RUSSIA'S HYBRID WARFARE IN THE EAST: USING THE INFORMATION SPHERE AS INTEGRAL TO HYBRID WARFARE

Article · June 2015

CITATIONS
39

READS
7,641

2 authors:

Sascha-Dominik Dov Bachmann
University of Canberra
129 PUBLICATIONS **494** CITATIONS
SEE PROFILE

Hakan Gunneriusson
Mid Sweden University
39 PUBLICATIONS **176** CITATIONS
SEE PROFILE

Russia's Hybrid Warfare in the East

The Integral Nature of the Information Sphere

Sascha Dov Bachmann and Håkan Gunneriusson

Future adversaries will increasingly rely on technological means to execute their operations, utilizing cyber capabilities to control or support 'Hybrid Threats.'[1] Hybrid Threats are multimodal, low intensity, kinetic as well as non-kinetic threats to international peace and security.[2] Examples of Hybrid Threats include asymmetric conflict scenarios, global terrorism, piracy, transnational organized crime, demographic challenges, resources security, retrenchment from globalization and the proliferation of weapons of mass destruction.

Cyber-conflict and cyber-warfare are great examples of the use of new technologies within the scope of Hybrid Threats. Cyber-war refers to a sustained, computer-based cyber-attack by a state (or non-state actor) against the IT infrastructure of a target.[3] The combination of new technology and its availability make cyber-supported or cyber-led Hybrid Threats so potent. Cyber threats strike at the core of modern war fighting by affecting Command and Control abilities, which have become vulnerable to such cyber-attacks.

Russia has been one of the most prolific users of cyber capabilities. In 2007, Russia attempted to disrupt Estonia's Internet infrastructure as retribution for the country's removal of a WWII Soviet War Memorial from the center of Tallinn.[4] Russia also augmented its conventional military campaign in Georgia with cyber capabilities, which severely hampered the functioning of government and business websites.[5]

Sascha Dov Bachmann, Assessor Juris, is an Associate Professor in International Law at Bournemouth University in the UK. He has served in various capacities as a Lieutenant Colonel in the German Army Reserves, and was a NATO Rule of Law Subject Matter Expert in NATO's 2011 Hybrid Threat Experiment and participates in related workshops at NATO and the national level.

Håkan Gunneriusson is the Head of Research of ground operations and tactical areas in the Department of Military Studies at Swedish Defense University, focusing on hybrid warfare, military ground tactics, as well as sociological and historical perspectives on military tactics and culture.

In the present conflict in Eastern Ukraine, Russia has effectively used the information sphere as an integral tool in its Hybrid War against the people of Ukraine.[6]

Hybrid Warfare. Russia's offensive policy of territorial annexation of Crimea and the active support of separatist groups within Ukraine has been met with a little resolve on the part of the West and NATO. Russia's (re-)annexation of Crimea is a fait accompli, and it is unlikely to be reversed anytime soon. Moreover, Russia's on-going support of separatist groups in the eastern parts of Ukraine, where Ukraine's Russian-speaking minority is in the majority, such as Donetsk and Luhansk, has markedly increased open military combat. President Vladimir Putin and Russia have already begun to fight a proxy war by using covert military operatives and mercenaries.[7] NATO has categorized this form of warfare as 'Hybrid War'.[8] Eastern Ukraine as "a new type of war, a Hybrid War, where armies do not always act as direct aggressors. Instead, they act to intimidate, while 'imported' diversionary groups, together with local extremists and criminal gangs carry out the fighting on the ground".[9] These actions are being supported by a plethora of Russian media-based disinformation and propaganda assets, as well as economic pressure tactics and the use of the information sphere to augment Russia's success.

Interestingly, Russia itself uses 'generational warfare' and others use terms like 'full-spectrum warfare' to describe the Ukraine conflict.[10] It is clear that the difference in Russian and Western terminology emphasizes the actors' perspectives and certain aspects of the conflict.[11] Along these lines, understanding 'hybrid warfare' in the context of the Ukraine crisis requires an analysis of the hybrid tactics employed and their goals relative to the actors involved in the conflict.

Russia has resorted to a new way of waging war, combining conventional and unorthodox methods of warfare, including the use of covert Special Forces as provocateurs, (dis) information campaigns by media outlets, cyber-attacks, and even leveraging its oil and gas resources to exert economic pressure.

Hybrid Warfare is a form of 'unreal warfare', and can be very difficult to define as warfare in the traditional sense. Ukraine's Security Chief concurred, describing Russia's war in

Following months of intense fighting in Ukraine, European powers reached a mid-February 2015 ceasefire, after a tense night of discussions in Minsk. The respite from hos-

tilities proved short-lived, as fighting resumed on Monday, February 16th, resulting in the capture of Debaltseve and subsequent retreat of Ukrainian forces. This fighting was part of a more elaborate information operation, relying heavily on Russia's ability to deny being involved. President Putin's goal of creating a Russian 'cordon sanitaire' against any EU/NATO expansion to the East means it is not farfetched to predict the conflict in Ukraine will continue and that the country will not be the last to encounter Russian aggression. At the time of the writing there are daily reports of new military activities by the Russian-backed rebels in the East of Ukraine.[12]

To achieve this objective, Russia has resorted to a new way of waging war, combining conventional and unorthodox methods of warfare, including the use of covert Special Forces as provocateurs, (dis)information campaigns by media outlets, cyber-attacks, and even leveraging its oil and gas resources to exert economic pressure.[13] This comprehensive mixture of methods and tactics of warfare can be best described as hybrid warfare,[14] which has strained NATO's response capabilities. With a political division among its member states evident, NATO seems unwilling to commit to a robust counter move to Russia's aggression.

The hybrid approach functions well for the West for two reasons. Firstly, it is obvious that the relative balance of military strength currently favors Russia. Given Russia's nuclear capabilities, there is a clear and omnipresent reluctance to go to war against Russia. This in itself is not just realpolitik, however.

Russia is also enjoying success against its EU and NATO rivals because the latter two have demonstrated little willingness to forcefully respond to the former's provocations. It's not just a lack of capability: the various publics constituting the European Union and NATO are wary of large-scale military engagements. The post-industrial states of Europe have excluded war and warfare – except in a limited and expeditionary form – from the horizon of possibilities as it is incompatible with economic progressivity. One can see this manifested in low military spending as a proportion of GNP in about every European country not bordering Russia.[15] One can also see it in the practice of EU states in relation to war. EU states often send expeditionary forces to former colonies (e.g. France in Mali 2012 and other African countries which have been French colonies) or contribute to UN-mandated missions and U.S. led operations (e.g. Libya 2011, Iraq 2003, or primarily NATO in Afghanistan from 2003). There has been no major military engagement or war of importance initiated by a EU country since the 1982 Falklands War, a conflict that was forced on the UK while it possessed a necessary level of combat readiness amidst the Cold War. Until recently, there was widespread optimism that war will not be seen on the borders of Europe for the foreseeable future. This belief paved the way for two interrelated weaknesses: cuts in domestic military spending and a focus on short-term, expeditionary missions rather than more traditional conflicts between states. This

fact is actively played upon by Russia. Peter Pomerantsev and Michael Weiss uses the phrase "weaponization of culture and ideas" to describe Russia's usage of culture as power.[16] One can extend the term to describe the exploitation of cultural weaknesses in other cultures, as in this case.

The first weakness might seem easy to correct by increasing defense expenditures. Yet the military weakness is also the symptom and consequence of the second reason mentioned above. This also makes the problem larger than just increasing the percentage of GNP spending on the military. It is an inherent structural problem in the post-industrial society of Western Europe.

As a result, Russia's denial of involvement in Ukraine, while hardly accepted as true, does provide states wary of military involvement the ability to "look the other way.".[17] As part of its denial strategy, Russia relies heavily on its information technology capabilities to sow disinformation. In short, hybrid warfare is based on relational asymmetries regarding the willingness to commit to war, the shortfall of capabilities to wage war, and the absence of the willingness to use force to repel Russian aggression.[18]

The denial of responsibility from the Russian government is an integral part of its hybrid warfare effort.[19] On a strategic-political level, it also allows Western European and other NATO states to not deal with the crisis in force for now. Deploying a rapid reaction force means little in this hybrid warfare scenario when it remains to be seen if there will be a political mandate to act in defense of, for example, the Baltic states against hybrid warfare and not conventional threats. The political will, and capability, in the West, to risk open war with Russia is small to say the least.[20] This approach is not without its risks, given that Russia seems committed to redrawing the post-Cold War political landscape of Europe. The UK defense secretary openly warned there was "a 'real and present danger' of Russia trying to destabilize the Baltic States of Latvia, Lithuania, and Estonia."[21]

Russia's Use of Disinformation in the Information Sphere. NATO's unwillingness to act in force in the Ukraine crisis can be explained in several ways: firstly, the war in Ukraine does not exist; secondly, even if it does exist, nothing can be known as certain (from the Russian deniability perspective, that Russian soldiers are seen in Ukraine are explained in a host of different ways) and thus cannot be communicated correctly. Thirdly, if the Ukraine conflict could be communicated, it cannot be understood completely, as it is a complex internal conflict and conflicting statements are produced all the time.[22] Russia disseminates misinformation to distract, confuse and degrade the opponent's capabilities and counter a threat. Denial from top-level Russian officials is the foremost tool for carrying out this disinformation approach. Furthermore, Russia utilizes strategic communication to promote de-escalation of the conflict. In many cases, international actors undertake de-escalating strategic communication in a legitimate way to avoid poten-

tial armed conflicts. However, Russia often communicates the necessity of compartmentalizing different incidents so they are not linked together in a way that risks conflict escalation. As a result, Russia's blurring of facts and fiction for disinformation purposes as well as its usage of strategic communication enables Russia further minimize the costs to its actions[23] These actions are especially useful against the EU and NATO, which are not used to or authorized to connect individual incidents into a bigger picture in a way that encourages escalatory retaliation.

Waging a concerted media campaign of disinformation on the Internet with sites such as Russia Today and Sputniknews are good examples of Russia's use of Internet media in support of military objectives. The fact the Russian air force is not being used in a close air support role highlights this observation. One reason for the air force's absence might be that its involvement would end the Russian masquerade of non-involvement: to perform airstrikes and other air missions while still denying accountability for the operations in Ukraine would be impossible. Despite these efforts to avoid detection, however, it has been widely verified that Russia has deployed regular Army units to fight in Ukraine.[24]

Russian cyber-war efforts are very much about perceptions and discursive power. During the conflict in Crimea, one finds more than a few Russian friendly actors on the Internet. Some are private actors and some are paid to wage the war over how the conflict is perceived: a meta-war. Russia is strong in this respect, predominantly because they are willing to invest in this activity. Support for this investment is driven primarily by internal factors in Russia, where the Internet is one the few remaining avenues to express popular dissent. Television is almost exclusively state-controlled and a common political tool of President Putin.[25] Even though the Internet is held out as a haven for liberal freedoms, it is hardly democratic: the Russian state has developed a robust capacity for information operations on the Internet.[26] Moreover, it is not a democracy in the respect that each individual has a single, equal voice. Russian authorities pay people to voice the same opinion from multiple "people." For example, one state-paid cyber-actor in St. Petersburg conveyed that she was acting as three different bloggers with 10 blogs while also commenting on other blogs as well. Another person was employed just to comment at least 126 comments every 12 hours. The purpose of both of these activities was clearly political: to support the Putin administration on the Internet.[27] These paid, online supports can spread a competing, false narrative about actual events, such as denying the presence of Russian military in Ukraine, or it can support fictional events as with the story of a crucified baby.[28] The latter serves the double purpose of both demonizing enemy forces (OPFOR) but also undermining the whole body of reporting from the conflict for those who do not believe in the statement. The Russian example suggests cyber activities will be integrated into future military conflicts, just as other revo-

lutionary technologies like electricity and the internal combustion engine. Going forward, more advanced regular or irregular conflicts will have a cyber-element, due in large part to growing dependence on cyber-enabled capabilities in civilian and military realms. Militaries are realizing the benefits of augmenting their conventional arsenal with cyber capabilities, especially since cyber-attacks could achieve short-term military objectives while minimizing risks associated with deploying actual kinetic capabilities.

Russia's use of misinformation is emblematic of its growing cyber-war capabilities and goes far beyond simple manipulation of digital media. Russia's ability to deny its direct and indirect support for Eastern Ukrainian rebels is essential for manipulation popular perception of what is happening in Ukraine. In this regard, the ability to control the media narrative surrounding events in Ukraine is a pre-requisite to the ongoing combat. That makes it a powerful weapon when integrated into warfare, but it is also a difficult weapon to control.

Russia has utilized a whole host of capabilities within the hybrid war/threat concept both in Crimea specifically and Ukraine more generally. Successful annexation of Crimea was very much dependent on Russia's ability to uphold its masquerade of deniability. This is increasingly clear if one looks at the conflict in the Donbas region of Ukraine, where tepid Western responses, up to and including the wish to ignoring Russian aggression altogether, have done little to inhibit Russia's comprehensive approach to waging hybrid war. The fact the United Nations Security Council approved a resolution calling for a stop of all fighting in Ukraine on February 17, 2015, despite the fact Russia is member of the Council and the primary instigator in Ukraine, is a powerful example of just how successfully Russia has successfully manipulated public opinion in the West, in no small part due to its policy of disinformation. Few modern historical examples demonstrate the success of an aggressor in promoting itself as a de facto appeaser similar to Russia today. The eventual outcome of the Munich Agreement of 1938, which can be seen as an act of aggression by Nazi Germany against Czechoslovakia in preparation of its eventual occupation, was mirrored in the Minsk Agreement of 2015, where Russia, like Germany before in 1938, as an aggressor tried to play a third party role of conciliator.[29]

...advanced regular or irregular conflicts will have a cyber-element, due in large part to **growing dependence on cyber-enabled capabilities in civilian and military realms.**

While debates regarding Russia's modus operandi and the proper international response are ongoing, it has

become increasingly clear the present crisis warrants a hybrid response. NATO's Bi-Strategic Command Capstone Concept of 2010 defines 'Hybrid Threats' as "those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives."[30] Having identified these threats, NATO began working on a comprehensive, conceptual legal framework for identifying and categorizing such threats within the wider frame of possible multi-stakeholder responses. In 2011, NATO's Allied Command Transformation (ACT), supported by the U.S. Joint Forces Command Joint Irregular Warfare Centre (USJFCOM JIWC) and the U.S. National Defense University (NDU), conducted specialized research into 'Assessing Emerging Security Challenges in the Globalized Environment (Countering Hybrid Threats) Experiment'.[31] In essence, hybrid threats faced by NATO and its non-military partners require a comprehensive approach allowing a wide spectrum of responses, including kinetic and non-kinetic, by military and non-military actors.[32] Essential to NATO's planning was the hypothesis that such a comprehensive response will have to be in partnership with other stakeholders, such as international and regional organizations, as well as representatives of business and commerce.[33]

In June 2012, NATO decided to cease work on Countering Hybrid Threats at its organizational level but continued to encourage its member states and associated NATO Excellence Centres to continue working on countering hybrid warfare tactics. Given NATO's inability and/or reluctance to address the Ukrainian situation with military force, as well as the fact that such force resides clearly outside of any NATO Non-Article 5 authority, its decision to cease work might have been made prematurely.[34] However, NATO seems once again willing to take up this challenge as its September 2014 Wales Summit Declaration shows:

> "We will ensure that NATO is able to effectively address the specific challenges posed by hybrid warfare threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design. It is essential that the Alliance possesses the necessary tools and procedures required to deter and respond effectively to hybrid warfare threats, and the capabilities to reinforce national forces."[35]

Russia's use of hybrid warfare may require a new NATO concept or a continuation of the work on NATO's dormant Hybrid Threat concept.[36] The official response and its level of success remain to be seen.

The Military and Cyber Warfare. Western militaries are often capable of protecting their own IT systems and hardware sufficiently, even if there are instances of breaches at the tactical level.[37] At the same time, the military has seldom possessed the capability to protect society as a whole. Civil society is a common target for cyber-attacks, even if it is not always apparent. This relation mirrors armed conflicts in general: the military has the ability to protect their operational assets and civilians

are protected indirectly from opposing military forces (OPFOR). However, civilian Internet Service Providers supply cyber-infrastructure, and they need to fend for their own in the modern cyber-arena. Civilian Internet providers are also important for supplying traditional logistics and communication systems to the military. If properly identified and attributed, the military might be in charge of confronting the source of said attacks. While that makes sense in theory, the reality of cyber-warfare is much more complex: it is nearly impossible to identify the perpetrators. This is especially important for hybrid attacks, even if not solely within the cyber-arena. In many ways, it seems as if the Russian hybrid war strategy in Crimea has borrowed from the lessons of the cyber-arena. In Ukraine, the use of soldiers without identification patches, also referred to as 'Green Men,' could be compared with malicious cyber-attacks with no clear method to identify the original perpetrator.

Russian military doctrine clearly underscores the importance of the information arena for their current definition of war. As one of the bullet points to define modern military conflicts in the Russian doctrine one finds the statement "the prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favourable response from the world community to the utilization of military force".[38] It is totally clear that what we see in Ukraine in terms of deniability and aspects of contactless war, augmenting the kinetic aspects of the conflict, is part of a coherent and preconceived doctrine.[39] Operations in the cyber arena are critical for Russian hybrid war efforts, as those operations make it easier for Russia to bypass international legal norms regarding territorial sovereignty and the use of force. Since NATO and other actors built their decision making on said international legal foundations, Russia can limit these actors' horizon of possibilities by manipulating information via their cyber capabilities.

Non-state actors are another consideration for the hybrid threat arena. The 2011 Arab Spring demonstrated the use of information technology by both citizens and the government had real effects on political stability.[40] Non-state actors, for better or worse, stand to benefit substantially from cyber capabilities, as they are relatively cheap and widely available. The 2008 Mumbai attack is one such example of the improved operational capabilities afforded by advances in the cyber domain.[41] The possibility to undertake these activities with scarce resources empowers resource-weak actors. This is a significant change to earlier conceptions of war and conflict being limited to contests between nation-states. Cyber-enabled, non-state actors pose a significant and ongoing challenge to controlling escalation in Ukraine. These groups are very difficult to distinguish from state-based actors, increasing the likelihood of misattribution in a crisis scenario. Valery Gerasimov, Russia's Chief of General Staff of the Russian Armed Forces, said these actors play a signifi-

cant role in the Ukrainian conflict. What led Russia to include non-state capabilities in their doctrine? As Gerasimov argues, Russian warfare should seek to influence events on the battlefield from afar and without use of kinetic warfare. Russia's cyberwar efforts exemplify the kind of warfare Geraismov describes.[42] The potential to deny perpetrating a cyber attack is considerable in the cyber sphere, but Russia has normalized this capability. In fact, one might see the whole of warfare in Eastern Ukraine as cyber-inspired in terms of deniability.

The Russian way of warfare takes place in different phases of conflict: The first three phases of the Russian warfare can be summarized as economic and diplomatic maneuvering, the use of targeted disinformation, and the use of bribing and even coercion of government personnel in order to make them comply with Russian political requests and strategies. The fourth phase aims at increasing dissent in the region, possibly with the influx of non-uniformed actors. The fifth phase includes military and economic blockades, private contractors and the imposing of a no-flying zone. The sixth phase includes electronic warfare, the use of air force and long-range artillery. The seventh phase is the end phase were ground troops as well as special forces attack. Special forces operatives are used in a combat role but also to guide missile strikes and close air-support.[43]

Examples of this modus operandi can be seen in the extensive use of artillery in Eastern Ukraine by separatist and anti-Ukrainian forces. The disproportionate use of artillery is telling when compared to the strategic dicta of the combined weapons doctrine, which posits that military victory is only possible when all military capabilities are effectively combined. In the case of Ukraine, this would require the supporting role of artillery for armor- and infantry-led operations. The Ukrainian theatre has seen periods of long intermittent shelling without actual maneuvers by rebel and government forces. This implies either the opposing forces lack the capabilities to apply the combined approach, or the use of artillery is used solely to terrorize the civilian population, reminiscent of tactics during the Balkans Wars of 1991 to 1995, during which Sarajevo was constantly bombarded by artillery to terrorize the civilian population. Valeriy Gerasimov's "non contact clashes" are exemplified by the extensive use of artillery in Ukraine as it provides the user with a certain degree of deniability.[44] Even if the artillery's position is tracked and identified, it is still difficult to fully corroborate the accusation. The lack of Russian air

Cyber-enabled, non-state actors pose a **significant and ongoing challenge to controlling escalation in Ukraine.**

assets in Eastern Ukraine is based on a similar logic: even though the Russian Air Force is powerful, the Kremlin does not want to give up its ability to deny direct involvement in the conflict. The possibility to deny involvement is much harder with aircraft that are easily tracked when they cross borders. At the same time, Russian anti-air capabilities have precluded the use of air assets by Ukrainian forces, as the tragic events of MH 17 highlight.[45] In this way, there are clear tactical effects on the ground linked to hybrid warfare that are perceivable for the spectator on the ground; the hybrid warfare concept is not just an abstract, strategic take on warfare.

It is also important to consider the host of other cyber actions that cannot be classified as direct physical attacks. The most important ones are the easiest ones: denying services and information operations. So called Distributed Denial of Service Attacks (DDoS) are not very harmful physically. They supress targeted sites, but only as long as attackers exert continuous pressure on compromised systems. Afterwards, the site returns to normal functionality. The 2007 Russian cyber-attack on Estonia is a prime example of this type of attack. Estonia was essentially sealed off from the Internet for several days.[46] The damage of DDOS attacks can be discussed in purely economic terms: the loss of profit due to downtime or lost opportunities.[47] DDOS attacks aren't just limited to economic sabotage; there is evidence of such attacks in conjunction with the Ukrainian election of 2014. Because elections are by their nature time-limited, DDOS attacks are especially effective, as they can undermine the political process by freezing critical assets for a short period of time.[48] Just as military offensives often create a state of emergency, one can expect DDOS attacks in compressed time and space horizons to generate similar and significant effects.

In short, cyber-attacks on the operational level are incredibly useful in support of military operations that go beyond the cyber arena alone. The more the Internet becomes integrated into all aspects of civilian life and military operations, the more effective cyber-attacks will become in supporting operations. This supporting role has to be distinguished from sole cyber-warfare, which is developing into a new form of warfare on its own. These multifaceted military applications of cyber capabilities raise questions about the legal framework governing their use. NATO has only recently developed a comprehensive legal framework to govern cyber operations. Since 2009, the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia has intensely studied the legal framework of such operations. In 2013, NATO produced the Tallinn Manual on the law governing cyber warfare in 2013.[49] The Manual highlights there is no distinct law governing cyber armed conflict and that the Law of Armed Conflict (LOAC) does apply when a cyber-attack "is reasonably expected to cause injury or death to persons or damage or destruction to objects," as witnessed in the Stuxnet operation.[50] Unfortunately, applying the Tallinn Manual to the conflict in Ukraine

would do little to help grapple with ongoing hybrid operations, as legal frameworks have not yet caught up to realities on the ground. Nevertheless, the Tallinn Manual is still a positive development in the development of binding frameworks that can account for future hybrid war scenarios.

Conclusion. For now, Russia seems to hold the edge in the Hybrid War in Ukraine: it has successfully annexed Crimea and effectively turned Ukraine in a state on the brink of wider failure. Russia's victory is a product of its relative military strength and the unwillingness of Western European countries to respond with military force. Russia's hybrid warfare strategy has allowed it to succeed on the ground while avoiding actions that could provoke a more forceful (and potentially kinetic) response from Western European nations and the United States. Russia's cyber capabilities have played an essential role in this careful balancing act. Cyber-driven deniability and misinformation have made it unlikely NATO will respond in a more forceful way, because lack of attribution gives Western European leaders the ability to look the other way and bide their time. Russia's use Western media outlets such as RT as well as various soft power assets in politics and media continue to delegitimize any further robust response by the West.

None of this is to say NATO has completely ignored the situation as the Wales Summit Declaration of 5 September 2014 shows. Whether that will translate into a more robust response to the Russian aggression remains to be seen. In November 2014, NATO released its new Readiness Action Plan, which promoted increased military presence and adaptation measures in Eastern member countries to boost readiness and bolster conventional deterrence. While this sounds like a robust response, it has to be noted nothing in the new plan expands NATO's Article 5 collective self defense commitment, hence doing little to resolve the problems posed by a Russian military strategy designed to stymie traditional strategic thinking in NATO. Tellingly, the new action plan also does little to deal with the threat posed by Russia's cyber capabilities. NATO's readiness plan is a step in the right direction, but many unanswered questions remain. What criteria will have to be met for it to be used in a 'hot' conflict situation? Will NATO commit combat assets in if response to a future separatist uprising of ethnic Russians? NATO intervention in this scenario may provoke Russia to intervene with the whole host of its conventional capabilities, which could start a war. While that would undoubtedly be a risky decision by the Kremlin, President Putin has surprised many with audacious actions in Ukraine. If NATO failed to intervene, the decision could fundamentally reshape the meaning of Article 5 treaty commitments. NATO leaders must answer these outstanding questions in the coming months if they wish to more fully control the situation in Ukraine and Eastern Europe.

NOTES

1 Bachmann, S-D., "Hybrid Threats, cyber warfare and NATO's comprehensive approach for countering 21st ccentury threats – mapping the new frontier of global risk and security management", 88 Amicus Curiae 2011; Bachmann, S-D. and Gunneriusson H, " Terrorism and Cyber Attacks as Hybrid Threats: Defining a Comprehensive 21st Century Approach to Global Security", *The Journal on Terrorism and Security Analysis*, 26-37.

2 Bachmann S-D and J Sanden, "Countering Hybrid Eco-threats to Global Security Under International Law": The Need for an Comprehensive x Approach", 33 (3) *Liverpool Law Review* 261 - 289.

3 See generally, Jenny Döge "Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime" (2010) 48 *Archiv des Völkerrechts* 486.

4 See Ian Traynor, "Russian accused of unleashing cyberwar to disable Estonia", *The Guardian* (17 May 2007) online: Guardian Unlimited http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

5 http://www.newsweek.com/how-russia-may-have-attacked-georgias-internet-88111?piano_d=1, http://www.computerworld.com/article/2534930/networking/georgia-president-s-web-site-falls-under-ddos-attack.html, http://www.civil.ge/eng/article.php?id=18896, http://www.computerworld.com/article/2532289/cybercrime-hacking/cyber-attacks-knock-out-georgia-s-internet-presence.html, http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html. [150325].

6 See more on this form of warfare, Bachmann, S-D. and Gunneriusson H, "Hybrid War: The 21st Century's New Threats to Global Peace and Security", *Scientia Militaria, South African Journal of Military Studies*, Vol 43, No. 1, 2015, pp. 77 – 98.

7 Bachmann S-D, Russia's 'spring' of 2014http://blog.oup.com/2014/06/russia-putin-Hybrid-war-nato/

8 John Vandiver, "SACEUR:Allies must prepare for Russia 'Hybrid war'" at http://www.stripes.com/news/saceur-allies-must-prepare-for-russia-Hybrid-war-1.301464. For a discussion of the term 'Hybrid War': Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, 2007.

9 *Ft.com,* "Ukraine's security chief accuses Russia of waging 'hybrid war'", 28 May 2014, http://on.ft.com/1kgoAmx.

10 Oscar Jonsson and Robert Seely "Russian Full-Spectrum Conflict: An Appraisal After Ukraine" in *Journal of Slavic Military Studies*, 28:1–22, 2015.

11 A term itself has to be filled with meaning, and after that the use of the term can be measured. Just stating that a term is "limited" before one makes use of it is a convenient way of staying within the own restricted parameters of strategic thinking. See Michael Kofman and Matthew Rojansky "A Closer Look at Russia's 'Hybrid War'" *Kennan Cable* no.7 2015. http://www.wilsoncenter.org/publication/kennan-cable-no7-closer-look-russia%E2%80%99s-%E2%80%9Chybrid-war%E2%80%9D [150528] They discharge the tem 'hybrid warfare' without really dealing with its content.

12 See e.g. *BBC* "Ukraine crisis: Heavy fighting rages near Donetsk, despite truce", 3 June 2015, at http://www.bbc.co.uk/news/world-europe-32988499.

13 See for example Oscar Jonsson and Robert Seely "Russian Full-Spectrum Conflict: An Appraisal After Ukraine" in *Journal of Slavic Military Studies*, 28:1–22, 2015. pp.12.

14 http://www.nato.int/docu/review/2014/russia-ukraine-nato-crisis/Russia-Ukraine-crisis-war/EN/index.htm

15 http://www.sipri.org/research/armaments/milex/milex_database [150609]

16 Peter Pomerantsev and Michael Weiss "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money" in *The Interpreter* http://www.interpretermag.com/the-menace-of-unreality-how-the-kremlin-weaponizes-information-culture-and-money/ [150529].

17 Gitta Sereny shows a similar mechanism in her book *Albert Speer: His Battle with Truth*. 1995 Vintage Books Where Albert Speer states that he didn't know about the Holocaust because he looked the other way. But looking the other way has the prerequisite of actually knowing.

18 This version of Hybrid War differs from what Frank G. Hoffman originally defined some years ago: "I define a hybrid threat as: Any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism and criminal behaviour in the battle space to obtain their political objectives." The difference between the two examples presented above is primarily about focus; Hoffman speaks in general terms, whereas this text aligns the term 'Hybrid' with the Ukrainian scenario. This level of specificity distinguishes the term such that it falls under the boundaries of short range social theory, i.e. it is operative within special cases. Hoffman's definition has a wider scope and focus; the fact that it can be applied wider and thus can be called a middle range social theory. When dealing with Russia's Hybrid Warfare, the short range theory is recommended. See Frank G. Hoffman "Hybrid vs. compound war. The Janus choice: Defining today's multifaceted conflict" in Armed Forces Journal International 2009. Springfield. http://indianstrategicknowledgeonline.com/web/4198658.pdf [150529].

19 Here one can refer to a term of Peter Pomerantse and Michael Weiss "the Weaponization of Information" They do not touch upon the aspect of communication deniability in conjunction with the duel situation versus the West, but the term is still a fitting one. Peter Pomerantse and Michael Weiss "The Menace of Unreality:How the Kremlin Weaponizes Information, Culture and Money" in *The Interpreter* http://www.interpretermag.com/the-

menace-of-unreality-how-the-kremlin-weaponizes-information-culture-and-money/ [150529].

20 See for example Janis Berzins *Russia's new generation warfare in Ukraine: Implications för Latvian defense policy.* In *National Defence Academy of Latvia Center for Security and Strategic Research* 2014:2. There he states that if NATO article 5 is not valid in a Crimean-scenario on Latvian soil then a provocation by the Latvian Army "must be avoided by all means". p. 9.

21 BBC, "Russia 'danger' to Latvia, Lithuania and Estonia," February 2015: http://www.bbc.co.uk/news/uk-31528981.

22 NATO's strategy is here described exactly as the thinking of Greek Sophist Gorgias (c. 485 – c. 380 BC) on the non-existent. Charles H. Kahn "Gorgias", Ed. Edward Craig. *Routledge Encyclopedia of Philosophy*, Volume 4 (1998). p.145. Routledge. London & New York.

23 See the report *Hiding in Plain Sight: Putin's War in Ukraine* for good proof of Russian involvement on the Ground in Ukraine, by Maksymilian Czuperski, John Herbst, Eliot Higgins, Alina Polyakova, and Damon Wilson https://www.dropbox.com/s/qmy5n0kgiw3pxwp/HPS_0528_web.pdf?raw=1 [150529]

See also Boris Nemtsov's [edited post mortem] Putin. War http://www.4freerussia.org/putin.war/ [150529].

24 "EU breaks taboo on 'Russian forces in Ukraine" *EU Observer* https://euobserver.com/foreign/127667 (last accessed 18-02-2015). A practical example of a tool for disinformation is *Russia Today* http://rt.com/. It is funded by the Russian state and broadcasts on television as well as having a large and active site on the Internet.

25 Peter Pomerantsev *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia.* (2014) PublicAffairs. New York.

26 *The Intepreter Magazine*, "Russia Update: Defense Ministry Plans New Computer Programs to Monitor, Analyze Social Media," January 29, 2015: http://www.interpretermag.com/russia-update-january-29-2015 [150529].

For more examples see: Peter Pomerantse and Michael Weiss "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money" in *The Interpreter*, Institute of Modern Russia. http://www.interpretermag.com/the-menace-of-unreality-how-the-kremlin-weaponizes-information-culture-and-money/ [150529].

27 "They are Putin's soldier on Internet" ("De är Putins soldater på nätet") http://www.dn.se/nyheter/varlden/de-ar-putins-soldater-pa-natet/ [150211].

28 About the crucified baby reporting, see link. The same women was used as acting as a survivor from an actual event when a grenade struck a bus in Donetsk: http://www.bbc.co.uk/monitoring/how-russian-tv-uses-psychology-over-ukraine [150211]

29 Al Jazeera, "UN Security Council calls for Ukraine fighting to stop", http://www.aljazeera.com/news/2015/02/resolution-ukraine-cease-fire-150217220633057.html

30 cf BI-SC Input for a New NATO Capstone Concept for The Military Contribution to Countering Hybrid Enclosure 1 to 1500/CPPCAM/FCR/10-270038 and 5000 FXX/0100/TT-0651/SER: NU0040, dated 25 August 2010.

31 cf NATO's *Transnet* network on Countering Hybrid Threats (CHT) at https://transnet.act.nato.int/WISE/Transforma1/ACTIPT/JOUIPT.

32 see "Updated List of Tasks for the Implementation of the Comprehensive Approach Action Plan and the Lisbon Summit Decisions on the Comprehensive Approach", dated 4 march 2011, p 1-10, paragraph 1

33 "NATO Countering the Hybrid Threat" at http://www.act.nato.int/multimedia/archive/41%E2%80%90top%E2%80%90headlines/747%E2%80%90nato%E2%80%90countering%E2%80%90the%E2%80%90Hybrid%E2%80%90threat

34 Bachmann S-D, "Crimea and Ukraine 2014: A Brief Reflection on Russia's 'Protective Interventionism", *Jurist-Forum, May 18th, 2014*, http://jurist.org/forum/2014/05/sascha-bachmann-ukraine-hybrid-threats.php

35 NATO *Wales Summit Declaration* , par 13 Sept 2015, at http://www.nato.int/cps/fr/natohq/official_texts_112964.htm?selectedLocale=en.

36 See Davis, J A, "Continued Evolution of Hybrid Threats – The Russian Hybrid Threat Construct ad the Need for Innovation",

http://www.jwc.nato.int/images/stories/threeswords/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf.

37 See for example Rawnsley, A, "Iran's alleged drone hack: tough, but possible", *Wired*, 2011. http://www.wired.com/dangerroom/2011/12/iran-drone-hack-gps/. [150128].

38 *The Military Doctrine of the Russian Federation*, February 5, 2010, [Translated excerpt] http://carnegieendowment.org/files/2010russia_military_doctrine.pdf. Also S.P. Rastorguev Informatsionnaya voina (Information Warfare) Radio i sviaz, 1998. Also V.K. Kopytko "Evolution of Operational Art" Military Thought, Vol. 17, No. 1, 2008. Also Afanasjev, M 2011, "Approaches to avoiding government censorship, blockade and surveillance on the Internet", Master's thesis, Tallinn University of Technology. Russia used cyber attacks before its war on Georgia too. Also Markoff, J, "Before the gunfire, cyber-attacks", 2008 NYTimes.com,http://www.nytimes.com/2008/08/13/technology/13cyber.html. Russian actors also laid a cyber-siege on Estonia 2007. Also Håkan Gunneriusson "Nothing is taken serious until it gets serious". 2012 in Defence Against Terrorism review. Vol IV, #7. Also Dan Holden "Estonia, six years later" in DDoS & Security Reports http://www.arbornetworks.com/asert/2013/05/estonia-six-years-later/ [150128].

39 Compare with Michael Kofman and Matthew Rojansky "A Closer Look at Russia's 'Hybrid War'" Kennan Cable no.7 2015. http://www.wilsoncenter.org/publication/kennan-cable-no7-closer-look-russia%E2%80%99s-%E2%80%9Chybrid-war%E2%80%9D [150528]. They simple state without backing it up with a look at 1) what is happening in Ukraine 2) Russian military doctrine that Russia's operations in Ukraine is neither part of a coherent or preconceived doctrine.

40 See for example Ivan Watson, *CNN* https://www.youtube.com/watch?v=1bSj4f9f8Eg&desktop_uri=%2Fwatch%3Fv%3D1bSj4f9f8Eg [150128].

41 Håkan Gunneriusson "Nothing is taken serious until it gets serious". 2012 in *Defense Against Terrorism Review*. Vol IV, #7.

42 Valery Gerasimov. "The value of science in anticipation. New challenges require rethinking the forms and methods of warfare". http://www.vpk-news.ru/articles/14632 [150325].

43 Berzinš, Janis. "Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy" *Policy Papper no 02 April 2014*. Riga: National Defense Academy of Latvia, 2014. p.6

44 For an example where MLRS is tracked as fired from Russia into Ukraine: https://www.youtube.com/watch?v=s5bB1726gLg [150325].

45 *Air denial* is a degree of air control, which is better than *Air incapability* but worse than Air parity. Air denial permits Air superiority for the other side, something which is not utilized in Ukraine. See Bachmann, S-D. (2014) "Malaysia Airlines Flight MH17: the day Russia became a state sponsor of Terrorism", 97 Amicus Curiae, p 14-16.

46 Ottis, R. (2008) "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective". In *Proceedings of the 7th European Conference on Information Warfare and Security,* Plymouth. Reading: Academic Publishing Limited, p 163-168.

47 Lindsey Havens, "DDoS on the rise: the AK-47 of cybercrime," *PhishLabs*, January 23, 2015: http://blog.phishlabs.com/ddos-on-the-rise-the-ak-47-of-cybercrime [150528].

48 Joseph Marks, "Hackers DDoS Ukraine Elections," *Politico*, October 2014: http://www.politico.com/morningcybersecurity/1014/morningcybersecurity15841.html [150128]. Even Russia has been attacked by similar means: See ITAR-TASS, "Kremlin says DDoS-attack unrelated to events in Ukraine," March 14, 2014: http://tass.ru/en/russia/723521 [150528].

49 The Tallinn manual: http://www.knowledgecommons.in/wp-content/uploads/2014/03/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf

50 Tallinn Manual, rule 30.