Hybrid Threats – And how to counter them

Ralph D. Thiele

September 2016

Abstract

Warfare remains a chameleon. Grey has become the new colour of war. Twenty-first century Europe exists in a dynamic strategic environment. Violent aggressions from state- and non-state actors along a broad spectrum of conventional and unconventional lines of operation include diplomatic, information, military and economic instruments of power. Three characteristics stand out:

- The decision of the war/conflict is searched for primarily at a non-military centre of gravity.
- Operating against specific vulnerabilities of the opponent in the shadow of interfaces is challenging traditional lines of order and responsibilities.
- Through combination of different concepts, methods and means „new" forms of warfare and fighting evolve.

As hybrid threats aim to exploit the seams of our economies, societies and networks, situational awareness, crisis management, resilience, military responsiveness and agility need to be enhanced. To better absorb whatever strikes us nations and organizations such as the European Union and NATO need to combine their knowledge, training and education capacities and improve their resilience readiness.

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.

In an ever more complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, bringing major opportunities but also risks, decision-makers in enterprises and 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 decades – in executive positions and possess a wide range of experience in their respective specialist areas.

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. Change

Warfare remains a chameleon. 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. Violent aggressions from state- and non-state actors along a broad spectrum of conventional and unconventional lines of operation include diplomatic, information, military and economic (DIME) dimensions of conflict. Anti-Access, Area Denial (A2/AD) capabilities undermine the freedom of access across all operating domains: air, land, sea, space, and cyberspace.[1] Features driving the development include comprehensive approaches, the mixture of direct and indirect activities, the increasing use of high-tech means and the particular role of information operations. These have been taking war from classical battlefields into grey zones between peace and war.

Particularly the year 2014 has marked a twofold paradigm change in and for Europe.

- Firstly, the Ukrainian-Russian conflict highlighted that the use of military force and violence by state actors to achieve political interests has returned to Europe.
- Secondly, the nature of security challenges has become increasingly hybrid.

Scanning Euro-Atlantic security geographically, in the east and north of Europe, Russia has become – again – the key cause of concern. Two reasons stand out: Russia's aggressive behaviour in Eastern Europe and its militarization of the Arctic.

From the south, Europe faces numerous security challenges as a result of a complex and unstable Middle East and North Africa (MENA). The Islamic State has become a relevant threat, not only by destabilizing the MENA region, but also as it actively recruits and trains foreign fighters who then return through Europe to their countries of origin.

On top, a wave of migrants and refugees keep coming to Europe from MENA. This has evolved to become a serious economic, humanitarian and even political problem. At the same time, it provides opportunities for violent extremist organizations and transnational criminal organizations to take advantage of the crisis to gain access to Europe.

Europe is also contending with further security challenges, to include growing adversary ballistic missile capabilities, the proliferation of weapons of mass destruction (WMD), infectious diseases, cyber-attacks, international and national terrorism, narco-terrorism, and illicit trafficking. Contributing to the complexity of the European security environment are financial challenges. Several European economies are in no good shape, causing overall instability. In Asia Security tensions have been mounting. These may well affect European security and prosperity. On top climate change will likely be a cause for significant disruption.

[1] Luis Simon. *„A European Perspective on Anti-Access/Area Denial and the Third Offset Strategy."* May 3, 2016. War on the Rocks. http://warontherocks.com/2016/05/a-european-perspective-on-anti-accessarea-denial-and-the-third-offset-strategy/

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

2. Hybrid

Hybrid concepts and strategies target vulnerabilities – from cyber-attacks on critical information systems, through the disruption of critical services, such as energy supplies or financial services, to undermining public trust in government institutions or social cohesion. To this end public opinion has become an attractive target.

Clearly, the cyber space constitutes the most extreme form of this vulnerability. Via the cyber space everything is connected to everything else: systems, machines, people. And everything can be damaged, disrupted or put out of service practically from anybody anywhere. Defenders don't know when an attack is being launched, where it will strike and how. The resulting ambiguity makes an adequate reaction difficult, in particular for societies or multinational organizations that operate on the principle of consensus such as the European Union and NATO.

Hybrid warfare is of strategic nature. It is a potent, complex variation of warfare 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. There are three characteristics

- The decision of the war/conflict is searched for primarily at a non-military centres of gravity.
- Traditional lines of order and responsibilities are being challenged through operations against specific vulnerabilities of the opponent in the shadow of interfaces.
- Through combination of different concepts, methods and means „new" forms of warfare and fighting evolve.

Hybrid warfare employs a broad mix of instruments – military force, technology, crime, terrorism, economic and financial pressures, humanitarian and religious means, intelligence, sabotage, disinformation – across the whole spectrum of warfare – traditional, irregular and/or catastrophic. A stealthy approach and disruptive capacity can be expected, executed within the context of a flexible strategy with altering centres of gravity. 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. Non-state actor's involvement includes militias, transnational criminal groups, or terrorist networks. While in the past, irregular tactics and protracted forms of conflict have mostly been marked as tactics of the weak, in future hybrid opponents may exploit them because of their effectiveness. Grey is the new colour of war.

3. Grey

Diving into grey two actors stand out – Russia and the IS. The so called Islamic State has emerged as a hybrid organisation following the initial Hezbollah model – part terrorist network, part guerrilla army, part proto-state entity. Its key features:

- Blended tactics – IS forces include traditional military units as well as smaller, semi-autonomous cells, combining both conventional and guerrilla warfare tactics. They own a wide array of weaponry, from improvised explosive devices and mines to rocket-propelled grenades, drones, and chemical weapons.
- Flexible and adaptable structure – IS quickly absorbs and deploys new resources. Whether new recruits, weaponry, or territory, it constantly incorporates new acquisitions into its strategy and structure.

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

- Terrorism – Through acts of grotesque and exaggerated violence, IS communicates its ideology to a global audience.
- Propaganda and information war – IS' social media campaigns highlight clear and careful messaging. Each tweet, video, and blog post aiming to glorify and recruit for the IS cause.
- Criminal activity – IS 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, IS' criminal enterprises ensure that the group stay financially solvent.
- Disregard for international law – Based on their extreme interpretations of Sharia law, IS inflicts violence against women and minorities, including barbaric punishments such as stoning, amputations etc. There is no respect of humanitarian and legal norms.

Russia has developed its hybrid approach based on intense studies of Western and other successful actor's behaviour and carefully derived a conceptual framework; it trained and exercised this framework and finally commenced operations.[2]

The conceptual framework has been presented already in January 2013 by General Valery Gerasimov, Chief of the General Staff of the Russian Federation, at the annual meeting of the Russian Academy of Military Science:

„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 ...

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.

Weapons based on new physical principals and automated systems are being actively incorporated into military activity. 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.

Asymmetrical actions have come into widespread us e, 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...."[3]

The subsequent Russian action in the Crimea and the Ukraine highlighted the inherent power Russian style hybrid warfare may generate. Russia's Special Forces helped to create a fait accompli before the other side was

[2] Ralph Thiele. „*Crisis in Ukraine – The Emergence of Hybrid Warfare*" ISPSW Strategy Series (2015).
[3] General Valery Gerasimov. „*Speech at the annual meeting of the Russian Academy of Military Science.*" In January 2013. 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

able to understand the overall situation. „*Hybrid warfare*" employed disinformation and deniable forces to maintain maximum ambiguity. Armed Forces helped to create political advantages operating via "*proxy*" non-governmental forces in the form of separatists. Throughout the operations Russia displayed the capacity to undermine and seriously weaken their adversary without crossing established thresholds that would trigger a military response. For example, while the rebels directly engaged the Ukrainian army in the Donbas, the Russian military engaged in training exercises just inside Russian territory. These exercises included 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.

Interestingly the non-military instruments of Russia's hybrid concept showed quite an impressive performance alongside the military instruments. Russian investments, trade, and capital were employed to influence key economic and political elites. Media were involved to support anti-integration and pro-Russian political parties. Forging of links between Russian organised crime and local criminal elements were noticed, also the establishment of ties among religious institutions, exploitation of unresolved ethnic tensions and campaigns for „*minority rights*" and massive coordinated cyber strikes on selected targets.

In sum, from the outset Russia never primarily has sought a decision of this conflict in the military field. The military elements of the Russian hybrid approach served the cover up and protection of subversive, secret service, propaganda or political operations. Using hybrid warfare, the focus on a non-military „*Centre of Gravity*" has become the core of the Russian action towards the Ukraine while optimizing the own performance in the grey zones of security.

4. Gravity

The military concept of a Centre of Gravity[4] in conflicts has been introduced by Carl von Clausewitz in the 1820s. It has evolved as a core element of military doctrines that planners draw on in designing strategies for winning wars despite occasional criticism from the academic front.[5] Carl von Clausewitz described the enemy's CoG as "*the hub of all power and movement, on which everything depends. That is the point against which all our energies should be directed*."[6] The only way that a military can achieve its objectives, according to Clausewitz, is to gather intelligence about the enemy's „*moral and physical character*," including their associated CoG. If the military strategist fails to do so, defeat is almost certain.

The U.S. Joint Staff defines centres of gravity as those „*characteristics, capabilities, or locations from which a military force derives its freedom of action, physical strength, or will to fight*." At the strategic level, they can include a military force, an alliance, national will or public support, a set of critical capabilities or functions, or national strategy itself. At the operational level, they are generally the principal sources of combat power – such as combat forces that are modern, mobile, or armoured – that can ensure, or prevent, accomplishment of the mission.

Interestingly the Australian Defence Force operational planning follows a CoG interpretation of Joseph L. Strange and Richard Iron. They offered a understanding that multiple CoGs might exist and „*may change from phase to phase within a campaign; and that they can change unexpectedly when an enemy shifts the weight of*

[4] CoG
[5] Lawrence Freedman. „*Stop looking for the Centre of Gravity*." War on the Rocks. June 24, 2014. http://warontherocks.com/2014/06/stop-looking-for-the-center-of-gravity/
[6] Carl von Clausewitz, „*On War*", eds./trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), pp. 595-6.

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

its attack, thus uncovering or relying on a previously unforeseen centre of gravity."[7] Once CoGs have been identified, the commander and planning staff determine how to undermine adversary CoGs while protecting friendly CoGs and influencing other actor CoGs in the desired manner.[8]

Clausewitz thought of the CoG effects based, focusing on achieving the collapse of the enemy, how at least first and second-order effects can be achieved. This makes the CoG approach particularly fitting vis-à-vis NATO's and the European Union's Comprehensive Approach to security that is effects based and provides a perspective that explicitly focuses operations on political, military, economic, social, infrastructure, and informational effects by using diplomatic, information, economic and military actions. In combination with the Strange/Iron approach of shifting, multiple CoGs and with the focus on non-military CoGs we are in midst of a conceptual approach dealing with hybrid challenges. The Russian focus on a non-military "*Centre of Gravity*" in the Crimea and the Ukraine highlighted that the military instrument per se may play only a limited role in hybrid warfare. Instead a broad mix of DIME instruments is employed in a synchronized way to achieve the desired political, strategic objectives.

Hybrid warfare appears to be a construct of vaguely connected elements. In reality the pieces are a part of an intended mosaic. Humanitarian convoys followed by conventional war with artillery and tanks in eastern Ukraine, peacekeeping operations in Transnistria, cyber attacks in Estonia, random forays of heavy bombers in the North Sea, submarine games in the Baltic Sea, etc. the diversity of hybrid tactics masks the thoroughly planned order behind the spectrum of tools used and the effects being achieved.

Clausewitz considered the calculation of a CoG a matter of „*strategic judgment*", to be addressed by the top decision-makers. Differing from the situation in the early 19th century today it is still important but not sufficient to focus on military decision-making. Unfortunately, most political decision-makers today have only limited education and training nor experience in CoG related developments and political-strategic options resulting from alternative DIME-employment options. Of course also military leaders have growth potential. Consequently, there is a need to improve and to develop politico-military skills dealing effectively with hybrid threats in a broad and comprehensive format. Civilian and military leadership needs to be better prepared for comprehensive interagency actions.

The good news: the European Union has taken with its Global Strategy presented in June 2016 a significant step in that direction as it aims to *„... deepen its partnership with NATO through coordinated defence capability development, parallel and synchronised exercises, and mutually reinforcing actions to build the capacities of our partners, counter hybrid and cyber threats, and promote maritime security."*[9] NATO shares this approach as Alexander Vershbow, Deputy Secretary General of NATO, pointed out: *„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*."[10]

---

[7] Dr Joseph L. Strange and Colonel Richard Iron, „*Centre of Gravity: What Clausewitz Really Meant*," *Joint Force Quarterly*, 35 (October 2004), pp. 20-27.
[8] Australian Defence Doctrine Publication (ADDP) 5.0, „*Joint Planning*", Edition 2 (Canberra: Department of Defence, February 2014) 2-11, 2-12.
[9] European Union. „*Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy*." Brussels. June 2016. http://europa.eu/globalstrategy/en
[10] 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

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

Intended steps aim 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, the European Union and their member nations now need to develop a sense of urgency to make the 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.

Recently, NATO ambassadors and defence ministers have held simulation and scenario-based exercises to improve their situational awareness and responsiveness vis-à-vis hybrid threats. Obviously, this has been a wake-up call to many. Allies are now more encouraged than ever to map potential vulnerabilities that can arise from Russia's involvement in business, financial, media or energy concerns, for example, and to share the lessons learned from resilience stress testing. These exercises have also highlighted the importance of effective strategic communications to dispel false information, propaganda, lies and myths.

5. Access

A twin brother of the CoG has become the Anti-Access/Area Denial concept – often used by weaker forces against stronger ones, because preventing the enemy from taking and holding a particular area is principally easier than controlling it. Over the past two decades, China, Russia, Iran, and others have developed considerable A2/AD capabilities such as ballistic and cruise missiles, offensive cyber weapons, electronic warfare, and more. These capabilities enable them to threaten freedom of access and presence for third parties across all operating domains: air, land, sea, space, and cyberspace.[11] Russian A2/AD capacities for example in the high north in Murmansk, the Kola Peninsula, in Kaliningrad and in the Black Sea, and recently also in the eastern Mediterranean are potentially impeding and complicating NATO reinforcements and other NATO operations.

In order to mitigate the impending global A2/AD challenge, the U.S. Department of Defense has not only rolled out in late 2014 the „*Defense Innovation Initiative*"[12], but also the corresponding „*Third Offset Strategy*".[13] The objective has been to leverage U.S. advantages in technologies such as big data, stealth, advanced manufacturing, robotics, and directed energy, with a view toward sustaining and advancing U.S. technological – to include military-technological – superiority and offset its shrinking military force structure in a new era of great power competition. Related developments will likely set the pace and evolution of military-technological innovation for decades to come and on a global scale.

Clearly, with the upcoming hybrid threats Europe will find its own A2/AD challenges. Soon the full spectrum of hybrid threats and consequently the whole spectrum of governmental and non-governmental means needs to be addressed. The Warsaw Summit decisions and the European Union Global Strategy point in a promising direction as Europeans must consider the geographical features of their eastern flank and southern neighbourhood, their prosperity interests in Asia, the technological maturity of Europe's A2/AD challengers, and Europe's

[11] Luis Simon. „*A European Perspective on Anti-Access/Area Denial and the Third Offset Strategy*." May 3, 2016. http://warontherocks.com/2016/05/a-european-perspective-on-anti-accessarea-denial-and-the-third-offset-strategy/
[12] Chuck Hagel, „*Secretary of Defense Memo: Defense Innovation Initiative."* 15 November 2014. http://www.defense.gov/Portals/1/Documents/pubs/OSD013411-14.pdf
[13] Deputy Secretary of Defense Bob Work, „*The Third Offset Strategy and its Implications for Partners and Allies*." (speech, Washington, DC, January 28, 2015, Department of Defense. http://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategyand-its-implications-for-partners-and-allies) The Third Offset Strategy has been modelled on two previous endeavours: in the 1950's it leveraged the overwhelming advantage of the United States' nuclear arsenal; the 1970-80's offset focused on the development of precision-guided munitions, stealth, and intelligence, surveillance and reconnaissance (ISR). Both aimed to counter the numerical superiority and improved technical capabilities of Warsaw Pact military forces in 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

own technological capabilities and political limitations, last but not least also cultural backgrounds that shape European societies.[14]

6. Resilience

Vis-à-vis hybrid challenges both – the European Union and NATO – consider resilience an urgent necessity – resilience in terms of the ability to cope, adapt and quickly recover from stress and shocks caused by a disruption, disaster, violence or conflict. Systems and organizations need to be prepared for attacks. Whatever damage is done by the intruder the system needs to continue functioning to the extent possible and recover quickly.

Such requirements are reflected in recent European Union and NATO decisions. In mid 2016 the European Commission and the High Representative adopted a Joint Framework to counter hybrid threats and foster the resilience of the EU, its Member States and partner countries. This approach also includes increasing cooperation with NATO. NATO's Heads of State and Government confirmed at their Warsaw Summit, 8-9 July 2016 their commitment „*to enhance resilience, i.e. to maintain and further develop the Alliance members' individual and collective capacity to resist any form of armed attack. In this context, we are today making a commitment to continue to enhance our resilience against the full spectrum of threats, including hybrid threats, from any direction. Resilience is an essential basis for credible deterrence and defence and effective fulfilment of the Alliance's core tasks*."[15]

Already in the Cold War resilience was designed to anticipate and resolve disruptive challenges to critical functions, and to prevail and fight through direct and indirect attack. Yet, with view to today's increased globalization, highly capable information and communication technology and the evolution of hybrid warfare resilience must be reinvented for the information and knowledge age acknowledging the interconnectedness between the military, civil and private sectors.[16] Allied Command Transformation has identified four mutually interdependent „*focus areas* with view to enhancing resilience:

- Identifying key vulnerabilities and associated risks;
- Synchronizing cross-governmental decision making;
- Building military sustainability and civil preparedness;
- Balancing the allocation of available resources.

These "*focus areas*" serve as a bridge between the presence and future and provide measurable change with view to the core question: How quickly can the "*system*" under attack by whatever combination of disruptive effects be restored to a new and stable state? Each focus area offers a prism for discrete analysis. As a military project, resilience has to be measured in readiness terms with clearly defined training standards. Scenario based simulation exercises for civil-military cooperation in complex emergencies can be a catalyst for learning. Yet, also as a civil-military readiness project resilience needs to be organized with defined standards and a training capacity to achieve it.

[14] Luis Simon. „*A European Perspective on Anti-Access/Area Denial and the Third Offset Strategy.*" May 3, 2016. War on the Rocks. http://warontherocks.com/2016/05/a-european-perspective-on-anti-accessarea-denial-and-the-third-offset-strategy/
[15] NATO Summit Guide. Warsaw, 8-9 July 2016. http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf
[16] HQ SACT. „*Building Resilience Across the Alliance*." Norfolk, 28 January 2016.

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

Building resilience requires protecting critical infrastructure, ensuring undisturbed production and distribution of power, cross-sectoral cooperation between civilian and military actors, safeguarding space infrastructures, protecting against the manipulation of communicable diseases or the contamination of food, soil, air and drinking water, the intentional spreading of animal or plant diseases, withstanding cyber attacks, protecting the financial system and its infrastructure, and last but not least strengthening defence capabilities. Efforts to counter violent extremism and radicalisation are further areas of relevance.

The primary responsibility for building and sustaining resilience lies at the national level. Most national vulnerabilities are country-specific. Early and preventive identification of vulnerabilities is critical. As states, societies and economies become more interdependent, resilience requires joint action of all relevant actors – to include whole-of-society and international partners. It has become essential to work across geographical borders, agency and governmental/non-governmental boundaries.

Shifting – often non-military – centres of gravity highlight that military, civil, and non-governmental organizations share responsibility. As a consequence, new organizations, command concepts, doctrine and performance objectives need to evolve. Shared knowledge helps building trust to prepare and respond together through modular, composable organizations. Multinational strategies will draw upon resources and commitment from levels below and beyond the nation-state. This puts a premium on strong partnerships.

The European Union and NATO are interested to strengthen partner nations' national capacities in the fight against hybrid threats. The European Union Global Strategy clearly states to this end: *„It is in the interests of our citizens to invest in the resilience of states and societies to the east stretching into Central Asia, and to the south down to Central Africa. Under the current EU enlargement policy, a credible accession process grounded in strict and fair conditionality is vital to enhance the resilience of countries in the Western Balkans and of Turkey."*[17] Several partner nations already have fallen victim of hybrid operations. Their experiences and lessons learned can help to better understand the advance and impact of hybrid tactics.

Of particular importance is the cooperation with the private sector.[18] This cooperation will not develop easily. For the Pentagon for example the increasing power and availability of 'dual use' technology is a particular challenge. From data mining and drones to 3D printing and sensor systems, many of the most significant technology developments today have both civilian and military applications. But governments are no longer necessarily attractive partners – these partnerships bring plenty of paperwork, formal and bureaucratic meetings while the financial incentives keep shrinking.

In order to provide a robust foundation supporting EU and NATO Member States in countering hybrid threats collectively existing policies need to be brought together, new approaches need to be added. Situational awareness will have to provide for achieving better protection against hybrid threats. Security risk assessment methodologies need to inform decision makers and promote risk-based policy formulation in areas ranging from aviation security to terrorist financing and money laundering. Indicators of hybrid threats and existing risk assessment mechanisms need to provide for early warning. Intelligence and information sharing has become even more important. Dedicated mechanisms for the exchange of information are required. Prevention, response to crisis and recovery measures need effective procedures to follow.

[17] European Union. *„Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy."* Brussels. June 2016. http://europa.eu/globalstrategy/en
[18] Edward J. Harres. *„Towards a Fourth Offset Strategy."* Small Wars Journal. August 11 2016. http://www.thestrategybridge.com/the-bridge/2016/8/16/a-new-plan-using-complexity-in-the-modern-world

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

7. Range

Up to now the NATO approach countering hybrid warfare has been centred on rapid military responses. Recent approaches aim at a more flexible policy, striving to deter and counter hybrid adversaries with a wide range of instruments. As the hybrid scenarios cover a hitherto not known broad spectrum of security challenges, this underlines the need for a broad-based approach, using the full range of hybrid warfare agents as those have been applied by possible opponents: rapid deployment and special forces; financial and economic measures; defensive and offensive cyber operations; intelligence operations and police investigations; information and social media campaigns. Of course, own vulnerabilities mirror vulnerabilities resident in opponents' networks that could be capitalized.

Rapid identification of a hybrid attack is a precondition for timely decision making in order to early engagement and blocking escalation. Allies and willing partners should continue to work on improving geographical expertise, updating threat assessments, and facilitating closer intelligence cooperation. The assessments should flow into an easy accessible knowledge network covering the political, military, economic, social, infrastructural, and informational disposition of hybrid opponents that may allow to identify centres of gravity and support assessments. To this end, knowledge networking is key to organisational learning and adaptation, to training and education and last but not least to operations – thus making available knowledge actionable.

Exercise and training programmes need to be adapted to reflect recent developments in and reactions to hybrid warfare. Developing a common and shared understanding of threats and vulnerabilities, the tools and mechanisms and improving integrated decision making to effectively deal with them should be captured in a comprehensive concept.[19] Higher level, joint civil-military education, training and exercises should employ best possible applications in next-generation, network-enabled, advanced learning methodologies - output focused, reflecting a systems approach, supporting individual and collective training and fostering knowledge development for interagency and coalition interoperability.

Education needs to broaden the understanding of the exposures security actors face. This is not only a technical matter. More than that it requires developing a comprehensive view across all dimensions, to encourage broad thinking about how to enhance the long-term sustainability of societies, nations, economies and organizations against a backdrop of constant change.

Educational deliverables should address areas NATO has identified already as baseline requirements for resilience readiness such as

- assured continuity of government and critical government services;
- resilient energy supplies;
- ability to deal effectively with the uncontrolled movement of people;
- resilient food and water resources;
- dealing with mass casualties;
- resilient communications systems;
- resilient transportation systems.

[19] HQ SACT. *„Building Resilience Across the Alliance."* Norfolk, 28 January 2016.

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 particular, those areas identified for closer EU–NATO cooperation and coordination are well suited for building resilience readiness: situational awareness, strategic communications, cyber security, crisis prevention and response.

New pathways toward holistic, cross-discipline and divergent thinking must be pursued in order to promote sustainable development and foster resilience. To this end a couple of goals would be productive:

- Support community decision-making in partner nations and in international bodies through modular, composable organizations, where people, ideas, processes and technology can be brought together as needed;
- Pursue „*whole of stakeholders*" approaches and enhanced information sharing;
- Build new learning tools with partners to improve common understanding and shared procedures for rapid, decisive, resilient responses;
- Contribute to significantly enhanced training and readiness capabilities for security and resilience through co-development of a network of regional and functional „*Resilience Readiness Centres*".

Hybrid warfare will be a defining feature of the future security environment. As it aims to exploit the seams of our economies, societies and global networks unpredictability has become a weapon. This dangerous development should widen the perspective of all involved. From the military side General Breedlove, when still in office as Supreme Allied Commander Europe, stated last year: „*What really deters, I think, that is we increase the readiness and responsiveness of the entire NATO force structure*," not just elite quick-reaction units. „*We have to get to these investments, exercises, and training scenarios that raise the responsiveness and readiness of the whole force*."[20] If the civilian side would consider this likewise, the DIME instruments of power would have a fair chance to meet upcoming hybrid challenges.

***

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

This paper was presented on the occasion of the Technical Exploitation Conference and Workshop held by the Norwegian Defence and Research Establishment / Norwegian Naval Special Operations Command on September 13, 2016 in Oslo, Norway.

[20] Sydney J. Freedberg Jr. „*Russians In Syria Building A2/AD 'Bubble' Over Region: Breedlove*". September 28, 2015. http://breakingdefense.com/2015/09/russians-in-syria-building-a2ad-bubble-over-region-breedlove/

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

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

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