The New Colour of War –
Hybrid Warfare and Partnerships

Ralph D. Thiele

October 2015

Abstract

Twenty-first century Europe exists in a dynamic strategic environment, in which opponents can be affected significantly by hybrid means, keeping them off balance politically, militarily, and even societally. At this point, neither the European Union (EU) nor the North Atlantic Treaty Organisation (NATO) is well prepared to meet these challenges. Hybrid war is a potent, complex variation of warfare. What makes it so dangerous is the rapidity with which one can escalate conflict in the digital world.

In the past, irregular tactics and protracted forms of conflict have mostly been marked as tactics of the weak, employed by non-state actors who do not have the means to do better. Today and in the future, opponents may exploit hybrid opportunities because of their effectiveness. The art of hybrid warfare is not found in front line manoeuvres, but rather in the zones of security that either not black-and-white: grey is the new colour of war.

In between already two models of hybrid warfare have come to the fore – the "*Russian*" model and the "*ISIS*" model. Both are relevant and have provided for a broad spectrum of insights and lessons. Clearly, while the colour of hybrid warfare is grey, meeting hybrid challenges requires a colourful spectrum of partner capabilities. Successfully meeting hybrid challenges requires trusted, capable and interoperable partners. Consequently, within any hybrid warfare strategy specific consideration must be given to the role of partner nations and organisations.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is objective and task oriented and is above party politics.

The increasingly complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, brings with it major opportunities but also risks: thus, decision-makers in the private sector and in politics depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, economy, international relations, and security/ defense. ISPSW network experts have worked – in some cases for several decades – in executive positions and thus dispose over wide–ranging experience in their respective fields of expertise.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analysis

1. Falling apart at the Seams

The increasingly hybrid nature of security challenges has rendered the security situation on a global scale far more complex. Today, this view is not necessarily broadly shared in Brazil.[1] However similar scepticism was evinced with regard to cyber security up until Edward Snowden, in the summer of 2013, unveiled the U.S. interest in Brazilian decision-making. Suddenly cyber became a No 1 issue in Brazilian foreign and security policy with Germany and Brazil jointly presenting a UN resolution on cyber privacy.[2] Perceptions can change swiftly these days.

Twenty-first century Europe exists in a dynamic strategic environment, in which opponents can be affected significantly by hybrid means, keeping them off balance politically, militarily, and even societally. At this point, neither the European Union (EU) nor the North Atlantic Treaty Organisation (NATO) is well prepared to meet these challenges.

NATO Secretary Stoltenberg stated recently: *"To the south we see turmoil, violence in Syria, Iraq, North Africa. We see terrorist attacks taking place in our own streets, often inspired by the violence in the Middle East, North Africa. And then we see to the east a more assertive Russia, a willing to use military force, to change borders, to annex a part of another country, for the first time since the Second World War. So therefore we have to adapt and we are adapting, partly by increasing the readiness, the preparedness of our forces. We are implementing the biggest reinforcement of collective defence since the end of the Cold War. And we are doing so as Alliance, and we work with partners ... to make this adaptation and to be ready to face the new security environment [sic]"*[3] It is expected that NATO will publish its hybrid warfare strategy this autumn.

It appears the world is falling apart at the seams. The opening sentences of the European Security Strategy of 2003 have become aged. *"Europe has never been so prosperous, so secure nor so free. The violence of the first half of the 20th Century has given way to a period of peace and stability unprecedented in European history".*[4] Suddenly, the rivalry between East and West is back. On top of which the challenges along Europe's southern flank have become considerable.

The security status quo has been altered, particularly by the crisis in the Ukraine. In a complex security situation issues and challenges such as the Global Commons, anti-access/area denial (A2AD) strategies and in particular hybrid challenges have come to the fore. Using the hybrid warfare model to advance its goals, Russia has started destabilising a whole region, seeking to exploit strategic ambiguity through a blend of soft and hard power, exploiting vulnerabilities in nations thus undermining the democratic rule of law and sowing seeds of doubt and insecurity so as to challenge the cohesion of the Alliance. This hybrid approach has been reinforced by the threatened use of conventional and even nuclear weaponry.

---

[1] Frederico Aranha. „Hybrid war – does it even exist?" defesanet.
http://www.defesanet.com.br/en/intelligence/noticia/19074/Hybrid-war-–-does-it-even-exist-/
[2] ALJAZEERA America. „*Germany, Brazil present UN resolution on cyberprivacy, Resolution calls for countries to extend right to privacy to Internet, other electronic communications*". November 7, 2013. http://america.aljazeera.com/articles/2013/11/7/brazil-and-germanydraftunresolutiononcyberprivacy.html
[3] Jens Stoltenberg. NATO Secretary General. Speech by at the opening session of the Croatia Forum 2015. Dubrovnik.
http://www.nato.int/cps/en/natohq/opinions_121655.htm?selectedLocale=uk
[4] European Security Strategy. Brussels 2003.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Russia's hybrid campaign in the Ukraine appears to be achieving Moscow's desired results.[5] Flooding the region with illegal weapons; using mercenaries to destroy regional infrastructure; weakening the local economy; blocking state functions, in particular law enforcement, justice and social welfare; causing a refugee crisis; exploiting social media and information warfare; and introducing its own peace keeping forces into the area – comprise some of the tactics which are proving effective. The core message that can be drawn from the hybrid campaign is: While traditional combat still remains a possibility, it will no longer be the primary means to victory on the battlefield of the 21st century.[6]

2. Hybrid Warfare

"Hybrid warfare" describes a form of violent conflict that simultaneously involves state and non-state actors, with the use of conventional and unconventional means of warfare that are not limited to the battlefield or to a particular physical territory. Of course, mankind has seen variations of hybrid warfare before.[7] The novelty is the scale of its use and the exploitation of old tools in modern, networked societies.

The term "hybrid" refers to something heterogeneous. It implies a blurring of the distinction between military and civilian.[8] Hybrid warfare employs all dimensions of state and non-state actors with elements of state-like power such as:

- The use of conventional military force (including use of unmarked Special Forces).
- Intimidation by the threatened use of nuclear weaponry.
- Employment of cyber to disrupt and destabilise.
- Use of economic levers to undermine the political cohesion of states and institutions.
- Massive propaganda and disinformation campaigns, through strategic communications and a distorted form of "*public diplomacy*".

Thus hybrid warfare is characterised by

- A broad mix of instruments – which includes the use of military force, technology, criminal activity, terrorism, economic and financial pressures, humanitarian and religious means, intelligence, sabotage, disinformation – are employed across the whole spectrum of warfare – traditional, irregular and/or catastrophic.
- Its stealthy approach[9] and disruptive capacity, executed within the context of a flexible strategy.
- Non-state actors' involvement such as militias, transnational criminal groups, or terrorist networks, mostly backed by one or several states, via a form of sponsor-client or proxy relationship. In other cases, states can also intentionally act in "hybrid" manners when they choose to blur the lines between covert and overt operations. Of particular interest in this context are irregular forces clothed in uniforms without national identification tags. As these irregular actors often are

[5] Reuben F Johnson. *"Russia's hybrid war in Ukraine 'is working'"*. IHS Jane's Defence Weekly. Kiev. 26 February 2015.
[6] Jordan Bravin. "*Getting behind Hybrid Warfare*". CICERO Magazine. July 17, 2014. http://ciceromagazine.com/essays/getting-behind-hybrid-warfare/
[7] Jens Stoltenberg. NATO Secretary General. "*Zero-sum? Russia, Power Politics, and the Post-Cold War Era*". *Brussels Forum*. 20 March 2015.
[8] Rob de Wijk. "*Hybrid Conflict and the Changing Nature of Actors*". In: Julian Lindley-French and Yves Boyer (eds.), "The Oxford Handbook of War". Cambridge 2012. p. 358.
[9] Andrew Kramer and Michael Gordon, "Ukraine Reports Russian Invasion on a New Front," *The New York Times*, 27 August 2014.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

provisioned with modern military equipment, they can perform and resist organised military assaults in force-on-force engagements.[10]

- Unlimited use of space. Hybrid warfare is not limited to the physical battlefield. On the contrary, hybrid actors seize every opportunity to engage in whatever space is available. This includes traditional and modern media instruments. The main intention in the strategy for political subversion is to isolate and weaken an opponent by eroding his legitimacy in multiple fields. "*Under this model, war takes place in a variety of operating environments, has synchronous effects across multiple battlefields, and is marked by asymmetric tactics and techniques*."[11]

Hybrid war appears to be a construct of vaguely connected elements. But the pieces are a part of a whole. It is a war that appears to be an incomprehensible sequence of improvisations, disparate actions along various fronts – humanitarian convoys followed by conventional war with artillery and tanks in, for instance, eastern Ukraine, peacekeeping operations in Transnistria, cyber-attacks in Estonia, vast disinformation campaigns on mass media, seemingly random forays of heavy bombers in the North Sea, submarine games in the Baltic Sea, and so on. The diversity of hybrid tactics masks an order behind the spectrum of tools used. It is this order and goal that makes it incumbent upon political leaders and strategic thinkers to classify such activities accurately within the political objectives discussed by Carl von Clausewitz, who noted that war is an extension of politics by other means.

Clausewitz also reminds us that war is a chameleon. Hybrid war fully lives up to this assessment. It is a potent, complex variation of warfare. What makes it so dangerous is the rapidity with which one can escalate conflict in the digital world. Consequently, a broad politico-military debate has started as to whether a new form of warfare has been born.

3. Hybrid Models

When ISIS made its way across western Iraq, observers described it as "*hybrid warfare*." The same happened, when Ukrainian rebels seized control of Crimea and various cities throughout south-eastern Ukraine. In the past months in Europe there has been a split as to which kind of hybrid challenges to focus on. Within NATO and the EU, northern members such as the Baltic States, Poland and Germany when considering hybrid warfare think immediately of the "*Russian*" model. Whereas Italy, France, Greece and Spain see the "*ISIS*" model as at least as threatening.

a. The "ISIS" Model

A decade ago ISIS[12] – known as the "*Islamic State in Syria*" – emerged as a small Iraqi affiliate of Al Qaeda. At that time it was specialised in suicide bombings and inciting Iraq's Sunni Muslim minority against the country's Shiite majority. Today ISIS is increasingly a hybrid organisation following the Hezbollah model – part terrorist network, part guerrilla army, part proto-state entity.[13]

Hezbollah demonstrated the ability of non-state actors to study and deconstruct the vulnerabilities of Western-style militaries and devise appropriate countermeasures in the war against Israel in 2006. Its combat groups

[10] Paul Scharre, "Spectrum of What?," *Military Review*, November-December 2012, p. 76.
[11] Alex Deep, "Hybrid War: Old Concept, New Techniques," Small Wars Journal, 2 March 2015.
[12] Other acronyms are IS, ISIS or the Arabic 'daeesh.'
[13] Steve Coll. "*Search of a Strategy*". The New Yorker. SEPTEMBER 8, 2014 ISSUE. http://www.newyorker.com/magazine/2014/09/08

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

engaged as a hybrid between a guerrilla force and a regular army and displayed all the elements of hybrid warfare: *"… the simultaneous use of a conventional arsenal, irregular forces and guerrilla tactics, psychological warfare, terrorism and even criminal activities, with support from a multi- dimensional organization and capable of integratingvery different sub-units, groups or cells into one united, large force."*[14]

The military effects of Hezbollah´s conventional strikes were rather limited. Yet the consequences for Israel were substantial. The attacks *"…terrorized the north of Israel, paralysed the country´s economy and forced over a million civilians to temporarily evacuate."*[15] Additionally Hezbollah challenged Israel with a broad propaganda campaign. This led to an overwhelming perception within the Arab world and beyond, that Israel had been defeated at the hands of Hezbollah.[16]

With the Syrian Civil War, a follow-on hybrid warfare case showed up. ISIS' current campaigns in Syria, Iraq and in a growing number of other places in the Middle East-North African region show many characteristics of the hybrid warfare concept. Founded as a jihadist terrorist organisation, ISIS was later reinforced by former officers from Saddam Hussein's dissolved army, as well as by local Sunni tribes, and Chechen fighters with experience in irregular warfare, and foreign jihadists from all over the world. ISIS' strategy of control of natural resources, speed of operations, and recruitment of foreign fighters has fuelled its rise throughout the Greater Middle East and North Africa. ISIS has conquered cities, oil fields, and vast territories in both Syria and Iraq. The movement draws its strength from Sunni Arab communities bitterly opposed to the Shiite-led government in Baghdad and the Alawite-dominated regime in Damascus. With the advent and spread of ISIS, state boundaries and national identities are fading. This shift has the potential to push the entire region into chaos.

In its military operations, ISIS employs bombings, artillery and mortar shelling, suicide attacks, aerial reconnaissance, and even chemical attacks. Most operations are conducted by small, highly mobile units on pick-up trucks that are equipped with heavy machine guns. ISIS has shown remarkable combat capabilities and a high level of intelligence and reconnaissance skills based on a network of local supporters and informants. Additionally, it conducts a modern and sophisticated propaganda operation to recruit international volunteers and obtain financial support. These activities are founded on the narrative of the "caliphate", an idealised Islamic government led by the supposed successor of the Prophet Muhammad, which is used as a religious source of legitimacy and as a tool to undermine the identity of its opponents. To finance its activities, it has generated significant income through criminal activities such as smuggling, the sale of oil, the looting of antiquities, kidnapping for ransom, blackmailing, and the "taxation" of ISIS controlled populations.

It comes as no surprise that ISIS has already arrived in the Libya where several thousand militants are now fighting for the Islamic State. Since early 2015, ISIS has carried out a number of attacks and has captured the Mabruk oilfield south of Sirte. The militants also beheaded 21 Egyptian Coptic Christians earlier this year.[17]

It must, however, be mentioned that ISIS' opponents also employ elements of hybrid warfare. The Baathist dictatorship has employed a wide array of means ranging from indiscriminate shelling and air force bombardments to targeted operations in combination with Shabiha paramilitaries. Iran has also contributed to the practice of hybrid war in Syria and Iraq, supporting both the Assad regime and Iraqi government troops with logistics, supplies and military planning. Even the international coalition against ISIS is implementing

[14] Marcin Andrzej Piotrowski. "*Hezbollah: The Model of a Hybrid Threat*". *PISM Bulletin*, no. 24, March 2015.
[15] Marcin Andrzej Piotrowski, "*Hezbollah: The Model of a Hybrid Threat*," *PISM Bulletin*, no. 24, March 2015.
[16] Alex Deep. "*Hybrid War: Old Concept, New Techniques*". *Small Wars Journal*, 2 March 2015.
[17] State Department. "*ISIS capitalizes on Libya security vacuum, establishes 'legitimate foothold'*". rt. March 21, 2015. http://rt.com/usa/242809-isis-threat-libya-security/

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

flexible and unconventional instruments of war against the terrorist organisation via a combination of traditional air power, weapons supplies to Kurdish Peshmergas, the deployment of advisors to Iraqi government troops and sectarian militias, and training activities for Syrian opposition forces.[18]

In a particularly pertinent article on the Islamic State, Scott Jasper and Scott Moreland conclude their remarks[19] with the observation that "*... the Islamic State is a formidable, but not unassailable hybrid threat*..." To illustrate this, they identify six characteristics:

- Blended tactics: ISIS forces include traditional military units as well as smaller, semi-autonomous cells, combining both conventional and guerrilla warfare tactics. They possess a wide array of weaponry, from improvised explosive devices (IEDs) and mines to rocket-propelled grenades (RPGs), drones, and chemical weapons.
- Flexible and adaptable structure: ISIS quickly absorbs and deploys new resources. Whether new recruits, weaponry, or territory, ISIS constantly incorporates new acquisitions into its strategy and structure.
- Terrorism: Through acts of grotesque and exaggerated violence, ISIS communicates its ideology to a wider audience. The slaughter of Yazida and Chaldean Christian minorities, the destruction of religious and cultural icons such as the tomb of the prophet Jonah, and the widely publicised beheadings of Western aid workers and journalists all provoke terror among the Iraqi populace and the world at large.
- Propaganda and information war: ISIS' social media campaigns highlight clear and careful messaging. Each tweet, video, and blog post aiming to glorify and recruit for the ISIS cause. High quality films in multiple languages bring the conflict from the battlefields of Iraq to the viewer's screen. This has clearly contributed to ISIS' success in recruiting of foreign fighters.
- Criminal activity: ISIS employs a variety of methods to fund its endeavours as it boasts a diverse investment portfolio: black market sales of oil, wheat, and antiquities; ransom money; and good old-fashioned extortion. While donations account for a portion of their funds, ISIS' criminal enterprises ensure that the group is financially solvent.
- Disregard for international law: ISIS has no respect of humanitarian and legal norms. Based on their extreme interpretations of Sharia law, ISIS inflicts violence against women and minorities, including barbaric punishments such as stoning and amputations etc. threatening.

b. The "*Russian*" Model

The culminating point of the hybrid war discussion has been the debate surrounding the "*Russian*" model as used in the Ukraine, with Russia's aggressive actions there since 2014. The Russian military's general staff has been preparing for Ukraine-type hybrid operations for years building on the "Gerasimov doctrine" – named after the Chief of the General Staff of the Armed Forces of Russia. This doctrine focusses primarily on the part played by interagency forces and components and on the crucial role of all manner of information warfare – kinetic and/or non-kinetic, blended in such a way as to confuse, surprise, immobilise and eventually defeat an

[18] Alex Deep, *"Hybrid War: Old Concept, New Techniques."* Small Wars Journal. March 2, 2015. http://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques
[19] Scott Jasper and Scott Moreland The Islamic State is a Hybrid Threat: Why Does That Matter? Small Wars Journal. Dec 2, 2014. http://smallwarsjournal.com/printpdf/18345

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

opponent without even needing to openly commit regular forces to that end.[20] Many elements of this doctrine are not new. Others, such as the use of cyber weapons or the use of social networks for propaganda purposes have only become possible due to the digital age. Yet, the core capability comes from the orchestration of all these seemingly small and disconnected pieces within a comprehensive concept.

A key to understanding the new doctrine has become the speech given by General Gerasimov at the annual meeting of the Russian Academy of Military Science in January 2013 and it is, thus, particularly worthy of being studied in depth. Here follows a brief excerpt: *"In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared, and, having begun, proceed according to an unfamiliar template. The experience of military conflicts … confirm that a perfectly thriving state can, in a matter of months and even days, be transformed into an area of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war …In terms of the scale of casualties and destruction – the catastrophic social, economic, and political consequences – such new-type conflicts are comparable with the consequences of any real war. … The very "rules of war" have changed. The role of non-military means of achieving political strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."*[21]

Gerasimov in fact observed that these methods tactics have been used by the United States for decades; he stated that Russia would therefore now fight in the same way. Russia, as per this doctrine, perceives an asymmetry of military capabilities and economic strength between herself and the United States including its Western allies. In view of this, the need is felt to be more aggressive and smarter than its opponents in fighting this new kind of war.

Long before the Ukraine crisis there were manoeuvres in several military districts. Particularly the Russian military's *ZAPAD 2013* exercise[22] involving more than 75,000 troops proved to be a form of rehearsal for parts of the Ukraine campaign. Consequently, the Russian military played a well-trained and well-orchestrated role.

In mid-February 2015 there were approx. 15,000 Russian troops on Ukrainian territory backing up approx. 30,000 illegally armed formations of separatists in eastern Ukraine. These units were well equipped with superior body armour as well as body-armour-piercing ammunition which can easily defeat normal infantry when combined with night vision and snipers. Artillery and multiple-rocket launchers utilise advanced munitions, which in combination with RPV/UAV target acquisition caused 85% of all Ukrainian casualties and can take battalion size units out of action in one strike. The modern Russian dense and overlapping air defence system drove opponent Close Air Support and Attack Helicopters off the battlefield, particularly due to the fact that sophisticated ECM and air defence suppression was not available to the Ukrainian troops. UAVs, drones & RPVs ensure front-end operational intelligence and tactical targeting. Electronic warfare techniques- including high-power microwave systems – jammed not only the communications and reconnaissance assets of the Ukrainian Armed Forces but also disabled the surveillance feed of unmanned aerial vehicles operated by Organisation for Security and Co-operation in Europe (OSCE) monitoring teams . At one point during the Ukrainian crisis Russia had more than 55,000 troops lined up on the Ukrainian border. But when it came to

[20] Dave Johnson, "Russia's Approach to conflict - Implications for NATO's Deterrence and Defence," Research Paper 111, NATO Defense College, April 2015.
[21] Gerasimov, Valery. "*The Value of Science Prediction*". In: Military-Industrial Courier. Moscow. 2013. http://vpk-news.ru/sites/default/files/pdf/VPK_08_476.pdf
[22] Pauli Järvenpää. "*Zapad-2013, A View From Helsinki".* Washington DC August 2014. http://www.jamestown.org/uploads/media/Zapad_2013_View_From_Helsinki_-_Full.pdf

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

sowing instability in the Ukraine, conventional forces were not the ones used, but rather unorthodox and varied techniques.

What defines Russia's course of action in the Ukraine is the systematic use of varied means that, all together, has the capacity to undermine and seriously weaken their adversary without crossing established thresholds that would trigger a military response. The Russian military hierarchy has been remarkably open in describing its use of hybrid warfare in the Ukraine. While the rebels directly engaged the Ukrainian army in the Donbas, the Russian military engaged in training exercises just inside Russian territory. These exercises include the use of space, missile and nuclear forces, Special Forces and conventional military units, psychological operations teams and political operatives. All branches of Russia's military and security services were pulled in, as well as the civilian leadership.

The non-military instruments of Russia's hybrid concept work impressively well, notably via[23]:

- Investments in key sectors of European economies;
- The use of Russian investments, trade, and capital to bribe and influence key economic and political elites;
- Buying up media to support anti-integration and pro-Russian political parties;
- Arms sales to gain influence over military decision-making;
- Large-scale intelligence penetration of European organisations;
- Forging of links between Russian organised crime and local criminal elements;
- Establishment of ties among religious institutions, exploitation of unresolved ethnic tensions and campaigns for "minority rights";
- Large-scale support for Russian information outlets abroad; and
- Massive coordinated cyber strikes on selected targets.

Although the specific features of Crimea and the Donbas may not be replicable elsewhere, it becomes clear that this repertoire of instruments allows Russia enormous flexibility in orchestrating relentless hybrid attacks wherever they may be. Russia has learnt how to "*tailor*" forces and non-military instruments to the requirements of the theatre or targets, e.g. targeting British finance in the City of London, French arms sales, German oil, gas, and electricity or Balkan media. And other actors may learn from them.

Particularly remarkable has been Russia's on-going propaganda element of their 'hybrid' war in order to silence independent voices – an aspect which has received much less attention than their (para)military engagements. Kremlin controlled radio, television and the printed press have become dominant players in Russian life, greatly shaping public opinion especially to reinforce resentment of the West. The Sputnik News Channel, which is used to spread Russian propaganda, has begun recruiting Estonian journalists. Russia Today has replaced the state owned RIA Novosti along with the Kremlin's international radio station, Voice of Russia. Russian media is once again owned by the state and all communications are shaped according to President Putin's political agenda through editors and journalists loyal to the Kremlin.

Apart from controlling news services throughout Russia the Kremlin has also recognised the power of social media to win hearts and minds of young Russians. VK, which was originally named VKontake, is the largest

[23] Stephen Blank. "*Russia, Hybrid War and the evolution of Europe*". Second Line of Defense. 2015-02-14. http://www.sldinfo.com/russia-hybrid-war-and-the-evolution-of-europe/

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Russian social network and is available in 17 languages. Launched in 2003, by 2006 it had a revenue in excess of $ US 121.4 million and by 2012 had over 209 million users. Once owned by Maluru.org, this popular social network for users living in Eastern Europe is now owned and controlled by the Kremlin. Many of the account holders who regularly contribute to these pages are either fighting in the Ukraine or have recently returned from the conflict. So-called 'Freedom Fighters' discuss their combat experiences and post graphic images of their activities. Since the start of the proxy war against the Ukraine there has been a dramatic increase in the number of account holders living in Russia.

4. Lessons to Learn

Up to this point, all involved nations and actors strive with significant difficulty when it comes to effectively fighting hybrid threats. It may be observed with both the models of ISIS and Russia that the exploitation of modern information technology, including modelling and simulation, has enhanced the learning cycle of hybrid opponents, improving their ability to transfer lessons and techniques learnt both inside a specific theatre of conflict, as well as from one theatre to the next. To successfully meet these hybrid challenges will require that decision-makers and first responders, societies and media learn faster and better than their opponents engaging hybrid warfare.

The art of hybrid warfare is not found in front line manoeuvres, but rather in the zones of security that either not black-and-white: grey is the new colour of war. In the past, irregular tactics and protracted forms of conflict have mostly been marked as tactics of the weak, employed by non-state actors who do not have the means to do better. Today and in the future, opponents may exploit hybrid opportunities because of their effectiveness. Unlike conventional warfare, the "*centre of gravity*" in hybrid warfare is the individual. The adversary tries to influence key policy- and decision makers by combining kinetic operations with subversive efforts. The aggressor often resorts to clandestine actions to avoid attribution or retribution. It is a type of warfare particularly dangerous to multi-ethnic societies.

There are lessons available[24]:

- Mixed ethnic societies are particularly susceptible to mass and social media manipulation.
- Prior to conflict, subtle economic influence and the practice of corruption serve to establish leverage and achieve compromises from key politicians and security organisations.
- Political agents, volunteers and mercenaries provide a variety of low visibility insertion, sabotage, training and advisory options.
- Terrorist type techniques include building seizures, infrastructure attack, intimidation of police, cyber disruption, political assassination, kidnapping of children, hostage taking, torture and mutilation.
- Low-intensity conflicts that escalate rapidly to high-intensity warfare unveil unpreparedness of police, border guards, security units and even SOF teams to deal with these challenges.
- A variety of subtle and direct nuclear threats, including nuclear alerts and fly-bys reopen the nuclear debate.

[24] Dr. Phillip A. Karber. "*Russia´s Hybrid War Campaign, Implications for Ukraine & Beyond*". Washington. CSIS 1o March 2015. http://fortunascorner.com/wp-content/uploads/2015/03/hybridwarfarebrief.pdf

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Hybrid warfare will be a defining feature of the future security environment. This should widen the perspective of decision-makers and their interest to cooperate with relevant partners. Success in hybrid war requires that political, military and civil echelon leaders be equipped with decision-making and cognitive skills that enable them to recognise and/or quickly adapt to the unknown. Organisational learning and adaptation is of importance, as is investment in training and education. To this end nations and defence organisations need to make far better use of lessons identified and learnt in recent campaigns. These lessons should be incorporated into a programme in which future capabilities to meet hybrid challenges are developed via a series of linked exercises and security education initiatives. Exercise and training programmes need to be adapted to reflect recent developments in and reactions to hybrid warfare.

Clearly prevention is vital. Early indicators should be established to enable more agile responses to hybrid threats, especially in the early phase of the conflict cycle. To counter complex hybrid challenges, nations – individually and within an allied framework – should firstly:

- Determine how to best promote democracy, human rights, and the rule of law.
- Emphasise transparency and due process across all elements of society.
- Strengthen cooperative regional approaches that build support for like-minded partners.

Hybrid warfare seeks to exploit the seams between collective defence. In view of this, crisis management, cooperative security, military responsiveness and agility need to be enhanced.

5. A time for Partnerships?

The nature of hybrid warfare is such that it is difficult to know whether we are still in times of peace, or already at war. Unpredictability has become a weapon. Up to now approaches countering hybrid warfare have been centred on rapid military responses. This approach has weaknesses. Particularly in defence alliances, when member states need to agree on the source of and response to conflict, the debate of which constitutes a significant barrier to rapid collective action.

Either way, hard power may prove insufficient to counter hybrid threats. The military instrument per se plays an important but nonetheless limited role. The challenge is to orchestrate the balanced employment of all of the instruments of power: diplomacy, information, military, and economic (DIME). This highlights the need for a broad-based approach, using:

- Rapid deployment and power projection.
- Special Forces and cyber operations.
- Intelligence operations and police investigations.
- Financial and economic measures.
- Information and social media campaigns.

Such a broad spectrum of instruments cannot come from a single source, from a single nation or a single organisation. In other words, while the colour of hybrid warfare is grey, meeting hybrid challenges requires a colourful spectrum of partner capabilities. Successfully meeting hybrid challenges requires trusted, capable and interoperable partners. Consequently, within any hybrid warfare strategy specific consideration must be given to the role of partner nations and organisations, regarding how best to enhance not only one's own resiliency but also that of Allies and Partners. Particular focus should be put on the protection of critical

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

national information and infrastructures as well as on consequence management. A useful first-step could be an analysis of key vulnerabilities to better understand how individual nations could be undermined by hybrid warfare. Such an analysis would include a better understanding of:

- How minorities are susceptible to manipulation.
- How vulnerable media are to external saturation.
- How the lack of a binding national narrative could be exploited.
- How electorates could be alienated from leadership during a hybrid warfare-inspired crisis, particularly through elite corruption.

Hybrid threats and risks are likely to become increasingly relevant on a global scale as they reflect a world pervaded by conflict. Asia provides first examples. The Japanese in particular have concerns about Chinese behaviour in terms of utilising 'grey-zone' contingencies regarding the Senkaku/Diaoyu Islands.[25] Another issue of concern is whether North Korea will become a close ally of Russia, perhaps even playing China and Russia against each other. As Moscow loses traction with the international community it aims to antagonise the U.S. as payback for what it sees as meddling in Russia's backyard over the Ukraine. North Korea and Russia have already announced that they will be holding joint military drills later in 2015. Their growing closeness is a likely scenario. The prospects for increased hybrid challenges in the region are considerable and the danger of unmanageable escalation has increased.[26]

Hybrid warfare presents considerable institutional challenges to both domestic defence capabilities and wider security alliances. NATO for example will need to strengthen co-operation with international organisations and partners such as the European Union. The NATO Summit in Wales last year has already acknowledged the European Union as a strategic partner. The common threat of hybrid warfare within the Euro-Atlantic area presents a solid opportunity to develop this partnership. Alexander Vershbow, Deputy Secretary General of NATO stated recently: "*NATO and the European Union each have distinct hard and soft power tools. Our challenge is to bring them together so that we complement each other, and reinforce the essential measures taken by our member states*."[27] NATO and the EU could create an effective institutional tandem that has a wide range of diplomatic, information, military and economical instruments at its disposal. Further steps aim at building the capacity of other arms of government, such as interior ministries and police forces, to counter unconventional attacks, including propaganda campaigns, cyber assaults or home-grown separatist militias.

Both NATO and the European Union will need to engage with strategic neighbours to bolster their security and capacities. Brazil and the European Union entertain a strategic partnership – a strategic partnership in political, economic, social and cultural terms. Brazil is a trusted, likeminded partner with which the European Union shares fundamental values as well as many common interests. As the next EU-Brazil summit will take place in autumn 2015, hybrid challenges – including cyber – will most certainly be discussed. There is already agreement *"to intensify EU-Brazil relations, strengthening political dialogue, deepening cooperation and encouraging all actors to make full use of the ample opportunities offered by our broad and diverse partnership."*[28] At the

[25] Prashanth Parameswaran. "Are We Prepared for 'Hybrid Warfare'?" The Diplomat. February 13, 2015. http://thediplomat.com/2015/02/are-we-prepared-for-hybrid-warfare/
[26] The Hague Centre for Strategic Studies. "Assessing Assertions of Assertiveness: The Chinese and Russian Cases." June 2014. http://www.hcss.nl/reports/assessing-assertions-of-assertiveness-the-chinese-and-russian-cases/145/
[27] Alexander Vershbow, "ESDP and NATO: better cooperation in view of the new security challenges". Speech by NATO Deputy Secretary General Ambassador Alexander Vershbow at the Interparliamentary Conference on CFSP/CSDP. Riga, Latvia. 5 March 2015. http://www.nato.int/cps/en/natohq/opinions_117919.htm
[28] Press Release, Meeting of the High Representative/Vice-president Federica Mogherini and Minister of Foreign Affairs of

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

recent EU-CELAC summit in Brussels, where Leaders from the EU and the Latin American and Caribbean Countries met, Federica Mogherini, High Representative of the European Union for Foreign Affairs and Security Policy, made a valid point: *"We share a lot of past, but we also share the challenges of today and shaping the future for next generations."*[29] In the spirit of that consideration, future hybrid challenges may find Brazil and Europe as close, capable and resilient partners.

***

Remarks: Opinions expressed in this contribution are those of the author.

This book contribution was originally drafted for the Brazil Office of the Konrad Adenauer Foundation on the occasion of the *XII. Forte de Copacabana Conference* in Rio de Janeiro on October 8, 2015.

About the Author of this Issue

Ralph D. Thiele is Chairman of the Political-Military Society (pmg), Berlin, Germany and CEO at StratByrd Consulting. In 40 years of politico-military service, Colonel (ret.) Thiele has gained broad political, technological, academic and military expertise. He has been directly involved in numerous national and NATO strategic issues while serving as executive officer to the Bundeswehr Vice Chief of Defence Staff, Military Assistant to the Supreme Allied Commander Europe, in the Planning and Policy Staff of the German Minister of Defence, as Chief of Staff of the NATO Defense College, as Commander of the Bundeswehr Transformation Centre and as Director of Faculty at the German General Staff and Command College in Hamburg.

He has published numerous books and articles and is lecturing widely in Europe, Asia (Beijing, Seoul, Tokyo, and Ulaanbaatar) in the U.S. and Brazil on current comprehensive security affairs, cyber security, border security, maritime domain security, protection of critical infrastructure and defence and also historical issues.

Ralph D. Thiele is a member of the German Atlantic Association and member of the Defence Science Board to the Austrian Minister of Defence.

Ralph D. Thiele

Brazil, Mauro Vieira on 9 June 2015, in the margins of the EU-CELAC summit. Brussels. http://eeas.europa.eu/statements-eeas/2015/150609_02_en.htm

[29] European Union External Action, „*EU and Latin American and Caribbean leaders agree to deepen their partnership*", Brussels 12 June 2015, http://eeas.europa.eu/top_stories/2015/120615_eu-celac_en.htm

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de