Chasing the Centre of Gravity in the Age of Accelerations[1]

Ralph D. Thiele

May 2018

Summary

In an Age of Accelerations, we can see the devolution of hegemonic power into increasing regionalism. Hybrid concepts and strategies come to the fore. Technological upheavals suggest that the portfolio of hybrid hazards will rapidly expand. These 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. The cyber domain has a particular role in applying and fighting hybrid action. Everything can be damaged, disrupted or put out of service practically from anybody anywhere. The resulting ambiguity makes an adequate reaction difficult.

Countering hybrid warfare requires more than rapid military responses, i.e. a flexible policy applying a wide range of particularly non-military instruments. The concept of a Centre of Gravity (CoG) in conflicts has been introduced by Carl von Clausewitz and has evolved as a core element of military doctrines who described the enemy's CoG as "the hub of all power and movement, on which everything depends." Chasing CoGs is something also civilian/political decisionmakers should urgently train as in hybrid conflicts the CoG will be likely on their side.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is an objective, task-oriented and politically non-partisan institute.

In the increasingly complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, which occasions both major opportunities and risks, decision-makers in the economic and political arena 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, the economy, international relations, and security/ defense. ISPSW network experts have held – in some cases for decades – executive positions and dispose over a wide range of experience in their respective fields of expertise.

[1] This think piece reflects my remarks given at the Symposium and Workshop INNOVATION IN THE "AGE OF ACCELERATIONS": GLOBAL RESILIENCE AND CYBER KNOWLEDGE NETWORKING, 6 APRIL 2018, George Mason University Science and Technology Campus, Manassas, Virginia

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

Security in No One's World

In the emerging security environment classical power projection will not suffice. Hybrid concepts and strategies come to the fore. These 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. A distinction can be made between hybrid influence (disrupting political space) and hybrid warfare (controlling territory or decisions), each by an ultimately state actor.

The cyber domain has a particular role in applying and fighting hybrid action. Via the cyber space everything is connected to everything else: systems, machines, people. 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 democratic societies or multinational organizations that operate on the principle of consensus. „New" forms of warfare and fighting evolve. Traditional lines of order and responsibilities are being challenged through operations against specific vulnerabilities of the opponent in the shadow of interfaces. The main focus of hybrid action is on people and decision-making. The decision of hybrid war/conflict is searched for primarily at non-military centres of gravity.

Technological upheavals suggest that the portfolio of hybrid hazards will rapidly expand. Computers are becoming faster and ubiquitous. Other fundamental breakthroughs include robotics, nano- and biotechnology, artificial intelligence and sensor technology. Machines are getting smaller and more powerful every day. They connect symbiotically with people's lives. In the increasingly developed knowledge society, knowledge proliferates not only legally, but very often as well as through systematic theft of intellectual property. Communication technologies are driving this development. The enormous potential of Big Data plays an important role here.

Resilience needed

Vis-à-vis hybrid challenges resilience has become 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, organizations and people need to be prepared for attacks. 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 rise to new levels.

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.

Investments in resilience are anything but trivial tasks. The hybrid complexity and ambiguity must be countered with an interdepartmental and trans-sectoral perspective. From the outset, a decidedly innovative approach is needed that builds on existing approaches and generates new momentum. A special opportunity is offered to strengthen the resilience of the state and society, armed forces and the private sector through a

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

networked simulation and experimental network of new technologies, innovative partnerships and creative thinking.

Of particular importance is the cooperation with the private sector. This cooperation will not develop easily. 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. There is much more money in the non-military business, while governmental partnerships bring plenty of paperwork, formal and bureaucratic meetings while the financial incentives keep shrinking.

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.

The primary responsibility for building and sustaining resilience lies at the national level as most vulnerabilities are country-specific. Yet, cross-functional, cross-national and cross-societal interdependencies require 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.

Resilience new cut is to generate an increase in value by means of innovation to proven projects and processes, which must be practiced lastingly and developed continuously. Creating resilience is both a process and a goal. It is about the attitude and motivation of key players, right down to the individual citizen. It is an iterative, inclusive, integrated, adaptable and flexible process. In liberal democratic societies it is supposed to protect a free, democratic basic order and its values. It has to come up with concrete and measurable skills. The key to success is the continued integration of new information and new knowledge as a basis for the current reassessment and reprioritization of existing activities.

Centre of Gravity

How can decisionmakers protect national security and the personal security of citizens against this background? Countering hybrid warfare requires more than rapid military responses. Valid approaches need to be based on a flexible policy, striving to deter and counter hybrid adversaries with a wide range of instruments. Rapid identification of a hybrid attack is a precondition for timely decision making in order to early engagement and blocking escalation. To this end networked knowledge, expertise, and situational awareness is of key importance.

While hybrid actions appear to be a construct of vaguely connected elements. In reality the pieces are a part of an intended mosaic. The military concept of a Centre of Gravity (CoG) in conflicts has been introduced by Carl von Clausewitz and has evolved as a core element of military doctrines. 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*."[2]

[2] Carl von Clausewitz, „*On War*", eds./trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), pp. 595-6.

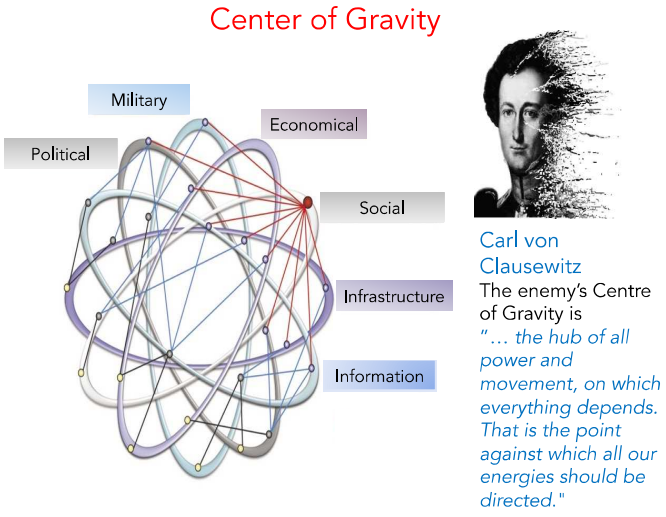
Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Joseph L. Strange and Richard Iron have offered an understanding that multiple CoGs *might exist and may even change from phase to phase within a campaign.*[3] This approach is perfectly suited to meet the recent challenges posed by hybrid influencing and hybrid warfare. Political and military decision-makers have then to determine how to protect own CoGs and influencing opponent actors CoGs in the desired manner.[4]

Clausewitz thought of the CoG effects based. This makes the CoG approach particularly fitting vis-à-vis the NATO Comprehensive Approach to security that is effects based too and explicitly focuses operations on political, military, economic, social, infrastructure, and informational effects by using diplomatic, information, economic and military actions.

What Education, Training, Networking?

Chasing CoGs is something civilian/political decisionmakers should urgently train as in hybrid conflicts the CoG will be likely on their side. Clausewitz considered the calculation of a CoG a matter of „*strategic judgment*", to be addressed by the top decision-makers. Unfortunately, too many political and military decision-makers today have only limited respective education, training and experience. This needs to be changed to enable viable political-strategic options resulting from alternative DIME-employment options. There is an urgent need to improve and to develop skills dealing effectively with hybrid threats on all levels of decision-making. Civilian and military leadership need to be better prepared.



[3] Dr Joseph L. Strange and Colonel Richard Iron, „*Centre of Gravity: What Clausewitz Really Meant*," *Joint Force Quarterly*, 35 (October 2004), pp. 20-27.
[4] Australian Defence Doctrine Publication (ADDP) 5.0, „*Joint Planning*", Edition 2 (Canberra: Department of Defence, February 2014) 2-11, 2-12.

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

Education has to broaden the understanding of the exposures security actors face. This is not predominantly a technical matter. It rather requires developing a comprehensive view across all dimensions, to encourage broad, innovative thinking about how to enhance the long-term sustainability of societies, nations, economies and organizations against a backdrop of acceleration and dynamic change.

New pathways toward holistic, cross-discipline and divergent thinking must be pursued in order to promote sustainable development and foster resilience. Exercise and training programs need to be adapted to reflect developments in and reactions to hybrid warfare. As hybrid actions build tactically on blended tactics, flexible and adaptable structures, special operations and Information operations the scope of tactical training is challenging. 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.

Knowledge networking is key to organizational learning and adaptation, to training and education and last but not least to operations – thus making available knowledge actionable. An easy accessible knowledge network needs to cover the political, military, economic, social, infrastructural, and informational disposition of hybrid opponents that may allow to identify centres of gravity and support assessments. Regional and even Global Knowledge Networking together with a network of regional and functional *„Resilience Readiness Centres"* would contribute to significantly improved education, training and readiness against hybrid threats.

***

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

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 President of EuroDefense Germany, 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 also a member of the ISPSW Speaker Management Team. Further information at ISPSW website: http://www.ispsw.com/en/speaker-management/


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