Crisis in Ukraine – The Emergence of Hybrid Warfare

Ralph D. Thiele

May 2015

Abstract

While traditional combat still remains a possibility, it will no longer be the primary means to victory on the battlefield of the 21st century. Hybrid challenges have become reality. Hybrid warfare will be a defining feature of the future security environment. The "*Russian*" model of hybrid war as shown in the Ukraine has unveiled three stages:

- Destabilizing a country via inspiring domestic conflict;
- Causing state collapse via ruining economy and destroying infrastructure;
- Replacing local political leadership with own operatives as "*invited saviour*".

It appears to be achieving Moscow's desired results. In between the prospects for increased hybrid challenges in Asia have become considerable. This should widen Asian and European interest to cooperate in particular via adopting respective security concepts and instruments of power and via networking global knowledge of relevance to meeting hybrid threats.

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. A Black Swan has emerged

„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."[1] These opening sentences of the European Security Strategy of 2003 have become history. A black swan has emerged. The crisis in Ukraine has altered the security status quo. Suddenly, the rivalry between East and West is back.

When on Sunday March 2, 2014, in the Crimea soldiers without insignia – whom Ukrainians referred to as 'little green men' – began to occupy important buildings, including barracks and town halls NATO ambassadors of the 28 Member States in Brussels would sit for hours and ask themselves: Who are these *"green men"* setting up roadblocks on the Ukrainian peninsula? What is happening to the Russian military bases? What is happening in the Crimea? The smoke disappeared. The *"green men"* turned out to be Russian soldiers. Vladimir Putin announced before Parliament in Moscow the return of the Crimea to the homeland.

The Russian general staff has been preparing for Ukraine-type hybrid operations for years. Long before the Ukraine crisis there were manoeuvres in several military districts. Particularly the Russian military's *ZAPAD 2013* exercise[2] involving more than 75,000 troops proved to be a kind of rehearsal for parts of the Ukraine campaign. Consequently, the Russian military played its 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 and body armour piercing ammunition, which can easily defeat normal infantry when combined with night vision and snipers. Artillery and multiple-rocket launchers utilize 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.

Russian modern overlapping dense air defence drove opponent Close Air Support and Attack Helicopters off the battlefield, particularly as sophisticated ECM and air defence suppression was not available for the Ukrainian troops. UAVs, drones & RPVs ensure front-end operational intelligence and tactical targeting. Electronic warfare means – including high-power microwave systems – jammed not only the communications and reconnaissance assets of the Ukrainian armed forces but to also disabled the surveillance unmanned aerial vehicles operated by monitoring teams from the Organisation for Security and Co-operation in Europe (OSCE).

Former NATO Secretary General, Anders Fogh Ramussen sees Russia engaged in a hybrid war and has warned that "*Russia has adopted this approach and it is a mix of very well-known conventional warfare, and new, more sophisticated propaganda and disinformation campaigns including efforts to influence public opinion through financial links with political parties within NATO and engagement in NGO's…"*[3]

Russia's hybrid campaign in the Ukraine appears to be achieving Moscow's desired results.[4] Flooding the region with illegal weapons, using mercenaries to destroy regional infrastructure, weakening local economy, blocking

[1] European Security Strategy, Brussels 2003
[2] 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 (Accessed: 17 May 2015)
[3] Damien Sharkov. Russia Engaging in 'Hybrid War' With Europe, Says Former Nato Chief. Newsweek. / APRIL 15, 2015 8:01 AM ED http://www.newsweek.com/2015/04/24/former-nato-chief-says-europe-hybrid-war-putin-322293.html
[4] Reuben F Johnson: Russia's hybrid war in Ukraine 'is working', - IHS Jane's Defence Weekly, Kiev, 26 February 2015

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

state functions, in particular law enforcement, justice, social welfare, causing a refugee crisis, exploiting social media & information warfare and introducing own peace keeping forces proved to be effective. The core message that has come along with 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.[5]

2. Hybrid War

"Hybrid warfare has been defined as a combination of conventional, irregular, and asymmetric means, including the persistent manipulation of political and ideological conflict, and can include the combination of special operations and conventional military forces; intelligence agents; political provocateurs; media representatives; economic intimidation; cyber attacks; and proxies and surrogates, para-militaries, terrorist, and criminal elements."[6] Hybrid war involves multi-layered efforts designed to destabilise a functioning state and polarize its society.

Hybrid war appears vaguely connected. In fact, 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 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. Hybrid tactics reflect an order behind the spectrum of tools used. That makes it incumbent upon political leaders and strategic thinkers to fit such activities accurately within the political objectives discussed by Carl von Clausewitz, who underlined that war was an extension of politics by other means. In thinking through the on-going hybrid campaigns, it is important to understand that "*hybrid*" refers to the means of war opposed to the principles, goals, or nature.

Clausewitz sees war as a chameleon and such a chameleon is hybrid war. It is a potent, complex variation of warfare. What is making it so dangerous is the rapidity with which one can escalate a conflict in the digital world. Consequently, a broad politico-military debate has started, whether a new form of warfare appears to have been born.

a. The "ISIS" model

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 on which kind of hybrid challenges to focus on. Within NATO and the European Union, Northern members such as the Baltic States, Poland and German think with view to hybrid warfare immediately of the "Russian" model. Whereas Italians, French, Greeks or Spanish see the "ISIS" model at least as threatening.

A decade ago ISIS emerged as a small Iraqi subgroup of Al Qaeda specialized in suicide bombings. Today ISIS has conquered cities and wide territories in both Syria and Iraq. The movement draws its strength from Sunni Arab communities opposed to the Shiite-led government in Baghdad and the regime in Damascus. Former U.S. defence secretary Chuck Hagel called ISIS "*as sophisticated and well funded as any group that we have seen … beyond anything we have seen*" as it includes former military officers who can fly helicopters, spot artillery, and

[5] Jordan Bravin. Getting behind Hybrid Warfare. CICERO Magazine. July 17, 2014. http://ciceromagazine.com/essays/getting-behind-hybrid-warfare/
[6] Robert A. Newson, Counter-Unconventional Warfare Is the Way of the Future. How Can We Get There? In: Janine Davidson Blogspot: Defense in Depth. October 23, 2014. http://blogs.cfr.org/davidson/2014/10/23/counter-unconventional-warfare-is-the-way-of-the-future-how-can-we-get-there/
(Accessed: 17 May 2015)

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

manoeuvre in battle. ISIS is increasingly a hybrid organization, on the model of Hezbollah – part terrorist network, part guerrilla army, part proto-state.[7]

In fact, Hezbollah – the mother of hybrid battle – clearly demonstrated the ability of non-state actors to study and deconstruct the vulnerabilities of Western-style militaries and devise appropriate countermeasures in the war with Israel in 2006. Hezbollah effectively fused militia forces with highly trained fighters and anti tank guided missile teams. It mastered the art of light infantry tactics against heavy mechanized forces. It even demonstrated its ability to hit Israeli naval assets. Also during subsequent operations such as Operation Cast Lead in 2008 and Operation Pillar of Defence in 2012, Gaza groups successfully run a hybrid warfare-type strategy.

With the Syrian Civil War another hybrid warfare case showed up. But, not only has the armed opposition been conducting hybrid concepts. Also the Baathist dictatorship has shaped its violent strategy by utilizing a broad spectrum of hybrid warfare means. A further scene of hybrid warfare has been the Sahel region. A key characteristic of the violent groups in the Sahel region is the fluidity of their leadership and organisational structures. Interpersonal relationships are holding these groups together. Particular complex is the mixed pursuit of the key actors' political agenda with criminal activities. In Somalia, al-shabaab derives a large part of its income from widespread extortion and commission on seizures affected by pirates. In Mauritania and Mali, the battalion led by Mokhtar Belmokhtar has largely financed its activities through cigarette, cocaine and weapons smuggling. In between, hostage taking has become a lucrative activity.

Particular in the Sahel region hybrid war blends the lethality of state conflict with the fanatical and protracted fervour of irregular warfare. In such conflicts, future adversaries such as states, state-sponsored groups, or self-funded actors exploit access to modern military capabilities, including encrypted command systems, man-portable air-to-surface missiles, and other modern lethal systems, as well as promote protracted insurgencies that employ ambushes, improvised explosive devices (IEDs), and coercive assassinations. This could include states blending high-tech capabilities such as anti satellite weapons with terrorism and cyber warfare directed against financial targets. The more non-state actors' access to game changer weapons increases, the more likely it is that hybrid conflicts will spread.

And in fact, ISIS has already arrived at the Mediterranean shores opposing the European Union. In Libya between 1,000 and 3,000 militants are now fighting for the Islamic State cause. The new ISIS affiliates in Libya are the IS Barqa Province, IS Fezzan Province and IS Tripoli. Since the start of 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.[8]

Scott Jasper and Scott Moreland conclude in their article on the Islamic State[9] with the observation that "*... the Islamic State is a formidable, but not unassailable hybrid threat*..." and identify six characteristics of hybrid threats:

- Blended tactics: ISIS forces include traditional military units as well as smaller, semi-autonomous cells, combining both conventional and guerilla warfare tactics. They possess a wide array of weaponry, from improvised explosive devices (IEDs) and mines to rocket-propelled grenades (RPGs), drones, and

[7] Steve Coll. In Search of a Strategy. The New Yorker. September 8, 2014 issue.
http://www.newyorker.com/magazine/2014/09/08 (Access: 17 May 2015)
[8] State Department. ISIS capitalizes on Libya security vacuum, establishes 'legitimate foothold'. rt. March 21, 2015.
http://rt.com/usa/242809-isis-threat-libya-security/ (Accessed: 17 May 2ß15)
[9] Scott Jasper and Scott Moreland The Islamic State is a Hybrid Threat: Why Does That Matter?

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

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 publicized 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 endeavors 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.

b. The "*Russian*" model

The "*Russian*" model of hybrid war is different. Three stages have been identified[10]:

- Destabilizing a country via inspiring domestic conflict;
- Causing state collapse via ruining economy and destroying infrastructure;
- Replacing local political leadership with own operatives as "*invited saviour*".

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 sowing instability in Ukraine, it was not conventional forces that were used, but rather unorthodox and varied techniques. The Russian military hierarchy has been remarkably open in describing how it has been applying hybrid warfare in the Ukraine. While the rebels directly engaged the Ukrainian army in the Donbass, 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, and psychological operations teams and political operatives. All branches of Russia military and security services were pulled in, as well as the civilian leadership.

It is amazing how well these non-military instruments of Russia's hybrid concept have been brought to fruition[11]:

Small Wars Journal. Dec 2 2014. http://smallwarsjournal.com/printpdf/18345 (Accessed: 17 May 2ß15)
[10] Karber, Dr. Phillip A. Russia´s Hybrid War Campaign, Implications for Ukraine & Beyond, Washington CSIS 1o March 2015, http://fortunascorner.com/wp-content/uploads/2015/03/hybridwarfarebrief.pdf (Accessed: 17 May 2ß15)
[11] 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/ (Accessed: 17 May 2015)

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

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

Although the specific features of Crimea and the Donbass may not be replicable elsewhere, it becomes clear that this repertoire of instruments allows Russia in general enormous flexibility in orchestrating relentless hybrid attacks. Russia has learned 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.

As the world's media concentrates on Russia's conventional and nuclear military capabilities, Russia's on-going propaganda element of their 'Hybrid' war in order to silence independent voices has received less focus. Kremlin controlled radio, television and the printed press have become dominant players in Russian life as they greatly shape public opinion and are used 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 Putin's political agenda through editors and journalists loyal to the Kremlin.

Apart from controlling news services throughout Russia the Kremlin has also recognize the power of social media to win hearts and minds of young Russians. VK, which was originally named VKontakte, is the largest 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 Ukraine or have recently returned from the conflict. 'Freedom Fighters' discuss their combat experiences in Ukraine and post graphic images of their activities. Since the start of the Proxy war against Ukraine there has been a dramatic increase in the number of account holders living in Russia.

The Russian controlled media show Putin as a masculine, aggressive, clear-language, strong leader. Related imagery, his deliberate poses and photo-shoots can be found on VT, Facebook, Twitter and other social media networks and go down well with his supporters. They go alongside comments about his strength of leadership and capabilities of restoring the Russian Empire.

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

Among the key lessons learned to this point are[12]:

- Mixed ethnic societies are particularly susceptible to mass and social media manipulation.
- Prior to conflict, subtle economic influence and the promotion of corruption serve to establish leverage as well as compromise of key politicians and security organisations.
- Political agents, volunteers and mercenaries provide a variety of low visible inserting, 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.

Many elements of the "*Russian*" model are not new. Others, i.e. the use of cyber weapons or the use of social networks for propaganda purposes have only become possible with the Internet. Yet, the core capability comes from the orchestration of all small pieces within a comprehensive concept.

To understand the "*Russian*" model one needs to look both at the small pieces and at the overall concept to understand the character and magnitude of the aggressiveness that has come along with it. A key to understanding has become the speech held by General Valery Gerasimov, Chief of the General Staff of the Russian Federation at the annual meeting of the Russian Academy of Military Science in January 2013.[13]

"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.

The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other non-military measures – applied in coordination with the protest potential of the population.

All this is supplemented by military means of a concealed character, including carrying out actions of informational conflict and the actions of special operations forces. The open use of forces – often under the guise of peacekeeping and crisis regulation – is resorted to only at a certain stage, primarily for the achievement of final success in the conflict.

[12] Karber, Dr. Phillip A. Russia´s Hybrid War Campaign, Implications for Ukraine & Beyond. Washington CSIS 1o March 2015, http://fortunascorner.com/wp-content/uploads/2015/03/hybridwarfarebrief.pdf (Accessed: 17 May 2015)
[13] This is a rather lengthy quote, but very telling. See 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

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

These days, together with traditional devices, nonstandard ones are being developed. The role of mobile, mixed-type groups of forces, acting in a single intelligence-information space because of the use of the new possibilities of command-and-control-systems has been strengthened. Military actions are becoming more dynamic, active, and fruitful. Tactical and operational pauses that the enemy could exploit are disappearing. New information technologies have enabled significant reductions in the spatial, temporal, and informational gaps between forces and control organs. Frontal engagements of large formations of forces at the strategic and operational levels are gradually becoming a thing of the past. Long-distance, contactless actions against the enemy are becoming the main means of achieving combat and operational goals.

The defeat of the enemy´s objects is conducted throughout the entire depth of his territory. The differences between strategic, operational, and tactical levels, as well as between offensive and defensive operations, are being erased. The application of high-precision weaponry is taking on a mass character. Weapons based on new physical principals and automized systems are being actively incorporated into military activity.

Asymmetrical actions have come into widespread use, enabling the nullification of an enemy´s advantages in armed conflict. Among such actions are the use of special operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected…

Another factor influencing the essence of modern means of armoured conflict is the use of modern automated complexes of military equipment and research in the area of artificial intelligence. While today we have flying drones, tomorrow´s battlefields will be filled with walking, crawling, jumping, and flying robots. In the near future it is possible a fully robotized unit will be created, capable of independently conducting military operations."

Gerasimov observed that these methods and such tactics had been used by the United States for decades. Now Russia would fight in the same way. Because of what Russia perceives as an asymmetry of military capabilities and economic strength between herself and the United States including its Western allies, Russia has to be more aggressive and smarter than its opponents in fighting this new kind of war.

3. A chance for NATO and the EU to work together?

Both Russia and IS are exploiting the implied division between the three pillars of NATO's Strategic Concept – realignment of collective defence, crisis management and co-operative security – by destabilising the home political base of Alliance nations upon which NATO defence solidarity is founded. NATO and the EU need to realign initiatives that have not delivered to this point such as Smart Defence, NATO Forces 2020 and the Connected Forces Initiative.[14] Clearly the concept of hybrid warfare needs to be studied carefully and conceptualized. Threats from both strategic directions „East" and „South" need to be dealt with, and there may even be a third one in Asia.

Russia's actions in and around Ukraine have reinforced the notion that the security environment in Europe is becoming increasingly unpredictable. The steady decline of defence budgets appears to have stopped. In response to the conflict in Ukraine, NATO member nations have decided to develop a set of tools to deter and

(Accessed: 17 May 2015)
[14] Julian Lindley-French. Hybrid Warfare: NATO needs a Stoltenberg Doctrine. Blogspot: http://lindleyfrench.blogspot.kr/2015/05/hybrid-warfare-nato-needs-stoltenberg.html
(Accessed: 17 May 2015)

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

defend against adversaries waging hybrid warfare. Up to now the NATO approach countering hybrid warfare has been centred on a rapid military response. This approach has weaknesses that need to be addressed. For example member states need to agree on the source of a conflict. This creates a significant barrier to prompt rapid collective action. And even more important, to counter irregular threats, hard power alone is insufficient.

Consequently, NATO will have to develop a more flexible policy, strive to deter or even counter hybrid adversaries with a wide range of instruments. To realize what are not only the possibilities but also the limits of respective instruments of power is an important requirement for purposeful and effective leadership. As the hybrid scenarios cover a hitherto not known broad spectrum of security challenges, this highlights the need for a broad-based approach, using the full range of hybrid warfare agents as those applied by the other side: rapid deployment and special forces; financial and economic measures; defensive and offensive cyber operations; intelligence operations and police investigations; Information and social media campaigns.

As discussed by Russia in its new doctrine the military instrument per se plays only a limited role. Instead all of the instruments of power are employed: diplomacy, information, military, and economic (DIME). The purpose of using these instruments in this synchronized way is to pressure, influence, and destabilize other countries, i.e. destroying or at least permanently weakening regimes that oppose Russian interests. None of these components is new to Europe, but its societies are more vulnerable than ever before as they are deeply integrated. Everything is connected to everything else: economy, diplomacy, finance, military, intelligence, communications, and cyber space. And everything can be damaged or put out of service via hybrid aggression. It is easy and cheap to launch for external aggressors, but it is costly for the defenders.

The combination and orchestration of different actions creates ambiguity, making an adequate reaction difficult, especially for multinational organizations that operate on the principle of consensus. Undoubtedly, hybrid warfare presents NATO with an institutional challenge. The Alliance will need to strengthen cooperation within the own organisation, but also with international organisations, particularly with the EU. By partnering with the European Union and expanding its set of instruments, the Alliance would be in a much better situation to successfully tackle hybrid threats from all necessary angles with a wide range of both political and military instruments at its disposal. The NATO Summit in Wales has already acknowledged the EU as a strategic partner of the Alliance. And the common threat of hybrid warfare within the Euro-Atlantic area presents a solid opportunity to develop this partnership.

Obviously we need not just to pay attention to conventional weapons and irregular tactics, terrorism and organized crime, but also to *non-violent* actions. These include information operations, economic, financial and subversive political acts. As we look at the scope of hybrid warfare this clearly affects the extent to which various government agencies need to get involved and capable of integrated, networked responses to hybrid challenges to security. Adapting to the threat of 'hybrid warfare' will require governments to invest with view to personnel, training and equipment as well as to concepts of operations in a wider array of capabilities and facilitate the comprehensive interaction between them.

Consequently, the Comprehensive Approach that already has been adopted by NATO and the European Union needs to have a central role in dealing with hybrid challenges as it utilizes all the instruments of power: diplomacy, information, military, and economic. The Comprehensive Approach provides a perspective that explicitly focuses operations on political, military, economic, social, infrastructure, and informational effects by using diplomatic, information, economic and military actions.

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

The core military capability within the Comprehensive Approach is a superior command and control process which – based on a network of governmental and non-governmental expert's knowledge and instruments of power – makes it possible to project national power at an early stage in order to achieve a maximum effect. As a rule, this approach will employ the means best suited for attaining an objective.

With hybrid warfare unpredictability has become a weapon. Are we still in peace, or we are already at war? According to Article 5 of the NATO treaty all Member States can trust in a guaranteed assistance. Each potential aggressor should know: If I attack a country, then I attack the whole alliance. There must be no grey area here. But obviously, grey is the colour of hybrid warfare. For NATO members article 5 marks the threshold of war, the art of an opponent will be to operate below this threshold.

In order to respond to hybrid challenges below the threshold of traditional collective defence first of all Early Warning and Situational Awareness are of key importance. Given the increasing practice of Russian "snap exercises," NATO and the European Union need to increase their situational awareness. Allies and willing partners should continue to work on improving geographical expertise, updating threat assessments, and facilitating closer intelligence cooperation. These assessments should flow into an easy accessible knowledge base and should cover political, economic, and societal influence of hybrid actors that may limit independent action and threaten governmental stability.

Alexander Vershbow, Deputy Secretary General of NATO stated recently: "*Hybrid warfare isn't new. But we have seen it applied in Ukraine with renewed vigour and ingenuity. Hybrid warfare mixes hard and soft power. And so our response should also be multi-faceted. 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.*"[15]

Steps should be taken to help build 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. NATO and the European Union now should develop a sense of urgency to make DIME work. By building up pre-crisis capabilities to deal with hybrid security challenges, nations will be better able to assign responsibility to an aggressor nation. Civilian and military leadership needs to be better prepared for comprehensive interagency actions. There is an obvious need to establish policies and technologies, procedures and a common knowledge base with the ability to practically share data in a timely manner for integrated operations and multinational information sharing.

4. Dealing with "*grey*" – the new colour of war

Irregular tactics and protracted forms of conflict have mostly be marked as tactics of the weak, employed by non state actors who do not have the means to do better. Instead of weakness, future opponents may exploit hybrid opportunities because of their effectiveness. As we have seen, unlike conventional warfare, the "*centre of gravity*" in hybrid warfare is people – a target population. 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. Thus hybrid war is subversive. It is warfare particularly dangerous to multi-ethnic societies. The art of hybrid warfare is not found on front line manoeuvres but rather in

[15] 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
(Access: 17 May 2015)

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

the grey zones of security. Grey is the new colour of war.

It could be observed with ISIS and Russia that exploitation of modern information technology has enhanced the learning cycle of hybrid opponents, improving their ability to transfer lessons learned and techniques within theatres and from one theatre to another. Insurgents have swiftly acquired and effectively employed tactical techniques or adapted novel detonation devices found on the Internet or observed from a different source. To successfully meet hybrid challenges will require that decision-makers and first responders, societies and media modify their mind-sets. Success in hybrid wars requires all political, military and civil echelons leaders with decision-making and cognitive skills that enable them to recognize or quickly adapt to the unknown. It requires smart leaders and smart responders with innovative thinking. Organizational learning and adaptation is of importance, also investment in training and education. Knowledge building and situational awareness need to become focus areas – knowledge and situational awareness about the different political, military, economic, social, infrastructure and information domains within the relevant theatre of operations.

Generally, networking national, regional and global knowledge would provide an ideal base to effectively deal with hybrid situations already from the outset. Integrating knowledge-centric architectures, organizations and people would empower innovative learning and leader development for complex security cooperation on a national, regional and global basis. Networking knowledge would promote interoperability empowering security collaboration with friends and partners around the globe.

Of course, organisations such as NATO or the EU need not to start from scratch. The problem is that information or knowledge often resides isolated in the heads and offices of internal or even external subject matter experts. This information and knowledge is not fused, de-conflicted nor shared. Very often it is not available in an electronically retrievable format. Consequently, there is a need to "*connect*" or "*fuse*" existing information, and the processes that are used to develop it, so that decision-makers of all echelons are presented with a clear holistic understanding, as early as possible in the decision-making process.

A process of permanent knowledge development would cover the full spectrum from collection, analysis, storage and distribution of information that helps to contribute to a common and shared understanding of the operational environment. This very process needs to provide political, civilian and military decision-makers and their staffs exactly with the broad scope of comprehensive understanding they need with view to complex hybrid challenges, including the relationships and interactions between systems and actors. As hybrid conflicts normally have a prehistory they can principally be recognized at an early stage and are – to an extent – predictable. The crucial problem, however, is the correct assessment of a multitude of information and drawing timely conclusions. Knowledge development needs to provide indications and warning of an emerging hybrid security problem.

Networking knowledge would help organizations to better prepare and operate together against a wide variety of challenges. This would strengthen situational awareness, support collaborative planning[16], and, in particular, help to determine the most appropriate responses. It would provide more comprehensive and adaptive perspectives based upon shared trust[17] in contrast to the compartmentalized thinking of today. It would systematically capture knowledge in ways that support leaders and organizations to work

[16] Allied Command Operations Comprehensive Operations Planning Directive COPD. Available at: https://publicintelligence.net/nato-copd/ (Access: 17 May 2015)
[17] Paul T. Bartone and Albert Sciarretta, Human Dimension Issues in Distributed and Virtual Teams. *Small Wars Journal*. Available at: http://smallwarsjournal.com/jrnl/art/human-dimension-issues-in-distributed-and-virtual-teams (Access: 17 May 2015)

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

better together. It would make knowledge persistent to organizations and less reliant on temporary access to subject matter experts. And in particular, it would support improved interoperability between actors across a wide spectrum of tasks using agreed-on information formats. In sum, such a dynamic, collaborative federated network of people, ideas and processes would make knowledge actionable in order to address current and emerging challenges such as hybrid threats.

5. Impacts on Asia

Stephan De Spiegeleire and Eline Chivot have described in their study about the assertiveness of Russia and China[18] – assertiveness, defined broadly as either a rhetorical or behavioural increase in the way a country asserts its power in the international system – that both powers have displayed increasing assertiveness over the past decade, with Chinese assertiveness increasingly more noticeable than Russian. The study highlights a rising Chinese power that is increasingly asserting its military muscle. Over the past decade, China appears to have increased its rhetorical and its factual assertiveness significantly more than Russia has. A second serious finding of the study is that in both countries factual assertiveness has increased more than rhetorical assertiveness.

With China's steep rise in the share of total Asian defence spending in the last five years, and other countries investing largely in maritime and aerial capabilities, it is little wonder that strategists and governments alike have begun thinking seriously about how this might play out amidst the region's "growing militarization". Particularly the Japanese have concerns about 'grey-zone' contingencies with the Senkaku/Diaoyu Islands as one concern.[19] Singapore Minister for Defence Dr Ng Eng Hen stated recently[20] that in face of hybrid warfare the Singapore Armed Forces must restructure to be "*leaner, more potent and versatile*".

Of course, North Korea should be mentioned. What could North Korea learn from the Russian model? Is there perhaps Russian interest in developing North Korean hybrid capabilities? Is it possible that 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 its meddling in Russia's backyard over Ukraine. North Korea and Russia have already announced they will be holding joint military drills later in 2015. Their growing closeness is a likely scenario. As Russia and North Korea grow closer, the U.S. and South Korea will certainly do the same. This comes on top of South Korea's growing need to cope with a series of emerging hybrid national security challenges[21] such as networked terrorism, accelerating cyber attacks, securing long-term energy supplies, and deepening maritime competition in the Indo-Pacific oceans. The prospects for increased hybrid challenges in the region are considerable. The danger of unmanageable escalation has increased.[22]

[18] 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/ (Access: 17 May 2015)
[19] Prashanth Parameswaran. Are We Prepared for 'Hybrid Warfare? The Diplomat, February 13, 2015, http://thediplomat.com/2015/02/are-we-prepared-for-hybrid-warfare/ (Access: 17 May 2015)
[20] Dr Ng Eng Hen, Minister for Defence, Speech at Committee of Supply Debate 2015, 06 Mar 2015, http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2015/05mar15_speech.html#.VQyLpLpSGRg (Access: 17 May 2015)
[21] Lee Chung Min. South Korea's Strategic Thinking on North Korea and Beyond. The ASAN Forum. Special Forum October. 07, 2013. http://www.theasanforum.org/south-koreas-strategic-thinking-on-north-korea-and-beyond/ (Access: 17 May 2015)
[22] 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/

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

In sum, the growing hybrid shape of security challenges has complicated the security situation on a global scale.[23] Hybrid challenges have become reality. Hybrid warfare will be a defining feature of the future security environment. This should widen our perspective and our interest to cooperate in particular via adopting our respective security concepts and instruments of power and via networking global knowledge of relevance to meeting hybrid threats.

***

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

This paper was presented on the occasion of the V. Joint Conference "Crisis Management in Asia and Europe" by the Konrad Adenauer Foundation (KAS) and the Research Institute for National Security Affairs (RINSA) at the Korea National Defense University (KNDU) in Seoul, South Korea on May 6, 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

(Access: 17 May 2015)
[23]Hoffman, Frank G. Hybrid Warfare and Challenges. Joint Force Quarterly, Issue 52, 1st Quarter 2009 / JFQ 34 – 39

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