014; and influence operations in NATO aspirants Montenegro and Sweden since at least 2015. Russia's implementation of the RHWM has differed slightly on implementation of its use of force, but in all cases where force was applied, either plausible deniability existed or the government that would counter the force ceased to exist due to orchestrated collapse from within. Following these examples of Russia's historical application of the RHWM, we can assess how the RHWM would be applied in future applications against sovereign nation states, including members of the NATO Alliance.

According to Damien Van Puyvelde, the term 'hybrid warfare' appeared as early as 2005, and subsequently was applied to describe the strategy utilized by Hezbollah in the 2006 Lebanon Conflict.[2] Frank Hoffman of the U.S. National Defense University, defined hybrid actions as, "a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behavior" employed to obtain political objectives.[3] To be fair to the Russian utilization of hybrid warfare tactics, there seem to be many more options than these and even the types, mannerism and implementation of these actions has evolved over time. Harkening back to its furthest roots of Spetsnaz operations in Spain supporting pro-communist forces during World War II, Russian hybrid warfare often manifested as sabotage operations: blowing up rail heads, bridges, transportation nodes, supply depots, and the like.[4] As Western-Soviet relations cooled into a "Cold War," Soviet actions behind enemy lines tended to follow models easily employed by the KGB and GRU: disinformation campaigns, sometimes referred to as active measures; deep reconnaissance; double agents; assassinations; and espionage.[5] The rising importance of computer networks created yet another means of non-traditional attack, as experienced in Estonia in 2007.

Estonia

In early 2007, Estonia got into a disagreement with Russia about a planned relocation of war graves in Tallinn, along with the Bronze Soldier of Tallinn, an elaborate Soviet-era grave marker

that was moved from the city center to the cemetery of the Estonian Defense Forces in Tallinn. On 27 April 2007, the Estonian parliament, ministries, banks, newspapers and news broadcasting websites were hit by a complex distributed denial of service (DDoS) cyber-attack, generally attributed to Russian-state actors (whether direct or via proxy is unclear); two days of rioting and looting commenced in Tallinn, instigated by ethnic Russians upset about the planned move; Russian propaganda issued false statements about the situation and who was to blame; and the Estonian embassy in Moscow was blockaded for a week.[6] Once the statue's move was completed and an opening ceremony was held on 8 May 2007, Victory in Europe Day, hostilities quickly abated. This example clearly shows some of the components of hybrid warfare defined by Hoffman, including criminal behavior and irregular tactics, if we consider cyber warfare an irregular tactic, launched with plausible deniability of government-directed instigation but clearly benefitting Russia's national position. Control of the information space is equally important so being able to broadcast a message that supports one party's side while denying the opposition a propaganda platform – via cyber-attack for example – enables a country's potential argument to authorize an escalation of the use of force, such as "to restore peace and security;" thankfully a step that did not occur in Estonia during this event. Diplomatic pressure was also clearly applied against Estonia, and this is an area that Russia focused on in its formalized military doctrines of Hybrid Warfare, published in 2010 and updated in 2014, but was not considered by Hoffman. Most importantly about this case, the incidents in Estonia in 2007 are a good example of how Russia has utilized RHWM methods at least once against a NATO partner, using means with plausible deniability and the absence of attributable armed conflict, in order to remain just below the Article 5 NATO Common Defense Clause. [Estonia became a member of NATO in 2004.]

Republic of Georgia

Events in the Republic of Georgia in 2008 followed a similar model to Estonia but did escalate to armed hostilities following a pretext excuse. In a 1,000-page EU-commissioned report on the five-day Russian-Georgian War, investigators concluded that while the Georgians fired the first shots, the attack was the culmination of years of rising tension and provocations for which both sides bore the blame. The report accused the Kremlin of abusing its status as a "great power" to coerce "a small and insubordinate neighbor."[7] Russian President Vladimir Putin, in particular, routinely made defamatory and inciting statements against Georgian President Mikheil Saakashvili, designed to spur Saakashvili to over-react and thus justify Russian actions in South Ossetia. The EU report concluded that South Ossetian irregular forces violated the rules of war in attacks on Georgian villages. However, Russian claims of Georgian "genocide" in South Ossetia, a semi-autonomous province within Georgia, were dismissed and Russian claims that Georgians had killed 2,000 civilians were found to be wildly exaggerated.[8] The Russians moved mercenaries and paramilitary forces into South Ossetia to influence events further and prepare for armed hostilities. Following a model also used in Abkhazia, Crimea and Transnistria, Russia embarked on a policy of "passportization," or the systematic distribution of Russian passports to grant Russian citizenship to Russian speakers in order to support Russia's territorial or pro-Russian-separatist ambitions. Once sizable populations of Russian-passport holding citizens were located in South Ossetia, Moscow felt justified to call for their "citizens" protection, creating a legal precedent for military action.[9] This reputedly followed a lesson learned that Russia garnered from NATO's own playbook. Russia has long considered NATO's stated goal of military intervention in post-Soviet Yugoslavia 'to prevent mass genocide' to be simply a pretext that enabled NATO to invade a sovereign country within Russia's sphere of influence. Building off that tactic, Russia officially launched a large-scale land, air and sea operation against Georgia with the stated aim of "peace enforcement" on 8 August 2008.[10] This five-day war was the first instance of Russian utilization of cyber warfare methods, employed

supplementary to armed military action as well as an active information campaign waged both during and after the conflict. As such, the Georgia conflict was one of the best examples of the Russian hybrid warfare model, and likely attributed to Russia's update of its military doctrine in 2010.

Russian Hybrid Warfare Model (RHWM) doctrine

On 5 February 2010, Russia published, "The Military Doctrine of the Russian Federation," which described modern warfare as entailing, "the integrated utilization of military force and forces [along with] resources of a nonmilitary character;" i.e. hybrid warfare. The doctrine also described that information warfare can be employed, "to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favorable response from the world community to the utilization of military force."[11]

General Valery Vasilevich Gerasimov, Russia's Chief of General Staff, further developed the RHWM as initially articulated in his article, "The Value of Science is in the Foresight," published 26 February 2013. It is important to consider seriously General Gerasimov's writing because his "position as chief of the General Staff makes him Russia's senior operation-strategic planner and architect for future Russian force structure and capability development."[12] From his uniquely powerful position, he envisioned the current and future operating environments, determined how war would be fought in that environment, planned the purchase of equipment to enable such fighting, set Russian military doctrine for said implementation, and oversaw its execution. There is no singular flag officer in the American military system that is equally empowered. General Gerasimov's position embodies the equivalent of more than a half-dozen American four-star generals. Perhaps most importantly to the US, in Gerasimov's view of the operational environment, the United States was and is the primary threat to Russia.[13]

In General Gerasimov's 2013 article, he stressed the importance of nonmilitary measures over military measures in order to achieve strategic or political goals, noting that nonmilitary measures were more effective than the military measures in the current operating environment, and thus specified these nonmilitary measures should actually out-number military measures by a ratio of 4:1. Gerasimov clarified, "The important point is that while the West considers these nonmilitary measures as ways of avoiding war, Russia considers these measures *as* war."[14] [Emphasis added.]

Nonmilitary measures might include: The formation of coalitions and alliances; political and diplomatic pressure; the search for methods of regulating a conflict; disruption of diplomatic relations; economic sanctions; economic blockade; transition of economy to military lines; formation of the political opposition; actions of opposition forces; change of political-military leadership; carrying out complex measures to reduce tensions in relations; information conflict; and cyber conflict. Gerasimov linked the Arab Spring and "color revolutions" as examples of 'non-military' forced regime change, thus emphasizing that political will can be exerted through forceful means that do not require a bullet to be fired, and many of the RHWM methods utilized in Crimea and Ukraine from 2014 onward reflect these lessons learned.

Gerasimov also envisioned less large-scale warfare; increased use of networked command-and-control systems, robotics, and high-precision weaponry; greater importance placed on interagency cooperation; more operations in urban terrain; a melding of offense and defense (such as irregular warfare and counter-insurgencies create); and a general decrease in the differences between military activities at the strategic, operational, and tactical levels (meaning that localized actions can have major strategic effects).

Gerasimov's refinement of the RHWM was codified in a 2014 addition to Russian Military Doctrine, which added the idea of utilizing irregular armed forces elements and private military companies to military operations, providing plausible deniability when utilizing peacekeepers, special operators, Cossacks, private military companies, foreign legionnaires, biker gangs, Russian-sponsored NGOs, and cyber/propaganda warriors to exert Russian political agendas.[15]

Gerasimov wasted no time putting this new doctrine to use as the RHWM was fully employed to clandestinely divide and conquer the province of Crimea from the sovereign country of Ukraine in 2014. Crimea began as a covert military operation that combined ambiguity, disinformation, non-traditional actors like Cossacks and Biker Gangs as political enforcers, Special Forces operating either without appropriate identifying markings on their uniforms, or utilizing non-military uniforms, and the element of surprise at the operational level with more traditional means such as electronic warfare.[16] Because of the magnitude and importance of Russian actions in Crimea, and because the methods utilized there have been replicated in Ukraine and other locations, and thus represent the RHWM to a possible maximum(?) potential application, the discussion of events in Crimea will be considered in more depth.

Crimea

In February 2014, a popular revolution ousted the Russian-backed Ukrainian president Viktor Yanukovych and sparked a political crisis in Crimea, a Ukrainian province that was more than 50% ethnic Russian at the time. The crisis initially manifested as demonstrations against the new interim Ukrainian government, but rapidly escalated out of Ukrainian governmental control.

On the night of 22-23 February, Russian President Vladimir Putin convened an all-night meeting with his security services chiefs to discuss the possible extrication of the deposed Ukrainian president. At the end of that meeting Putin reputedly remarked, "We must start working on returning Crimea to Russia."[17] Mere hours later, pro-Russian demonstrations began in the Crimean city of Sevastopol.

By 24 February, with thousands waving Russian flags and protesting in Sevastopol against the new Ukrainian government, Russian protagonists imposed a parallel government administration in Crimea, and created 'civil defense squads' with the support of the Russian Night Wolves motorcycle club. Protesters chanted, "Putin is our president," and claimed they would refuse to pay further taxes to the Ukrainian state. Russian military convoys were also reportedly seen in the area.[18]

On 26 February, Russian troops took control of the main route to Sevastopol by establishing a military checkpoint on the main highway between Sevastopol and Simferopol, utilizing Russian military vehicles and openly displaying Russian flags.[19]

On 27 February, Russian Spetsnaz/Special Forces soldiers, wearing masks and nondescript green uniforms with no insignia, seized the Supreme Council of Crimea, as well as the Council of Ministers in Simferopol and other strategic sites across Crimea, raised Russian flags over the buildings, and erected barricades outside the buildings.[20] Whilst the so-called "little green men" were occupying the Crimean parliament building, parliament members convened an emergency session. During this session, the Crimean parliament voted to terminate the Ukrainian-affiliated Crimean government, and replaced Prime Minister Anatolii Mohyliov with Sergey Aksyonov, a pro-Russia politician aligned with the Russian Unity Party, which had received only 4% of the

popular vote in the previous election.[21] The parliament also voted to hold a referendum on greater autonomy on 25 May, which was later moved up to 16 March 2014. Throughout these momentous parliamentary actions, the Russian Spetsnaz troops cut all of the building's communications, and took the politicians' phones as they entered the building. No independent journalists were allowed inside the building while the voting took place. Some of the politicians said they were threatened to vote as instructed while others claimed that their votes were cast for them, even though they were not in the voting chamber.[22] Interfax-Ukraine reported, "it is impossible to find out whether all the 64 members of the 100-member legislature who were registered as present [were in-fact present] when the two decisions were voted on, or whether someone else used the plastic voting cards [on their behalf]" because due to the armed occupation of parliament it was unclear how many MPs were present.[23]

Additionally on 27 February, Russian troops from the 31st Separate Airborne Assault Brigade, dressed in local Crimean riot police uniforms, established security checkpoints on the Isthmus of Perekop and the Chonhar Peninsula, which separates Crimea from the Ukrainian mainland. Within hours, Ukraine was effectively cut off from Crimea.[24]

On 1 March 2014, Aksyonov declared Crimea's new *de facto* authorities would exercise control of all Ukrainian military installations on the Crimean peninsula. He also asked Russian President Vladimir Putin, who had been Yanukovych's primary international backer and guarantor, for "assistance in ensuring peace and public order" in Crimea. Putin promptly received authorization from the Federation Council of Russia for Russian military intervention in Ukraine under the pretext, "until normalization of a socio-political environment in the country [exists]."[25]

By 2 March, Russian troops overtly moved out of Russia's Crimea naval base in Sevastopol and were further reinforced by tanks, troops and helicopters from mainland Russia in order to exert complete control over the Crimean Peninsula.[26] However, Russian troops continued to operate in Crimea without insignia. Despite numerous media reports and statements by the Ukrainian and foreign governments describing the unmarked troops as Russian soldiers, Russian government officials concealed the identity of their forces, claiming they were local "self-defense" units over whom they had no authority.[27] It was not until 17 April 2014 that Putin finally acknowledged the Russian military had backed Crimean separatist militias, stating that Russia's intervention was necessary, "to ensure proper conditions for the people of Crimea to be able to freely express their will."[28]

On 13 March, Putin privately justified his actions by making a comparison between Russia's intervention in Crimea and the US/NATO intervention in the former Yugoslavia republic of Kosovo during a phone call with US President Barack Obama; repeating the justification also used in the 2008 Russia-Georgia War.[29]

On 16 March, Crimea held a referendum on its status as a state, and on 17 March, officially announced the referendum results: The Supreme Council of Crimea had declared the formal independence of the Republic of Crimea, comprising the territories of the Autonomous Republic of Crimea and the city of Sevastopol.

On 18 March 2014, the Republic of Crimea and Sevastopol requested terms for the immediate admission as federal subjects of Russia and to become part of the Russian Federation.[30]

On 19 March, Putin submitted a treaty on Crimea's reunification with Russia. The Russian Constitutional Court quickly found the treaty to be in compliance with Russia's Constitution. The

State Duma then ratified the treaty on 20 March, and the Federal Assembly followed suit on 21 March, backdating the official date of Crimean reunification with Russia to 18 March 2014.[31]

As a post-script, in February 2015, the leading independent Russian newspaper *Novaya Gazeta* reported that it had obtained documents, allegedly written by Russian oligarch Konstantin Malofayev and others, which provided a strategic template for the Russian government to utilize in the event Ukrainian President Viktor Yanukovych was removed from power, an event that was considered by the authors as likely to occur. The documents outlined plans for the annexation of Crimea as well as the eastern portions of Ukraine, and closely described the events that actually transpired following Yanukovych's removal from power. The documents also described plans for a public relations/information campaign that would seek to justify Russia's actions in the local and international press.[32]

During opening remarks at a Berlin conference sponsored by the Atlantic Council, the European Council on Foreign Relations, and the Heinrich Böll Foundation on June 25, 2015, titled, "Exposing Russian Disinformation in the 21st Century," US Ambassador John B. Emerson highlighted the extent of the Kremlin's global disinformation campaign through the $400 million media enterprise it finances to extend influence through some 100 countries in which it operates. This disinformation campaign follows what some have termed the 4D approach, including: "dismiss," as Putin did for more than a month when he attempted to dismiss the fact that Russian soldiers had occupied Crimea; "distort," as an actress did in playing the role of a pro-Russian Ukrainian on a Russia Today news-clip; "distract," as the Russian media did by advancing outrageous theories about what might have happened to Malaysian Airlines Flight 17 in July 2014, attempting to deflect attention away from events in Crimea; and "dismay," as Russia's ambassador to Denmark did in March 2015 when he threatened Danish warships with nuclear targeting if the country of Denmark joined NATO's missile defense system.[33]

Sweden

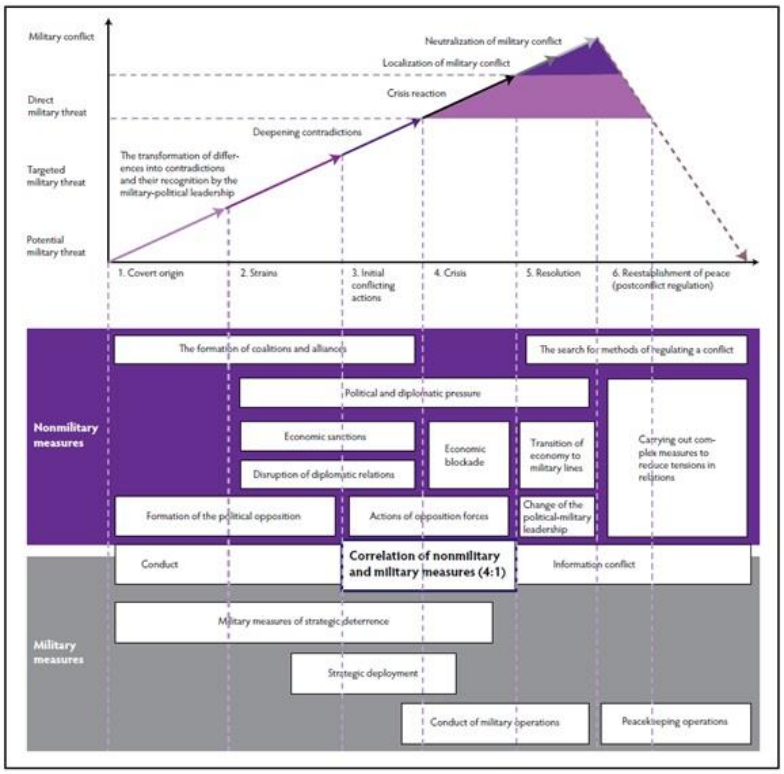
Russia shows concern anytime it loses control or influence in its near abroad, especially when it interprets events as an encroachment by NATO into that sphere of influence. Such has been the case of the proposed accession of Montenegro into NATO and the vote for proposed increased access for NATO forces to Swedish ports, airfields and land, both of which resulted in RHWM activities in each country from 2015-2016.

According to the Sakerhetspolisen, the Swedish Security Services or SAPO, which released its latest annual unclassified report on 17 March 2016, about one third of Russian diplomats in Sweden are reputedly spies. These Russian spies are claimed to have been carrying out an aggressive reconnaissance of civilian and military infrastructure, and were also involved in disinformation campaigns, intended to influence the Swedish decision-making process concerning its proposed closer working relationship with NATO. Russian intelligence services were also blamed for DDoS and cyber-attacks directed against Swedish news services during the lead-up to the 25 May 2016-vote on Sweden's relationship update with NATO.[34] However, as occurred in Estonia following the movement of the Bronze Soldier of Tallinn, once the Swedish vote was concluded (favorably in this case), Russia's Hybrid Warfare Model actions to influence politics and public opinion in Sweden died down – at least temporarily.

Counterintelligence: The Best First-Response Option against RHWM Actions

Given Russia's obvious inclination to utilize RHWM techniques to exert national influence over its neighbors, countermeasures can be employed to monitor and react to these incidents as

they occur. This requires layered and proactive security measures, with increased cooperation and intelligence sharing between neighbors and NATO Alliance members. Security services with a counterintelligence (CI) charter are a nation's first line of defense against phase one to phase three RHWM activities, according to Gerasimov's own doctrine (inset), where military force really begins in phase four.



Graphic from Gerasimov article in *Voyenno-Promyshlennyy Kurier*, 26 February 2013, translated by Charles Bartles

Early phase RHWM activities that can be detected, and in many cases countered by CI and security services include: espionage and double agent operations, terrorism, sabotage, deep area reconnaissance, subversion, demonstrations, propagandizing, disinformation campaigns, political opposition support, "passportization," cyber warfare, organized criminal behavior, intimidation and blackmail.

While CI and security are first and foremost a national-level responsibility, the US and NATO can support Allied efforts to maintain a better understanding of the threat environment by mutual cooperation and sharing activities.

Counterintelligence as a security function begins with defensive measures, such as investigations, but the first lead has to come from somewhere; whether that be a walk-in source, a liaison tip, a derivative lead, etc. Where counterintelligence excels is in its unique pairing of multiple intelligence and investigative functions into a singularly focused intel activity. The counterintelligence agent is really a jack-of-all-trades: not only an investigator, but also an analyst; an erudite subject matter expert on the opposition and their operational methodology while also a socialite liaison officer with partners and Allies; a technician of arcane specialties such as cyber warfare and electronic 'bug sweeps,' but also a master of disguise, able to blend into a crowd and follow a target without detection. When you pair these and many other capabilities together, you get an intelligence activity that adapts well and responds as needed to assess and counter the threat in whatever form is presented by the opposition. What might start as a simple lead: a janitor, for example, observed and reported to be working without a badge, may quickly morph into an investigation supported by signals intelligence and analysis, that may develop further still into a source operation to penetrate a hostile intelligence or terrorism cell, and even into a liaison meeting with an Allied service to share the discovered information and decide on a course of action to neutralize the revealed threat.

This adaptable utility makes counterintelligence the most appropriate first line of defense against the RHWM, and as such, is strengthened even further when Allied national and military CI services work together. Within Europe, national borders are easily crossed with minimal or

no border checks, thus aiding not only legal business and tourism traffic, but also criminal enterprises and illegal intelligence activities. Counterintelligence thus plays a primary role in liaison and intelligence sharing to counter hostile intelligence service activities. For example, an intelligence officer may reside in one country where he conducts legal, overt diplomatic or business activities, and then travel to another country, perhaps even using an assumed identity where he conducts clandestine activity such as meeting a source, delivering or retrieving material, information or money, or any number of other intelligence activities. If the host nation where such intelligence activity is occurring has not identified the person using the false identity as a hostile intelligence officer, they won't know to surveil or investigate his activities while he secretly traverses through their country. Thus, counterintelligence excels by sharing information between Allied services in order to develop a more comprehensive shared understanding of the operational environment.

Let's take a look at one such recent success case. Frederico Carvalhão Gil, a Portuguese intelligence officer with Portugal's domestic intelligence agency, the Security Intelligence Service, SIS for short, was arrested in Rome under cooperative arrangement with Italian authorities on Saturday, 21 May 2016, along with his Russian intelligence 'handler' during a clandestine intelligence meeting between the two at a local Roman café, according to the Observer and other news sources.[35]

The SIS suspected it had a mole in its service as early as 2014 and with the help of Allied intelligence services to identify the suspect, eventually focused their attention on Mr. Carvalhão by late 2015. At that point, SIS transferred Mr. Carvalhão to a duty position where he would have less access to classified information, and placed him under constant surveillance and monitored his conversations as SIS continued to look for evidence of his betrayal and spying activities. They soon discovered Mr. Carvalhão had a proclivity for indiscreet liaisons with women from countries comprising the former Soviet Socialist Republic, and made regular trips across Europe. SIS assessed these were strong indicators of a 'honeypot' intelligence relationship between Mr. Carvalhão and a Russian intelligence service, and his international travels in particular would be conducive for clandestine meetings with Russian SVR intelligence officers in order to pass secrets to the Russians. Meetings conducted outside Portugal would be generally less risky for a foreign intelligence service like the SVR than meeting Portuguese sources inside Portugal where the SIS would have greater capabilities and authorities to monitor the local security environment.

This investigation culminated in a joint operation in Rome which led to Mr. Carvalhão's arrest. In coordination with Europol and their Italian partners, SIS agents watched Mr. Carvalhão's movements as he boarded a flight to Rome on Friday, 20 May 2016, in preparation for the following day's planned meeting with his Russian intelligence handler. That clandestine rendezvous was spoiled when Italian police appeared at their meeting location, a downtown Roman café nestled beside the Tiber River, and arrested Mr. Carvalhão on charges of espionage and corruption levied by Portuguese authorities. Neither Mr. Carvalhão nor his Russian contact resisted arrest.

In an interesting twist, his Russian SVR handler was not in Rome under official diplomatic cover, posing as either a diplomat or national trade representative, the most common covers in espionage circles. Rather, the SVR agent was what the intelligence community terms an 'Illegal,' meaning he was operating without any official government affiliation – or protection. He therefore was subject to arrest and prosecution by Italian authorities. The identity of the Russian SVR officer in custody has not yet been released.

Illegals are unique in intelligence circles because they are rarely discovered, especially in comparison with their counterparts posing as diplomats. This is because they are much tougher to detect since they aren't working at an embassy or consulate where the movements, contacts, and activities of diplomatic employees can be monitored and assessed for likely affiliation with a foreign intelligence service. Unless a tip or accident leads to their discovery, 'illegals' may operate for years or even an entire career without being identified as intelligence officers, and thus their movements across international borders raise little or no attention, and their activities generally go unmonitored. The case of Mr. Carvalhão thus interrupted not only Russia's handling of this important NATO spy but also the (presumably) many other RHWM activities and intelligence sources for whom the Russian illegal officer was also responsible. Within the realm of counterintelligence, this recent arrest in Italy may well serve as the first domino in a series of Russian intelligence activities that are discovered and subsequently interrupted all across Europe, and possibly beyond, and represents one of the primary ways CI can defeat, degrade, disrupt and deny the RHWM in its earliest stages.

A Fictional Worst Case Scenario:

More than one million ethnic Russians reside in the three Baltic States, Estonia, Latvia, and Lithuania, amongst a total population just over 6 million. This number represents about a 41% decline since the Baltic States gained their independence from the Soviet Union but is still large enough that Russian interests, due to both proximity and population, must still be given serious consideration in the Baltics. Consider just their national capitols: Vilnius, Lithuania, less than 25 miles from the Belarussian border and about 80 miles to the Russian border of Kaliningrad, is nearly 15% ethnic Russian while the country itself is about 5% ethnic Russian. Riga, Latvia, about 120 miles to the Russian border is just over 50% Russian while the country is more than 27% ethnic Russian. Tallinn, Estonia, also about 120 miles from the Russian border, is about 38% ethnic Russian while the country is more than 24% Russian. In this RHWM example, no specific Baltic country will be used so as not to enflame any political sensitivities. Rather, a general representation will be used to express the serious nature the Baltics, the US, and all the NATO Allies face from the real threat of the RHWM in the Russian near-abroad. The following is a fictional 'worst case' scenario designed for academic consideration only.

It was 10:00 pm, Saturday evening in the capital of the small Baltic country. Markus, an ethnic Russian teen, and Emilija, his young date for the evening, were on their way home after watching a movie at the downtown cinema. Tensions had been rising lately between ethnic Russians and the local Baltic populace, stemming from long-standing resentment of the two-class system in their post-Soviet reality, but Markus and Emilija paid it no mind. They were young and in love, and that's all that mattered. As they crossed the street to the parking lot where his car waited, a group of Baltic teens approached and castigated Emilija for dating outside her ethnicity. Not to be intimidated, Emilija told the teens to mind their own business. The nearest teen slapped Emilija and replied that protection of their national identity was their business. Seeing his date slapped, Markus immediately intervened, pushing the Baltic teen back from his date. Unfortunately, the other teens quickly jumped Markus and beat him to an unrecognizable pulp, leaving him for dead as they ran off, swallowed anonymously by the night.

Markus' death was the top news event on Sunday morning, and brought immediate cries for justice and protection of the Russian ethnic population in the country. After all, if they weren't safe in the capitol where the largest number of Russians resided, how could they be safe anywhere in the country? The Russian government echoed the call for immediate actions in the Baltic state to protect their ethnic brethren. Commentators on Russia Today (RT) suggested the people should stand-up for their rights and demand the Baltic government take action for

demonstrable change, and ensure justice was served. Within an hour of the morning news report a massive demonstration formed around the buildings in the governmental heart of the capitol. Demonstrators waved Russian flags and called for a dissolution of the local government that had failed them and refused to guarantee their security. As the day progressed, RT reported the Baltic police forces were 'over-reacting' to the 'peaceful' demonstrators and were countering them with undue lethal force. Pandemonium in the capitol ensued.

Though the banks were closed on Sunday, concerned citizens started lining up at ATM machines to withdraw cash in case they needed to hold-up in their homes until peace resumed in the capitol. However, to their horror, not a few of these Baltic citizens soon discovered that their accounts were mysteriously empty. Their entire life's savings were gone; but how? Word soon got out that the Baltic banks were the victim of a concerted cyber-attack and many tens of billions of Euros were missing. Commentators on the Baltic country's news channel suggested the cyber-bank heist seemed to mimic a cyber-attack on Moldovan banks that had occurred in 2015, generally attributed to Russian-state actors, and resulted in the loss of more than one billion euros and the near collapse of three Moldovan banks.

As Sunday progressed to the late afternoon, the banking panic escalated into a full scale riot as concerned citizens of all ethnicities, including an undue number of Russian Night Wolves motorcycle gang members, often attributed as an organized crime unit with direct ties to and perhaps operating on behalf of the highest levels of the Russian government and intelligence services, began attacking the banking and governmental structures throughout the capitol. Unfortunately, further news of the situation was unavailable from within the Baltic nation because the local news services were also subjected to a ruthless and effective DDoS attack. Even the on-air news services went off-line so updates were only available from RT and its 'concerned' subsidiary news services inside the small, embattled Baltic nation, as well as in Russia and in the surrounding countries.

As Sunday evening approached, Baltic military forces were called in to help restore peace through martial law, and were met by a less-than-compliant armed 'civilian' force intermingled amongst the demonstrators. Upon closer inspection, the armed 'civilian' force seemed to be primarily ethnic Russians, sporting close-crop military haircuts and wearing unmarked green uniforms, looking rather like the stereotypical 'little green men' seen in so many other Russian-instigated crisis locations. Could Russian Spetsnaz personnel have already infiltrated the Baltic nation and its civilian demonstrations in an effort to drive a desired reaction in the capitol?

RT duly reported the Baltic military responded to the 'peaceful, civilian' demonstrators with unjustified lethal measures, resulting in the deaths of many hundred Baltic civilians. The rioting demonstrators reacted to the attacks by moving and disbursing constantly throughout the city. Intercepted radio communications from the Baltic military, reporting to its higher headquarters, described 'little green men' conducting highly effective harassment attacks, ambushes and sniper engagements against the Baltic military throughout the night. They begged for armored personnel carriers to protect their own forces, tanks to dislodge embedded enemy positions, and medevacs to speed injured and dying soldiers to hospitals and more secure rear areas. Near 3 am, one young Baltic troop was heard crying over the radio for all available aid after a surface-to-air missile, possibly an old Russian SA-7, took down a medevac helicopter with a full crew plus six injured soldiers in the process of being evacuated off the front lines.

As Monday morning dawned, RT provided exclusive reporting on the evenings' hostilities against 'peaceful' Baltic civilians by the 'blood-thirsty' government forces. RT added the banks' reported losses were continuing to mount though the banks were unable to fully investigate the

matter given the on-going cyber and DDoS attacks against them. The stock market reacted predictably by dropping more than 20% within minutes of the opening bell before a fail-safe mechanism halted all further trades for the day. RT continued to report from the capitol that the demonstrators, comprising a 'unified front' of ethnic Russians and 'concerned' Baltic citizens, were calling for a complete overhaul of their nation's governmental system, which obviously was not working to protect anyone or anything.

At 11:00 am, the NATO Secretary General called the Baltic state's Prime Minister to ask if NATO could be of any service to the state. The Prime Minister clarified that this was a purely internal, national security matter, and while the Secretary General's concern was appreciated, NATO's assistance under Article 5 of the North Atlantic Treaty was both premature and inappropriate. The Baltic state would quickly resolve matters on its own.

At 11:30 am, further phone calls or live news reports from within the Baltic state became impossible to conduct in real-time because a massive cyber-attack, this time directed against the country's electrical distribution system, resulted in a complete national blackout and immediately impacted the nation's ability to communicate both internally and externally. This seemed to mimic the 23 December 2015 electrical grid attack in Western Ukraine that had turned out the lights of an entire province and was attributed to Russian state or state-affiliated actors. With the absence of power inside the Baltic state, RT continued 'reliable' delayed news reports 'driven' across the border.

RT reported at 12:00 pm local that the Baltic government had indeed 'decided' to convene in emergency session, and the country's parliamentary building was being secured by 'concerned citizens' to ensure the 'corrupt' Baltic military and police forces did not seek to effect a coup de'tat in these troubling times. One might wonder whether these 'concerned citizens' were similar to the Russian Spetsnaz forces, 'the little green men,' who likewise secured the Crimean parliamentary building as its own impromptu so-called emergency session was held on 27 February 2014, and during which the small Ukrainian province 'independently decided' to seek separation from Ukraine and join with Russia.

At 2:00 pm local, RT judiciously reported the Baltic government had voted 'overwhelmingly' to dissolve its current system, and subsequently elected Anatoli Yeltsen, an ethnic Russian, as its interim President who would rule by decree until the nation's constitution could be redrafted and a new government formed in accordance with that new constitution. The nation's 'corrupt' military forces were largely disbanded forthwith and its senior leaders would be arrested for crimes against the state, including 'treason' and murdering innocent, 'peaceable' civilian demonstrators. Senior police officials were also relieved and replaced with ethnic Russians and Cossacks 'focused' on returning peace to the capitol.

Around 4:00 pm electricity was restored to the country, and shortly thereafter RT reported peace to have been fully restored to every corner of the capitol given the recent positive turn of events. The local news channels seemed to still be suffering from cyber-attacks and were unable to fully recover until later that week when the attacks suddenly and inexplicably ceased. However, general clean-up efforts had commenced throughout the capitol, and the new government shortly reported success at finding and retrieving the vast majority of the stolen bank assets, assuring the populace that the government would personally guarantee all bank losses up to 100,000 Euros, protecting more than 99% of the citizens except the 'corrupt,' wealthy former politicians of the Baltic state.

By the following day a new constitution was drafted; this one calling for closer ties with Russia and an exit from the 'corrupt' NATO Alliance. A national referendum was scheduled for Friday that same week to ratify the constitution, which was reported by RT to have passed with an overwhelming majority of the state's citizens voting in its favor. By 8:00 am Saturday, all news services were back on line and reported the Baltic state had indeed passed its new constitution and would withdraw from NATO immediately.

One week to the hour from the initial incident outside the Baltic movie theater, in a dark room, deep within the Kremlin, a senior Russian politician raised his vodka glass to the trusted group of men surrounding him. He toasted their efficiency at effecting a political transition in their former ally, turned opponent, turned ally again in that little Baltic nation to their West. And all without raising the slightest rumblings of a NATO Article 5 retaliation. The Baltic State's government had fallen, seemingly of its own accord through internal manipulations of 'concerned citizens,' before it ever even knew it was under attack. By the time someone in the former government might have figured it out, it was too late to stop the momentum for 'internal' change. Change had been plausibly orchestrated to appear as is coming 'from within.' Gerasimov's doctrine of hybrid warfare worked not only in non-NATO nations like Ukraine where they had successfully peeled off Crimea, but had now also proven successful against a NATO ally. And now, having proven they could assert Russian political will in their own backyard without having to openly employ Russian military forces, they could turn their attention to the two remaining Baltic States…

Conclusion

If the hypothetical worst case scenario, above, frightens the reader due to realism given the examples already cited, then I have succeeded at conveying the gravity of the current situation found in Eastern Europe when faced with Gerasimov's RHWM under Russian President Vladimir Putin's leadership. Putin, as a former KGB officer, is neither afraid nor hesitant to employ the full powers of his nation's unified intelligence apparatus against perceived Russian national adversaries in his near abroad. The only counter for a war conducted by a concerted intelligence bureaucracy is an equally effective and empowered counterintelligence service; one connected to and working in concert with all willing Allies and partners.

Gerasimov's assertion that nonmilitary means *are* warfare being conducted every day, there is reason to be concerned about our nations' leaders taking this threat seriously. We need our CI services to be empowered so they can ensure when a cyber-attack occurs there is no nation-state connection; or when UAVs start flying over our military bases, they are not being controlled on behalf of a foreign government; and CI is empowered to react accordingly and rapidly to hundreds of other existential threats. With all these increased threats in the current operating environment, the demand for competent and *legally empowered* CI services is only increasing, and the new RHWM is a tangible inclusion amongst those threats that effects every nation in the NATO Alliance, including the US. It may well be that only CI stands in the way of disproving Einstein's prediction of World War IV by preventing World War III from ever occurring in the first place.

[1] Alfred Werner, *Liberal Judaism* 16, April-May 1949.

[2] Damien Van Puyvelde, "Hybrid War – Does it even exist?" accessed 6 June 2016 at http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm.

[3] Frank Hoffman, "*On Not-So-New Warfare: Political Warfare vs. Hybrid Threats*," War on the Rocks (blog), 28 July 2014, accessed 6 June 2016 at http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybridthreats/.
[4] Burgess III, William H., ed. *Inside Spetsnaz: Soviet Special Operations, a critical analysis*, (Novato, CA: Presidio Press, 1990).
[5] Andrew, Christopher and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB*, (New York: Basic Books, 2001).
[6] "*Estonian nationalists attempt to vandalize monument,*" Russia Today, 27 February 2007*;* "*Tallinn tense after deadly riots,*" *BBC News, 28 April 2007;* and "*Kremlin-backed group behind Estonia cyber blitz,"* Financial Times, 11 March 2009.
[7] Traynor, Ian, "Georgian president Mikheil Saakashvili blamed for starting Russian war," 30 September 2009, accessed 17 July 2016 at https://www.theguardian.com/world/2009/sep/30/georgia-attacks-unjustifiable-eu.
[8] Saparov, Arsène (2014). *From Conflict to Autonomy in the Caucasus: The Soviet Union and the Making of Abkhazia, South Ossetia and Nagorno Karabakh.* Routledge; 82, 148.
[9] Grigas, Agnia, "*How Soft Power Works: Russian Passportization and Compatriot Policies Paved Way for Crimean Annexation and War in Donbas*," Atlantic Council (blog), 22 February 2016, accessed 20 June 2016 at http://www.atlanticcouncil.org/blogs/new-atlanticist/how-soft-power-works-russian-passportization-and-compatriot-policies-paved-way-for-crimean-annexation-and-war-in-donbas.
[10] Ibid., 77.
[11] "*The Military Doctrine of the Russian Federation*," 5 February 2010, accessed 20 June 2016 at http://carnegieendowment.org/files/2010russia_military_doctrine.pdf.
[12] Bartles, Charles K. "*Getting Gerasimov Right*," Military Review, Jan-Feb 2016, 37.
[13] Ibid.
[14] Bartles, Charles K. "*Getting Gerasimov Right*," Military Review, Jan-Feb 2016, 34.
[15] Bartles, Charles K. "*Getting Gerasimov Right*," Military Review, Jan-Feb 2016, 33.
[16] Kofman, Michael and Matthew Rojansky, *"A Closer Look at Russia's 'Hybrid War',"* Kennan Cable, No 7, April 2015, accessed 20 June 2016 at https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf.
[17] Shuster, Simon, *"Putin's Man in Crimea Is Ukraine's Worst Nightmare*," Time, 10 March 2014.
[18] *Ukraine crisis fuels secession calls in pro-Russian south*," The Guardian. 24 February 2014; and Huzar, Bogdan, *"Rosja przygotowuje się do zbrojnej interwencji na Ukrainie?" [Russia is preparing for military intervention in Ukraine?]*. Newsweek Polska (in Polish), 23 February 2014.
[19] MacKinnon, Mark, "*Globe in Ukraine: Russian-backed fighters restrict access to Crimean city*". The Globe and Mail, 26 February 2014.
[20] Weaver, Courtney, "*Putin was ready to put nuclear weapons on alert in Crimea crisis*," Financial Times, 15 March 2015*;* and Higgins, Andrew and Steven Erlanger, "*Gunmen Seize Government Buildings in Crimea*," The New York Times, 27 February 2014.
[21] "*RPT-INSIGHT: How the separatists delivered Crimea to Moscow*," Reuters, 13 March 2014.
[22] Ibid.
[23] "*Number of Crimean deputies present at referendum resolution vote unclear*," Interfax-Ukraine, 27 February 2014.
[24] "*How 'Ukrainian Berkut Officer' from Russian Ulyanovsk Assaulted Crimean Parliament Back in 2014,"* InformNapalm, 9 July 2015.
[25] *Постановление Совета Федерации Федерального Собрания Российской Федерации от 1 марта 2014 года № 48-СФ "Об использовании Вооруженных Сил Российской Федерации на территории Украины."* Federation Council of Russia council.gov.ru (in Russian).
[26] Walker, Shaun, "*Russian takeover of Crimea will not descend into war, says Vladimir Putin,*" The Guardian, 4 March 2014.
[27] *"Russia says cannot order Crimean 'self-defense' units back to base*," Reuters, 5 March 2014.
[28] *"Direct Line with Vladimir Putin,"* kremlin.ru, 17 April 2014.
[29] Goodenough, Patrick, *"Crimea Vote: Putin Cites Kosovo 'Precedent',"* CNS News, 16 March 2014.

[30] "*Ukraine crisis: Putin signs Russia-Crimea treaty*," BBC, 18 March 2014.
[31] *"Crimea, Sevastopol officially join Russia as Putin signs final decree,"* RT, 22 March 2014.
[32] Schofield, Matthew, *"Russian news report: Putin approved Ukraine invasion before Kiev government collapsed*," McClatchy DC, 21 February 2015.
[33] Emerson, John B., "*Exposing Russian Disinformation*," Atlantic Council (blog), 29 June 2015, accessed 20 June 2016 at http://www.atlanticcouncil.org/blogs/new-atlanticist/exposing-russian-disinformation.
[34] Faith, Ryan, "*Russian Spies are Reportedly Trying to Stop NATO and Sweden From Hooking Up*," Vice News, 3 May 2016, accessed 20 June 2016 at https://news.vice.com/article/russian-spies-are-reportedly-trying-to-stop-nato-and-sweden-from-hooking-up; and UAWire, "*Swedish Security Service: One Third of Russian Diplomats in Sweden are Spies*," 18 March 2016, accessed 20 June 2016 at http://uawire.org/news/swedish-security-service-one-third-of-russian-diplomats-in-sweden-are-spies.
[35] Schindler, John R., "*NATO's Big New Russian Spy Scandal*," Observer News and Politics, 25 May 2016, accessed 26 June 2016 at http://observer.com/2016/05/natos-big-new-russian-spy-scandal/.