Democracy Under Fire

Ralph D. Thiele

June 2019

Summary

Russia is currently perfecting its abilities in hybrid warfare. Particularly, the Baltic states, Georgia, Moldova and the Ukraine are under constant hybrid fire by all technological means with special use of media and social media. Technology matters, because it plays a decisive role in hybrid aggression and its defence. We can expect a wide range of technologies to contribute to hybrid warfare and its objectives, i.e. artificial intelligence, virtual reality and quantum computers. NATO and EU should cooperate with governmental and non-governmental organizations in the Baltic region, Georgia, Moldova and Ukraine and create a common platform for resilience and defence against 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 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.

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

Within sight of the European public, but without its attention, Russia is currently perfecting its abilities in hybrid warfare. This insidious form of aggression includes military elements such as intelligence, cyber-attacks and fake news, as well as the firing of riots and terrorism. Not only Russia, but also China, Iran and North Korea are increasingly developing extensive capabilities. They are thus putting democracies at risk.

It is clear that Russia has not only modernised its armed forces in recent years but has also developed the hybrid capabilities of its instruments of power. This is demonstrated by the continuing aggression in Eastern Ukraine, Russian involvement in Syria, global interference in elections and referendums, the poisoning of the Skripal family, and support for radical political parties in European states.

What is hybrid warfare about? To impose its will on its opponent without crossing the threshold of open war. That is why hybrid aggression lives from ambiguity and cavorts in grey areas of internal and external security, economics and crime, information and deception. It targets the vulnerabilities of our open societies, their economies and infrastructures. By undermining people's confidence in the democratic rule of law and the ability of rulers to ensure its viability and prosperity, it fights the target both internally and externally. In the "ideal case" the attacked state implodes before it can defend itself.

The successes of Russia's hybrid warfare in Ukraine have shown us its effectiveness. I have just returned from a conference in Lithuania at which representatives of the Baltic states, Georgia, Moldowa and the Ukraine reported on how their democratic orders are under constant hybrid fire by all technological means with special use of media and social media. The governments and citizens of the Baltic states, for example, are the daily targets of Russia's strategic information operations and propaganda activities. These aim to undermine confidence in state institutions, fuel ethnic and social tensions and weaken the cohesion of NATO and the European Union. In addition, there is hybrid aggression through Russian special operations and regular armed forces stationed near their borders.

How can hybrid warfare be countered? A common understanding of the situation, joint threat and risk assessments, joint planning and training processes for the most important actors and institutions are the first steps. Regular exercises based on hybrid scenarios should be established. Not only the education of officials, politicians, media and society is an important issue in the fight against hybrid threats, but also active communication in the identification of lies, their deconstruction, the development of own messages and narratives.

Since trust in the democratic order is the target of the attack, all social forces must take part in the defence, i.e. also companies and local politicians, churches and welfare associations. In addition, hybrid threats must be countered not only nationally, but also regionally and multilaterally. This is one of the reasons why NATO and the EU are joining forces. In this way, any missing national capabilities and capacities can be "covered" or their development supported.

In addition to the traditional instruments of national power such as the police, the Office for the Protection of the Constitution, intelligence services and armed forces, a nation's own resilience in particular becomes its immune system. It is a critical factor in resisting stress in the face of hybrid threats and returning to everyday life after shock events.

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

Technology matters, because it plays a decisive role in hybrid aggression and its defence. While ongoing digitalization is already bringing with it enormous demands for change, the world is rapidly moving towards a post-digital era. Artificial intelligence, virtual reality and quantum computers will not only reshape prosperity and security, but also the human-machine relationship between individuals and entire societies. People are using new technologies with verve: customers and employees, government officials and criminal actors. We can expect a wide range of technologies to contribute to hybrid warfare and its objectives. At the same time, it is crucial to resist hybrid aggression. It is therefore important that resilience and technology centres can work together.

NATO and EU should cooperate with governmental and non-governmental organizations in the Baltic region, Georgia, Moldova and Ukraine and create a common platform for resilience and defence against hybrid threats. This serves not only the democratic institutions there, but also those of NATO/EU member nations. Democratic order needs resilience and strength, otherwise its days are numbered.

***

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, born in 1953, is President of EuroDefense, Germany, Managing Director StratByrd Consulting, Germany, Chairman Political-Military Society, Germany and Member Advisory Board German Employers Association, Wiesbaden. He is a retired Colonel, held in his 40-year military career in the German Armed Forces key national and international positions. He

- Commanded troops up to the battalion level;
- Developed concepts and capability requirements in the Ministry of Defence;
- Drafted speeches and policy papers for Federal Presidents, Ministers of Defence, Major NATO Commanders and Service Chiefs;
- Drove educational innovation at the German Armed Forces Command and Staff College (Director Faculty) and at the NATO Defense College (Chief of Staff);
- Shaped the Bundeswehr's path towards network enabled capabilities (Commander Bundeswehr Transformation Command).

In his honorary and business functions he advices on Defence Innovation and Cyber issues in times of digital transformation. He has been frequently consulting, publishing and lecturing in Europe, America and Asia.

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