Building Resilience Readiness against Hybrid Threats – A Cooperative European Union / NATO Perspective

Ralph D. Thiele

September 2016

Abstract

In global security there are two new kids in town: hybrid threats and resilience. Hybrid warfare is a potent, complex variation of warfare seeking the decision primarily at non-military centres of gravity. Nations need to be better able to resist, recover, and to assign responsibility to an aggressor nation. Resilience requires joint action of all relevant actors. Decision-makers in nations and organizations, in public and private functions need to be cross-linked to overcome modern, hybrid challenges. Consequently, resilience requirements are reflected in recent European Union and NATO decisions. Four mutually reinforcing *„focus areas"* will provide for 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 could serve as a bridge between the presence and future and provide measurable change. „*Resilience Readiness Centres*" could contribute to significantly enhanced higher level, joint civil-military education and training.

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. New Kids in Town

„… a perfectly thriving state can, in a matter of months and even days, be trans-formed 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 … ."[1] This January 2013 statement by General Valery Gerasimov, Chief of the General Staff of the Russian Federation at the annual meeting of the Russian Academy of Military Science has illustrated a paradigm change in global security as there are two new kids in town: hybrid threats and resilience.

The nature of security challenges has become increasingly hybrid. Russia's recent employment of a sophisticated hybrid strategy has challenged Western nations and societies – to include governance and norms – despite their economic, technological, intelligence and military superiority.

Hybrid warfare 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. The decision of the war/conflict is searched for primarily at non-military centres of gravity. Hybrid warfare is not limited to the physical battlefield. Any space available may be engaged. This includes traditional and modern media instruments. Non-state actor's involvement includes militias, transnational criminal groups, or terrorist networks of strategic nature.

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. Hybrid warfare appears to be a construct of vaguely connected elements, but in reality the pieces are a part of an intended mosaic. The diversity of hybrid tactics masks the thoroughly planned order behind the spectrum of tools used and the effects being achieved.

Hybrid actors most likely not just seek to inflict damage or death on regions, nations or organisations. They are rather striving to achieve political goals and objectives. To this end they will attempt to influence their target society's collective mind-set so that their values and principles become challenged, their resolve weakened and consequently political objectives are abandoned or modified.

In the past approaches countering hybrid warfare have been centred on rapid military responses. This will likely be counterproductive in future. Hybrid warfare may have achieved already its strategic objectives before conventional war starts. Once the threshold of military operations is crossed, it may be too late to defend. Consequently, recent approaches aim at a more flexible policy, striving to deter and counter hybrid adversaries with a wide range of instruments while fostering resilience – 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 civil, the private and the security sectors need to continue functioning to the extent possible and recover quickly.

[1] 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

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, civil, private, and military sectors.[2]

2. Strategic Task

Building resilience has become a strategic task. By building up pre-crisis resilience to deal with hybrid security challenges, nations will be better able to resist, recover, and to assign responsibility to an aggressor nation. From the military perspective, nation's and organisation's military and capabilities and capacities build on civil and private resilience for both missions at home or out of area. Critical infrastructure is a particular critical area as the critical infrastructure systems that are the mainstay of nations' economy, security, and health are interdependent – for example, the water supply system of a community is dependent on the pumping stations and they, in turn, are dependent on electric supply.

Cascading failures among these critical infrastructure systems can be eased, or even avoided, when the systems are resilient. Any successful hybrid attack on targets such as energy supply chains, transport could lead to serious economic or even societal disruption. Consequently, an essential element for promoting resilience is to ensure undisturbed production and distribution of power to diversify energy sources, suppliers and routes. The diversification of energy sources and promotion of high safety and security standards will particularly increase resilience of nuclear infrastructures.

Hybrid threats could also target space infrastructures with multi-sectoral consequences. Satellite communications are key assets for crisis management, disaster response, police, border and coastal surveillance. They are at the same time the backbone of large-scale infrastructures, such as transport, space or remotely piloted aircraft systems. Critical infrastructures such as energy, telecommunication, and finance rely on exact timing information to synchronise their networks or timestamp transactions.

The population's health could be jeopardised by the manipulation of communicable diseases or the contamination of food, soil, air and drinking water by chemical, biological, radiological and nuclear agents. The intentional spreading of animal or plant diseases may seriously affect the food security and have major economic and social effects on crucial areas of the food chain.

The cyber space constitutes the most extreme form of this vulnerability. Broad reliance on cloud computing and big data has increased vulnerability to hybrid threats. 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. Consequently, improving the resilience of communication and information systems is important. Industry needs to be involved. Public-Private Partnership on cyber security could improve protection and also ensure continued research and innovation.

[2] 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

3. Stakeholder Cooperation

As states, societies and economies become more interdependent, resilience requires joint action of all relevant actors – to include whole-of-society and international partners. Consequently, resilience requirements are reflected in recent European Union and NATO decisions. Both organisations have understood that only cooperation will enable them to come up with proper resilience. 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 Joint Communication outlines actions designed to help counter hybrid threats and foster the resilience at the EU and national level, as well as partners.

Actions have been outlined to build resilience in areas such as cyber security, critical infrastructure, protecting the financial system from illicit use and efforts to counter violent extremism and radicalisation. In each of these areas, implementation of agreed strategies by the EU and the Member States, as well as Member States' full implementation of existing legislation are critical initial steps. Further concrete actions have been put forward to reinforce these efforts. In particular, it is proposed to step up cooperation and coordination between the EU and NATO in common efforts to counter hybrid threats.

NATO's Heads of State and Government have echoed and confirmed this approach at their Warsaw Summit on July 8-9, 2016 with the 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."*[3]

Also partner nations of the European Union and NATO are among the stakeholders. 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. Consequently, the European Union and NATO are investing to strengthen partner nations' national capacities in the fight against hybrid threats. The European Union Global Strategy 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."*[4]

Of particular importance is the cooperation with the private sector.[5] The military has become increasingly dependent on infrastructure and assets in the private sector. NATO for example faces two distinct but interrelated resilience challenges: first, to ensure that it can rapidly move all the forces and equipment needed to mission areas when facing an imminent threat or attack; and second, to be able to anticipate, identify, mitigate and recover from hybrid attacks with minimum disruptive impact.

[3] 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
[4] 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
[5] 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

Without doubt the transfer of ownership and responsibility to the private sector has brought cost-efficiencies; but the quest to reduce costs and overheads to increase profitability has also led to less redundancy and less resilience. Today, 90 per cent of NATO's supplies and logistics are moved by private companies and 75 per cent of the host nation support for NATO forces forward deployed on the territory of the eastern Allies comes from private sector contracts. A possible disruption of supply chains highlights the present over-reliance on "just-in-time" approaches which may pose grave implications for the military – and as well for the civilian population. Similar dependencies exist with view to critical resource and services such as fuel, power and food. Also when facing distributed denial of service cyber-attacks against its outward-facing networks, military increasingly rely on cooperation from the telecoms sector and the internet security companies to filter and capture data, identify malware and provide extra bandwidth.

More than that the private sector has become a key driver of change through technology and innovation. 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 the attractive partners from the past for the private sector as these partnerships bring plenty of paperwork, formal and bureaucratic meetings while the money is earned predominantly in the non-governmental business.

4. Resilience Readiness

Resilient systems and organizations need to maintain some functionality and control while under attack. To this end three elements are critical:

- Capacity to work under downgraded conditions;
- Ability to recover quickly;
- Readiness to learn from experienced attacks.

NATO's Allied Command Transformation (ACT) has identified four *„focus areas"* with potential to enhancing resilience:

- Identifying key vulnerabilities and associated risks – this enables governments to develop adequate responses and mechanisms to manage consequences orchestrating all suitable instruments of power – both nationally and internationally.
- Synchronizing cross-governmental decision making – countering hybrid threats demands a different, cross-governmental approach employment of security mechanisms than in the past. Political and military decision-makers need to be able out-manoeuvring opponents attacking own centres of gravity.
- Building military sustainability and civil preparedness – the civil population is not only a potential victim; at the same time, it is a critical source of strength, of resilience. Civil preparedness enables military sustainability, while military capabilities protect the population and its prosperity.
- Balancing the allocation of available resources – enhancing the links between the civil, private and military sector will enable cost-sharing and benefit resilience at the same time. It provides for developing means of mitigation, such as diversification of supply, resource and service.

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

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. As a civil readiness project resilience needs to be organized with defined standards and a training capacity to achieve it. Scenario based simulation exercises can be a catalyst for learning in complex emergencies – for civil and military actors, but in particular for civil-military cooperation. From ACT perspective these *„focus areas*" could 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?

Situational awareness is the starting point of meeting hybrid challenges and building respective resilience. This requires first of all common and shared understanding of own vulnerabilities, i.e. a shared risk assessment of own critical vulnerabilities, own centres of gravity, but also an understanding of those perceived by opponents as they are likely to exploit these and those of the opponent as one should likely have a deeper look at them. Dedicated mechanisms for the exchange of information are required. Rapid identification of a hybrid attack is a critical precondition for timely decision making in order to early engagement and blocking escalation. Indicators of hybrid threats and existing risk assessment mechanisms need to provide for early warning.

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. Intelligence and information sharing has become even more important. 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 reflect recent developments in and reactions to hybrid warfare. They will be instrumental to developing a common and shared understanding of threats and vulnerabilities, the tools and mechanisms and improving integrated decision making.[6]

To this end, joint civil-military education, training and exercises – to include higher level training – need to 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.

Recently, NATO ambassadors and defence ministers have held simulation and scenario-based exercises to check their situational awareness and responsiveness vis-à-vis hybrid threats. Obviously, this has been a wake-up call to many. Civil leadership and civil-private-military interaction needs to improve facing challenging hybrid threats. Many are now more encouraged than ever to map potential vulnerabilities that can arise from Russia's involvement in business, financial, media or energy concerns, and to share the lessons learned from resilience stress testing.

As hybrid warfare with 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 political decision-makers need to improve their skills in dealing with comprehensive, cross governmental security operations. In the Ukraine Russia didn't seek a decision of this conflict in the military field. The military elements of the Russian hybrid approach rather served the cover up and protection of subversive, secret service, propaganda or political operations. These may shift from the military to the civil realm, from nation to nation, from organisation to organisation and crossover new organizations, command concepts.

[6] 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

To this end, 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. To promote sustainable development and foster resilience new pathways toward holistic, cross-discipline and divergent thinking need to

- 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*".

Such *„Resilience Readiness Centres"* would provide an experimentation, simulation & training environment in order to

- Fuse knowledge, experience, skills and tools of all relevant stakeholders;
- Promote network enabling meeting political and operational demands,
- Identify and help close interoperability gaps,
- Prepare involved decision-makers to optimally perform their respective functions.

Applications would include training, exercise, decision support, testbed, modelling & simulation, research leadership and cooperative support. Dynamic scenarios would reflect current hybrid challenges, the latest policy development and research, provide challenging conflict dynamics and allow for simultaneous gaming on national and regional level. They would maximize civil-military-police interaction, include mandates, themes and incidents that trigger multi-functional coordination.

As a network of institutes – i.e. as regional and/or functional „*Resilience Readiness Centres*" – these should design programmes to advance research and exercises to find practical solutions to existing challenges posed by hybrid threats. They could network closely with existing centres of excellence in order to benefit from insights into hybrid threats that have been gained from cyber defence, strategic communication, civilian military cooperation, energy and crisis response. They could focus on researching how hybrid strategies have been applied, and could encourage the development of new concepts and technologies within the private sector and industry to help member states build resilience. The strength of such centres would rely on the expertise developed by its diversity of national, multinational and cross-sector participants from the civilian and military, private and academic sectors.

Clearly, decision-makers in nations and organizations, in public and private functions need to be cross-linked to overcome modern, hybrid challenges, integrating and empowering unity of effort. Hybrid warfare has become a defining feature of the security environment. Unpredictability has become a weapon. This dangerous development needs to widen the perspective and the sense of urgency of all involved.

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

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

This paper was presented on the occasion of the 5th *Germany-Malaysia Security Dialogue* on September 19, 2016 in Kuala Lumpur, Malaysia. The conference was organized by the Malaysia Office of the Konrad Adenauer Foundation in cooperation with the Institute of Strategic and International Studies (ISIS) Malaysia.

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