

BACKGROUND REPORT

PRAGUE **PRAŽSKÝ**
STUDENT **STUDENTSKÝ**
SUMMIT



NATO

Hybrid Threats



Autor: Jitka Richterová
Imprimatur: Martin Mezenský, Jan Kotara
Jazyková úprava: Adéla Jiříčková
Grafická úprava: Jan Hlaváček

Model NATO

Vydala Asociace pro mezinárodní otázky (AMO) pro potřeby XXI. ročníku Pražského studentského summitu.

© AMO 2015

Asociace pro mezinárodní otázky (AMO)
Žitná 27, 110 00 Praha 1
Tel.: +420 224 813 460, e-mail: summit@amo.cz
IČ: 65 99 95 33

www.amo.cz

www.studentsummit.cz



1 NATO and hybrid threats

Today media often mention the so called hybrid wars. Though most articles do not explain the concept at all, often misinterpret it or use it in a misleading way. How to really understand the concept and tactics of hybrid war regarding NATO operations?

The concept is very challenging to understand given its complexity and abstractness on the theoretical level when explained outside the borders of one concrete example. That is a part of the art of hybrid warfare.

The background report introduces the term hybrid threat and aims to explain it. Afterwards the report describes common used tactics and thoughts behind the strategy of hybrid warfare, aspects and phases of hybrid warfare and the strategy of comprehensive defence as an effective way to battle hybrid threats. Moreover, the report describes hybrid threats that are identified by NATO and how the Alliance battles them.

2 Introduction to the term

"hybrid attack", "hybrid war", "hybrid warfare", "hybrid threat".

The term "hybrid war" refers to a conflict where both/all sides involved use hybrid warfare that combines conventional (regular), irregular and other approaches to combat. The concept was not created in the context of the Ukraine conflict, in which context it is often mentioned, but was first used much earlier, even though the combination of tactics and combats to which the term refers goes technically according to main definitions way further.¹ Frank Hoffman in his short interview² for the Center for Strategic & International Studies, commented on his use of the term in his article as a term aiming to describe what kind of wars the West or the U.S. will be facing in the future.

¹ For example the Cambridge publication „Fighting Complex Opponents from the Ancient World to the Present” shows that the combination of different tactics and combats is not a modern military strategy but existed even during the ancient world, it is the term that is newer. Nicu Popescu in his paper "Hybrid Tactics: neither new nor only Russian" says that such combinations of unconventional tactics "are as old as war itself" and Western states used to use them effectively on the tactical level themselves. (Popescu, January, 2015) Similarly Michael Kofman and Matthew Rojansky in their article "A Closer Look at Russia's 'Hybrid War'" (Rojansky, 2015, p. 2) say that the term is „as old as warfare itself". Some of the mentionable examples of hybrid warfare are the conflicts of Hezbollah movement in Lebanon, Georgia, Russian invasion in Afghanistan, Spanish Guerrillas during Napoleon's Spanish invasion and many others.

² For more information go to: <http://csis.org/blog/military-scholar-frank-hoffman-meaning-hybrid-warfare>



2.1 Conventional (regular) warfare

Regular warfare is, according to NATO's definition, warfare where regular opponents, officially enlisted by state, are engaged and regular tactics and activities are used, while respecting international treaties, conventions and laws.

2.2 Irregular warfare

Irregular warfare is according to available NATO's definitions a warfare that denotes a form of conflict, where one or more protagonists adopt irregular methods.³ Additionally, *"irregular troops are any combatants not formally enlisted in the armed forces of a nation-state or other legally constituted entity."*⁴ Other definitions describe it as *"a violent struggle among state and non-state actors for legitimacy and influence over the relevant populations. Irregular warfare favours indirect and asymmetric approaches⁵, though it may employ the full range of military and other capabilities, in order to erode an adversary's power, influence, and will."*⁶ Moreover irregular opponents are unlikely to adhere to recognised treaties and international conventions. On the other hand they are likely to rely on local support, fight in the place they live and they are often hard to distinguish from local civilians. The irregular opponents' tactic will often include undermining and eroding target's will and determination. The tactic also includes avoiding regular decisive deployment of national forces, and if necessary, then preferably under the terms and circumstances chosen by the irregular opponents.⁷

2.3 Hybrid warfare

Hybrid warfare in NATO's view is a violent conflict applying combination and simultaneous use of conventional and irregular warfare, involving both state and non-state actors, used adaptively in pursuit of their objectives and not limited to physical battlefield or territory. Each attack contains its own combinations and mutations of the two and targets further aspects of state and society to undermine it and reach its goals. Hybrid warfare can be employed in conflicts not only by states and armed forces but also by a variety of actors beyond the

³ According to "Countering Irregular Activity within a Comprehensive Approach" Joint Doctrine Note 2/07 "Irregular Activity is defined as: Behaviour that attempts to effect or prevent change through the illegal use, or threat, of violence, conducted by ideologically or criminally motivated non-regular forces, groups or individuals, as a challenge to authority."

⁴ AJP-3.2, *Allied Land Operations, 2d Study Draft, February 2006*

⁵ Asymmetric warfare is such in which opposing groups or nations have unequal military resources, and the weaker opponent uses unconventional weapons and tactics, as terrorism, to exploit the vulnerabilities of the enemy (definition taken from dictionary.com)

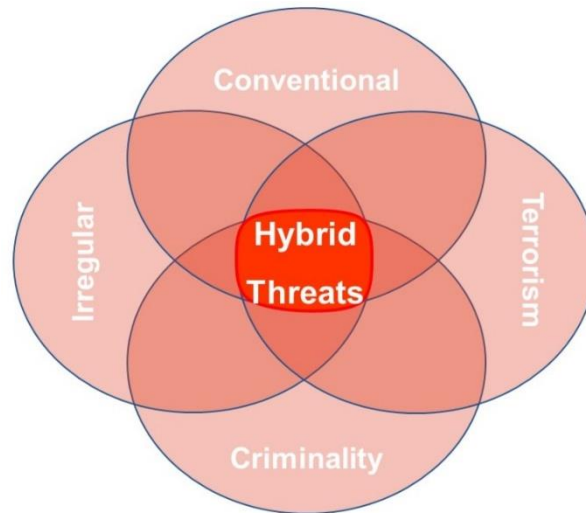
⁶ *USA Irregular Warfare Joint Operating Concept*

⁷ PURTON, Simon a . Why half of winning an Irregular War is agreeing on what it is.... *NATO, Allied Command Transformation: Future Capabilities, Research and Technology* [online]. [cit. 2015-08-01].



authority of states.⁸ (Such as terrorist or extremist groups.) Even though the phenomenon is hardly new, what is new and surprising is the “**scale of use and exploitation of old tools in new ways.**”⁹

Figure 1: Hybrid Threats¹⁰



3 The most common use of tactics of hybrid warfare

The hybrid warfare often indicates a different use of methods. Instead of a large-scale military invasion the attacker aims to target and undermine the subject by **other methods**, often involving use of **disinformation campaign, subversive intelligence, cyber-attacks, sabotage or (not only) political support of separatist or other groups advantageous for the attacker**. Other researchers also describe it as a combination of “*conventional capabilities, irregular tactics and formations, terrorist acts that include indiscriminate violence and coercion*”¹¹, and *criminal disorder*.¹² Such hybrid attacks often target **both physical, psychological, cultural, political and human dimension**. The psychological and political dimension involve aiming on separation of military and highly educated and professional classes from average civilian population. Such steps lead to division of society, making political decisions more difficult to employ. The combination of using all mentioned aspects of hybrid

⁸ BACHMANN, Hybrid Threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats: mapping the new frontier of global risk and security management. *Amicus Curiae* [online]. 2011, (88) [cit. 2015-08-01]. pages 24-25

⁹ JACOBS, Andreas a Guillame LASCONRAJIAS. NATO's Hybrid Flanks, Handling Unconventional Warfare in the South and the East. *NATO Defence College* [online]. [cit. 2015-08-01].

¹⁰ Simon Purton, Future Capabilities, Research and Technology, Allied Command Transformation, NATO: „Why half of winning an Irregular War is agreeing on what it is...”

¹¹ The action or practice of persuading someone to do something by using force or threats.

¹² *Hybrid Warfare and Challenges: Frank G. Hoffman* [online]. Washington D.C.: National Defense University, Institute or National Strategic Studies, 2009 [cit. 2015-07-11].



warfare together with conventional military attacks and flexibility largely adds to the danger of the threats of hybrid warfare.

Altogether, hybrid attacks are using and **exploring the interdependencies and vulnerabilities of societies**. The concept of hybrid war is **confusing war and peace** as it is unclear when the actual war starts and ends, whether during information and cyber attacks or during military operations, even more so as cyber attacks tend to be the spearheads¹³ of hybrid operations. Especially in the case of the North Atlantic Treaty Organisation the concept currently brings up the notion of totalitarian wars¹⁴.

In conclusion, further characteristics or tactics of hybrid warfare include:

- Blended tactics – combining military capabilities with small (and/or guerrilla) units, asymmetric attacks¹⁵ and mobile units;
- flexible and adaptable structure – as the units are small, they are usually capable of both adaptable small and quick reacting units and mass scale formations;
- terroristic and cyber terroristic attacks;
- technologically advanced systems (mis)used beyond their original means;
- propaganda, media control and/or disinformation campaign;
- criminal activity as a common source of finance or as an attack;
- aiming at separation of society, undermining its unity and making carrying out of political decision difficult;
- and disregard for international law – use of subversive¹⁶ intelligence, sabotage or political support of extremist groups advantageous for the attacker.¹⁷

¹³ Leading the attack

¹⁴ Cederberg, Aapo, Geneva Center for Security Policy Institute, presented in PSSI's NATO Summer School, Měříň, July 23, 2015.

¹⁵ Definition taken from dictionary.com: „warfare in which opposing groups or nations have unequal military resources, and the weaker opponent uses unconventional weapons and tactics, as terrorism, to exploit the vulnerabilities of the enemy.“

¹⁶ Actions designed to undermine the military, economic, psychological, or political strength or morale of a governing authority, Source: DoD; Joint Education and Doctrine Division (November 2010). "Dictionary of Military and Associated Terms: (As Amended Through 15 May 2011)" (PDF). *Joint Publication 1-02. Department of Defense*. p. 351. Retrieved 2011-06-21.

¹⁷ MORELAND, Scott. The Islamic State is a Hybrid Threat: Why does that Matter. *Small Wars Journal* [online]. [cit. 2015-08-01].



4 Aspects of hybrid warfare

As mentioned, the hybrid threats mostly contain not only military domain but target as thoroughly and widely as possible in order to achieve their goals. Hence the aspects of the attack have been identified as seen below in picture 2¹⁸.

The attack often consists of a combination of following **factors: political, military, diplomatic, economic and private sector power, terrorist power, cyber power, civil power and media power**. All these factors in combination contribute to the strength of attacker and complexity and chance of success of an attack.

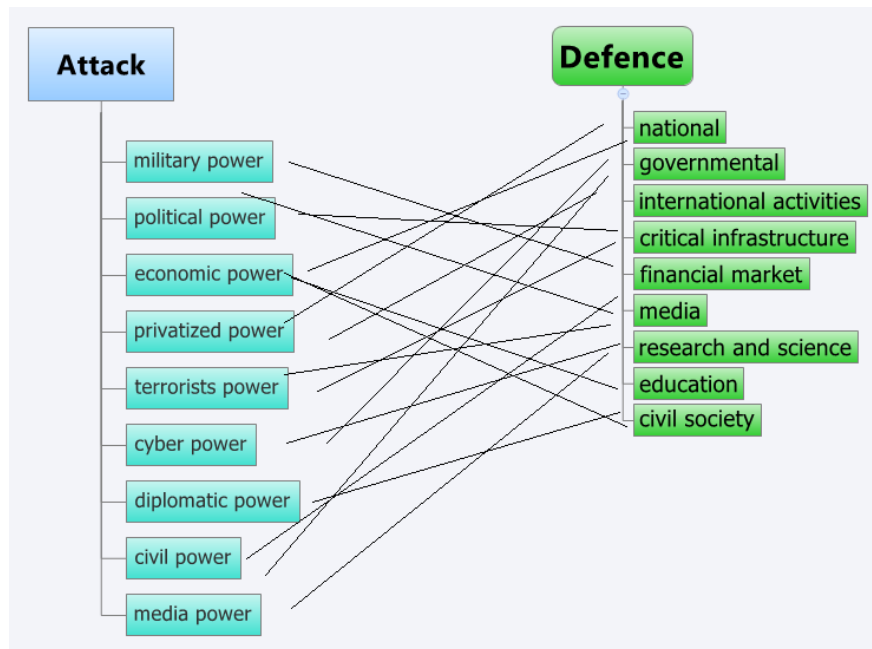
The aspects of defence on the other side should and need to be responding to the aspects of attack. It is also important to recognise that the combinations and strength of attacking aspects are always different, hence for comprehensive and successful defence states and Allies have to have developed all the defending aspects and have to be able to use all of them both separately and in combinations to secure the defence or even counter attack. The aspects of defence then include: **national and governmental defence, international activities, critical infrastructure, financial market, media, research and science, education and civil society**.

The defence has to respond in parallel series of these aspects to respond to the tactical "surprise" of the combination of attack of the enemy.

¹⁸ Cederberg, Aapo, Geneva Center for Security Policy Institute, presented in PSSI's NATO Summer School, Měřín, July 23, 2015.



Figure 2: Aspects of hybrid attack and defence¹⁹



5 Phases of hybrid attack

Although the phases of hybrid warfare may not be used in common and settled international terminology, the Background Report has a quick description of them included in this chapter as it considers it useful for our perception of hybrid attacks and warfare.

The phases are according to Geneva Center for Security Policy's²⁰ researcher, Aapo Cederberg, as follows: the preparation phase, the attack phase and the follow up phase.

5.1 The preparation phase

This phase labels the steps, situations and decisions taken prior to the actual attack in order to secure advantageous environment to carry out the attack itself. From the previous chapter describing the aspects of an attack it is deductive what areas could such steps and decisions include. This phase has a very broad reach, from preparing the military, economic and private sector power, through gaining sufficient political mandate, playing diplomatic games, taking steps and situations in domestic policy in order to prepare the society and gain its support to media control and specific releases. It is very important to study this phase and steps as it

¹⁹ Aapo Cederberg presentation for the Geneva Center for Security Policy Institute presented in PSSI's NATO Summer School, Měříň, July 23, 2015.

²⁰ For more information, please see: <http://www.gcsp.ch/News-Knowledge/News/GCSP-S-Aapo-Cederberg-talks-hybrid-defence-at-Prague-Security-Studies-Institute>



contains very important warning signs that the Western society and NATO are to recognise if they want to successfully battle hybrid threats.

5.2 The attack phase

The attack phase may be surprisingly shorter than the preparation phase, or even the shortest of the three. It includes the chosen combination of available and known military and non-military attack aspects. Thereby it usually includes military operations, paramilitary units or rebel units operations and support, political and diplomatic steps, terrorist and cyber threats with the domestic support often secured by regulated media/information broadcast or other presentation. Another very important precondition to the attack is presence in the targeted country. In some cases it is difficult to define where the actual attack, or war, starts and which actions are already an open war compared to actions of preparations phases or closed conflict.

5.3 Defending the end state

The follow up phase aims to ensure carrying out of the goals of the mission, and often again includes series of political, diplomatic and military steps responding to current situation. This phase comes after the attacking itself and hence it is once again difficult to identify the conflict as it is not an open war but seems more like a diplomatic chess game clearing out the path for victory.

6 Fighting hybrid threats and comprehensive defence

Given that we described the phases of attack in three phases, the Background Report now suggests three steps of defence in accordance.

6.1 The defence phases

For successful defence, the states and Allies have to be able to **recognise early warning signs** of possible hybrid attack or operations during attacker's preparation phase. This is a very important step of defence as early recognition can lead to prevention of further actual attack, damages and casualties or at least minimising their extent. The early recognition also allows the defender to gain time to strengthen defence and prepare crisis infrastructure.²¹

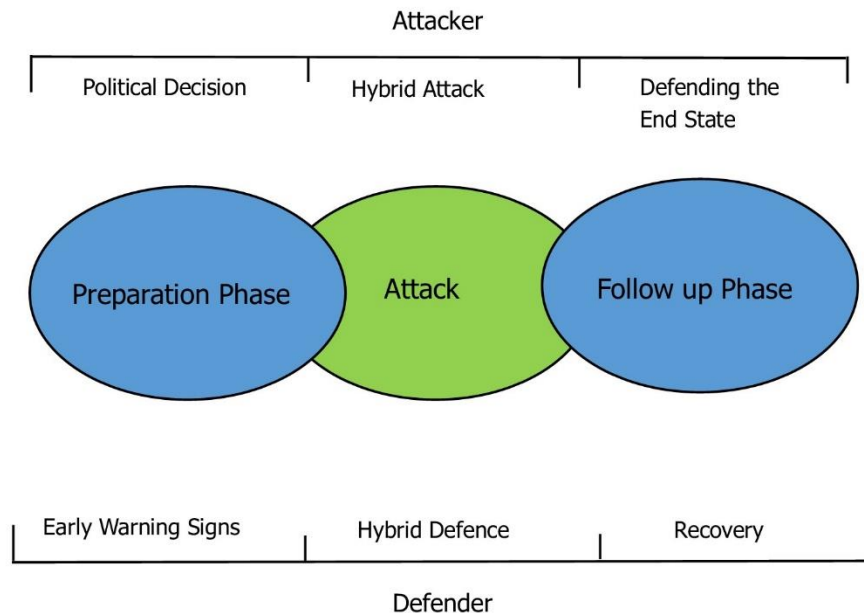
During the attack itself, the defender has to employ sufficient combination of defence aspects as a response to the attack, hence the **hybrid defence phase**. These are largely unpredictable and need to adapt to the original tactics of the attack.

²¹ Several critics claim that i.e. in the Ukraine Crisis the West has underestimated the early warning signs, did not respond to Russia's provocations adequately as it was dealing with other issues such as the economic crisis.



After the attack and the defence there is a need for **recovery time** for the states to rehabilitate their military, economy, civilians and other harmed aspects of state.

Figure 3: Phases of Hybrid Warfare²²



6.2 Comprehensive defence system

Given the complexity of hybrid attacks the most effective way to counter hybrid threats is through comprehensive defence system functioning both nationally and supranationally²³. For building successful comprehensive defence system there is a need for: **prevention, intelligence, situational awareness, risk assessment, preparedness, resilience²⁴, planning, training and political will.**

The **Comprehensive Approach** aims to “*employ a complex blend of means that includes the orchestration of diplomacy, political interaction, humanitarian aid, social pressures, economic development, savvy use of the media and military force,*”²⁵ hence including **political, military and civilian areas** that are all needed for effective dealing with hybrid threats.

²² Aapo Cederberg presentation for the Geneva Center for Security Policy Institute presented in PSSi's NATO Summer School, Měřín, July 23, 2015.

²³ According to Cambridge Online Dictionary, supranationally means: involving more than one country, or having power or authority that is greater than that of single countries.

²⁴ According to Cambridge Online Dictionary, resilient means: able to quickly return to a previous good condition

²⁵ AARONSON, Michael, Sverre DIESEN, Yves DE KERMAON, Mary Beth LONG a Michael MIKLAUCIC. NATO Countering the Hybrid Threat. *Prism 2* [online]. (4) [cit. 2015-08-01].



To effectively counter the hybrid threats NATO will have to strengthen political-military relationships among Allies, fasten reactions, tighten cooperation, improve domestic politics to be capable of comprehensive defence against hybrid attacks and strengthen cooperation with other international organisations in particular with the EU.²⁶

The Alliance has demonstrated an effort especially in the field of cyber defence.²⁷ Nevertheless, NATO, being a military organisation²⁸, will never be on its own capable of full comprehensive defence and will most likely rely a lot on the member states' steps and defence infrastructures as well as cooperation with other supranational bodies.

7 Hybrid threats as identified and countered by NATO

The Alliance is fighting in the 21st century both its old battles, referring to Russia, and the new, international ones to which it has to be able to respond as a defensive, military alliance. Hence even hybrid threats to it are both from its traditional and new, international/overseas threats. Specifically, NATO is facing hybrid challenges currently from **Russia, in Afghanistan²⁹, and possibly by the Islamic State.**

At the international, broader level, NATO has identified several actions as hybrid threats. Among them are: **multimodal³⁰, low intensity³¹, kinetic and non-kinetic³² threats to international peace and security including cyber war, low intensity asymmetric conflict³³ scenarios, global terrorism, piracy, transnational organised crime,**

²⁶ For more information see: http://www.nato.int/cps/en/natohq/topics_49217.htm

²⁷ BACHMANN, . Hybrid Threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats: mapping the new frontier of global risk and security management. *Amicus Curiae* [online]. 2011, (88) [cit. 2015-08-01], pages 24-25.

²⁸ without the authorisation rights to intervene and apply other spheres of comprehensive defence approach

²⁹ Davis, John, R. Jr. Major, *Defeating Future Hybrid Threats: The Greatest Challenges to the Army Profession of 2020 and Beyond* [online]. Military Review, September-October 2013 [cit. 2015-09-25]. Available at: http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20131031_art006.pdf

³⁰ Definition taken from the free dictionary:

„In transport operations, a term applied to the movement of passengers and cargo by more than one method of transport.“

³¹ Definition taken from Oxford Reference: „Political-military confrontation, ranging from propaganda and subversion to the actual use of armed forces, between contending states or groups below the level of conventional war and above the level of unconventional warfare.“

³² Kinetic actions are those taken through physical or material means (like bombs, bullets, rockets, and other munitions) as opposed to non-kinetic, meaning the non-physical actions as defined by US Air Force Doctrine Document 2.

³³ Asymmetric warfare is such where in which opposing groups or nations have unequal military resources, and the weaker opponent uses unconventional weapons and tactics, as terrorism, to exploit the vulnerabilities of the enemy (definition taken from dictionary.com)



demographic challenges, resources security, retrenchment from globalisation and the proliferation of weapons of mass destruction³⁴.”

Figure 4: Hybrid Threats



On the more traditional note, the Russian invasion and annexation of Crimea are often labelled as a hybrid war. Many Western observers analyse the Russian tactic as a combination of conventional to irregular combat operations as well as sponsorship of political protests, economic coercion, and a powerful information campaign³⁵ thus as a hybrid war.

Due to this label, the Ukraine conflict demonstrating the hybrid threat of Russia poses the most actual and biggest hybrid threat to NATO. Even though hybrid threats to NATO are not and will not be limited to this conflict. Nonetheless the debates and critical voices arising around the conflict brought attention to this kind of threats and its current increasing use and “popularity” among sides that are not NATO’s enemies. Hence the absolute need for NATO to adapt and reform its defence strategies in order to be able to successfully respond to such threats and combat them.

7.1 NATO’s Comprehensive concept

Due to NATO’s experience with hybrid threats and irregular wars the comprehensive concept does not have to be built from zero. The Alliance has encountered hybrid threats in Afghanistan and Libya. Moreover, NATO’s member states, namely the USA has experienced more irregular

³⁴BI-SC Input for a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Enclosure 1 to 1500/CPPCAM/FCR/10-270038, 25 August, 2010

³⁵ Often identified and labelled as „the disinformation campaign“ posing security threat for European countries, with the aim to confuse reader enough to gain an opinion that truth does not exist or is impossible to find in the amount of information and theories. For more information see e.g.: Interview with Ivana Smolenova from PSSI on disinformation campaign - <http://video.aktualne.cz/dvtv/cil-ruske-propagandy-ze-pravda-neexistuje-rika-analyticka/r~56783a8c19b011e5b1d8002590604f2e/>



wars³⁶ and started to make necessary changes in defence sooner (as of 2006) than the Alliance as a whole and can therefore provide expertise and advice to other member states.

Furthermore, speaking of the Ukraine Crisis, many of the Russia's manoeuvres and tactics are actually not that new. Russia demonstrated similar tactics in Georgia in 2008, Chechnya war in 1994 and in the Soviet invasion to Afghanistan.

However, the Ukrainian conflict and the Crimean annexation did request more attention to the development of defence and its adaptation to hybrid threats. NATO after the Ukrainian conflict did indeed take on the task "to develop a set of tools to deter and defend against adversaries waging hybrid warfare."³⁷ To effectively counter the hybrid threats NATO's researches claim that the Alliance will have to strengthen partnerships with stakeholders such as international and regional organisations, EU in particular, and representatives of business and commerce.³⁸

NATO recognises the need for comprehensive defence as it is the most effective one in combating hybrid threats and concerns all the aspects of hybrid attacks. NATO is working on the **conceptual comprehensive framework; the Capstone Concept**³⁹.

So far the Alliance has demonstrated great effort especially in the field of cyber defence as well as organising several hybrid **defence conferences, experiments and gaming**. Another reassuring reaction to the Ukraine conflict is establishment of the **Very High Readiness Joint Task Force (VJTF)**.⁴⁰ The VJTF is a brigade-size unit which is supposed to be able to move within 48 hours, while able of both deployment South or East, countering the threats or as defence unit in the territory of any of the member states⁴¹.

Additionally, recent NATO's research shows 3 common opinions on comprehensive approach⁴² which include these themes:

³⁶ I.e. Vietnam, Korea or Iraq.

³⁷ PINDJÁK, Peter. *NATO Review Magazine: Deterring hybrid warfare: a chance for NATO and the EU to work together?* [online]. [cit. 2015-08-18]. Available at: <http://www.nato.int/docu/review/2014/also-in-2014/Deterring-hybrid-warfare/EN/index.htm>

³⁸ Other than cooperation with the EU (mainly in sanctions), NATO can also strengthen the relations with International Monetary Fund, United Nations, Gulf Cooperation Council and the World Bank. Both the EU and NATO vowed to strengthen their cooperation in this field.

³⁹ To see the input for the Capstone Conceptual Framework visit:

http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

⁴⁰ AARONSON, Michael, Sverre DIESEN, Yves DE KERMABON, Mary Beth LONG a Michael MIKLAUCIC. NATO Countering the Hybrid Threat. *Prism 2* [online]. (4) [cit. 2015-08-01].

⁴¹ In one of the experiments, in April 2015 the VJTF was tested with around 1500 personnel where units from the Netherlands and the Czech Republic were physically deployed and successfully trained. The training demonstrated enduring commitment of the US troops, international cooperation, collective security and multinational training. (Source: JACOBS, Andreas a Guillaume LASCONRAJIAS. NATO's Hybrid Flanks, Handling Unconventional Warfare in the South and the East. *NATO Defence College* [online]. [cit. 2015-08-01].)

⁴² For more information please see: <http://www.act.nato.int/nato-countering-the-hybrid-threat>



- Coherent application of national instruments of power
- Comprehensive interaction with other actors
- Comprehensive action in all domains and elements of crises

Furthermore, the Alliance works on 4 key areas⁴³ of comprehensive approach:

- Planning and conduct of operations
 - Training, education, exercises
 - Enhancing cooperation with external actors
 - Public messaging
- In order for the defence to be effective as the comprehensive approach, it must include the civilian area, the public has to be informed, trusting and connected to the military field.

Picture 5: NATO Countering Hybrid Threats



7.2 Building comprehensive defence within national capabilities:

As the Alliance cannot ensure fully functioning comprehensive capabilities by itself there is a need for each member states to develop its own national defence capabilities on its own. In order to build and develop such national comprehensive capabilities there is a need for:

- **Political will** (with the policy definition, strategies, strategic models and plans)

⁴³ For more information please see: http://www.nato.int/cps/en/natolive/topics_51633.htm



- **Security infrastructure/organisation** (carrying out research, providing professional guidance and assisting to ministries, provides information to public, engaging key stakeholders,...)
- **Cyber power**
- **Critical Infrastructure** (energy, oil, gas, water, energy government, emergency service, electricity, banking and finance, transportation)
- **Vision** (international activities, management of governmental activities, defence capabilities, internal security, economy and infrastructure, psychological resilience, income security)
- **Strategic Guidelines** (collaboration mode, situational awareness, preparedness, capacities of police, cyber defence, international cooperation, education, knowledge, legislation, tasks)
- **Implementation** (preparedness, threats, risk analyses, vulnerability assessment, impacts)
- **Adopting changes in time** (planning, anticipation, strategic agility)
- **Knowledge** (e.g. courses for public to inform them, such as National Defence Course, Regional Defence Course, Preparedness exercises, etc...) ⁴⁴

7.3 Further Recommendations

It is clear that NATO has reflected hybrid threats and has taken steps and measures to move on to a comprehensive and effective defence. However, the concept has yet some way to go in order to be truly effective.

Firstly, in the military dimension, according to experts, the VJTF is a correct way to go, even though the deployment still has to be practiced and the Alliance as well as each and every member state should make sure that it is fulfilling the political, bureaucratic and military requirements in order for the VJTF to be fully functioning within 48 hours⁴⁵. Moreover, NATO should also work on involving its partner countries and organising the VJTF unit around Special

⁴⁴ Cederberg, Aapo, Geneva Center for Security Policy Institute, presented in PSSI's NATO Summer School, Měříň, July 23, 2015.

AARONSON, Michael, Sverre DIESEN, Yves DE KERMABON, Mary Beth LONG a Michael MIKLAUCIC. NATO Countering the Hybrid Threat. *Prism 2* [online]. (4) [cit. 2015-08-01].

⁴⁵ JACOBS, Andreas a Guillaume LASCONRAJIAS. NATO's Hybrid Flanks, Handling Unconventional Warfare in the South and the East. *NATO Defence College* [online]. [cit. 2015-08-01].



Forces if these units are to be potentially deployed in the South (most likely against the ISIL and other extremist threats)⁴⁶.

Moreover, cyber-defence team should protect NATO's communication network, military police and law enforcement units could train and monitor friendly units, where the psychological operation teams would help to counter disinformation and propaganda followed by civilian-military units providing support to local population. All of these units should be able to cooperate and work simultaneously if necessary while being supported by the intelligence systems, awareness of the situation and the Alliance's crisis infrastructure. NATO should also consider better preparation on fighting propaganda by perhaps enhancing the Communication of Excellence in Riga⁴⁷.

8 Conclusion

So far, there has been significant increase in researching hybrid warfare. Many researchers and historians commented on the current hybrid threats posed mostly by Russia and the Islamic State and why it matters. Several articles and studies aim to predict the future hybrid challenges by looking closely further to history on other examples of hybrid wars and their use of irregular tactics.

The rising popularity of the use of hybrid warfare within more and more parts of conflict areas rise questions how to adopt traditional Western conventional warfare so that it is able to face new challenges of the 21st century. The future conflicts will however no longer be possible to categorise only as conventional or irregular, state or non-state.

This is also true for the North Atlantic Treaty Organisation. Among its member states, this topic is currently being reflected significantly by the United States military forces that are likely to have to face the hybrid threats from the Islamic State the most and have experienced a lot of irregular wars with non-traditional tactics. Other largely influenced states are the former USSR members, threatened in the East by Russia. That includes states such as Poland, Baltic States (Latvia, Lithuania, and Estonia), the Czech Republic, Slovakia, Slovenia, Hungary, Romania and Bulgaria. Other possibly affected states by the Russian threat are Sweden and Norway. However, not less interested in adopting comprehensive defence are the United Kingdom, Germany and France as the European leading powers.

⁴⁶ AARONSON, Michael, Sverre DIESEN, Yves DE KERMABON, Mary Beth LONG a Michael MIKLAUCIC. NATO Countering the Hybrid Threat. *Prism* 2. (4) [cit. 2015-08-01].

⁴⁷ JACOBS, Andreas a Guillaume LASCONRAJIAS. NATO's Hybrid Flanks, Handling Unconventional Warfare in the South and the East. *NATO Defence College* [online]. [cit. 2015-08-01].



The NATO dialogue should be reflecting the threat of Russia and its use of hybrid strategy as well as the threat of hybrid tactics from non-European states and movements such as the Islamic State threat. (The so called threats from the East and the South.) What are the member states already doing to adapt to hybrid threats and what more to do to increase chance of successfully challenging NATO threats of 21st century?

One of thy most respected military historians of our time, Sir Michael Howard said that the very military aspect needed to be looked at the most is "*the capacity to adapt oneself to utterly unpredictable, the entirely unknown.*"⁴⁸ That quote remains very relevant to the current situation of the Allies. Will NATO be able to adapt to the unpredictable and unknown?

Suggested further reading:

- [Hybrid War – Does it even exist?](#)
- [Countering the Hybrid Threat](#)
- Input for the [Capstone Conceptual Framework](#)
- [NATO updated list of Comprehensive Approach Action Plan](#)
- [NATO's Comprehensive Approach to Crises](#)
- [The Lisbon Declaration 2010](#)
- [From Comprehensive Approach to Comprehensive Capability](#)
- [Hybridní hrozby a vývoj nové operační koncepce NATO](#)

⁴⁸ Howard, "Military Science in the Age of Peace", Chesney Memorial Gold Medal Lecture, October 03, 1973, printed in *RUSI Journal* (March 1974)



Sources

A Comprehensive Approach to Crises [online]. NORTH ATLANTIC TREATY ORGANISATION. 2014, 13 November [cit. 2015-08-18]. Dostupné z:

http://www.nato.int/cps/en/natolive/topics_51633.htm

AARONSON, Michael, Sverre DIESEN, Yves DE KERMABON, Mary Beth LONG a Michael MIKLAUCIC. NATO Countering the Hybrid Threat. *Prism 2*. (4) [cit. 2015-08-01].

ACT Countering Hybrid Threats Task Force identifies future challenges. *NATO: Allied Command Transformation* [online]. May 5. 2011 [cit. 2015-08-18]. Dostupné z:

<http://www.act.nato.int/act-countering-hybrid-threats-task-force-identifies-future-challenges>

BACHMANN. Hybrid Threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats: mapping the new frontier of global risk and security management. *Amicus Curiae*. 2011, (88) [cit. 2015-08-01], pages 24-25.s

Capstone Concept Input [online]. NORTH ATLANTIC TREATY ORGANISATION. 25 August. Belgium, 2010 [cit. 2015-08-18]. Dostupné z:

http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

Cederberg, Aapo, Geneva Center for Security Policy Institute, presented in PSSI's NATO Summer School, Měříň, July 23, 2015.

Davis, John, R. Jr. Major, *Defeating Future Hybrid Threats: The Greatest Challenges to the Army Profession of 2020 and Beyond* [online]. Military Review, September-October 2013 [cit. 2015-09-25]. Dostupné z:

http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20131031_art006.pdf

http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20131031_art006.pdf

HOFFMAN, Frank G. Airpower's Crucial Role in Irregular Warfare. SMALL WARS FOUNDATION. *Small Wars Journal* [online]. SWJ Blog Post, 2007, August 6 [cit. 2015-08-01]. Available at: <http://smallwarsjournal.com/blog/airpowers-crucial-role-in-irregular-warfare>

HOFFMAN, Frank G. Review Essay: Fighting and Learning Against Hybrid Threats. *Small Wars Journal* [online]. April 4. 2012 [cit. 2015-08-18]. Dostupné z:

<http://www.nato.int/docu/review/2014/also-in-2014/Deterring-hybrid-warfare/EN/index.htm>



- HOUVINEN, Petri. HYBRID WARFARE – Just a Twist of Compound Warfare?: Views on warfare from the United States Armed Forces perspective. *National Defence University* [online]. April. 2011 [cit. 2015-08-18]. Dostupné z: <http://www.nato.int/docu/review/2014/also-in-2014/Deterring-hybrid-warfare/EN/index.htm>
- Howard, "Military Science in the Age of Peace", Chesney Memorial Gold Medal Lecture, October 03, 1973, printed in *RUSI Journal* (March 1974)
- Hybrid war - hybrid response?* [online]. NORTH ATLANTIC TREATY ORGANISATION REVIEW MAGAZINE. [cit. 2015-08-18]. Dostupné z: <http://www.nato.int/docu/review/2014/Russia-Ukraine-Nato-crisis/Russia-Ukraine-crisis-war/EN/index.htm>
- Hybrid Warfare and Challenges: Frank G. Hoffman* [online]. Washington D.C.: National Defense University, Institute of National Strategic Studies, 2009 [cit. 2015-07-11]. Dostupné z: smallwarsjournal.com/documents/jfqhoffman.pdf
- JACOBS, Andreas a Guillaume LASCONRAJIAS. NATO's Hybrid Flanks, Handling Unconventional Warfare in the South and the East. *NATO Defence College* [online]. [cit. 2015-08-01].
- Lisbon Summit Declaration* [online]. NORTH ATLANTIC TREATY ORGANISATION REVIEW. 2010, 20 November [cit. 2015-08-18]. Dostupné z: <http://www.nato.int/docu/review/2008/03/ART7/EN/index.htm>
- Military Scholar Frank Hoffman on the meaning of hybrid warfare. CENTRE FOR STRATEGIC & INTERNATIONAL AFFAIRS. *Strategic Insights and Bipartisan Policy Solutions* [online]. 2013, September 9 [cit. 2015-08-01]. Available at: <http://csis.org/blog/military-scholar-frank-hoffman-meaning-hybrid-warfare>
- MIKLAUCIC, Michael. NATO Countering the Hybrid Threat. *NATO: Allied Command Transformation* [online]. August 18. 2015 [cit. 2015-08-18]. Dostupné z: <http://www.act.nato.int/nato-countering-the-hybrid-threat>
- MORELAND, Scott. The Islamic State is a Hybrid Threat: Why does that Matter. *Small Wars Journal* [online]. [cit. 2015-08-01]. Dostupné z: smallwarsjournal.com/printpdf/18345
- PETERSON, Friis Arne a BINNENDIJK. *From Comprehensive Approach to Comprehensive Capability* [online]. NORTH ATLANTIC TREATY ORGANISATION REVIEW. [cit. 2015-08-18]. Dostupné z: <http://www.nato.int/docu/review/2008/03/ART7/EN/index.htm>



PINDJÁK, Peter. *NATO Review Magazine: Deterring hybrid warfare: a chance for NATO and the EU to work together?* [online]. [cit. 2015-08-18]. Dostupné z:

<http://www.nato.int/docu/review/2014/also-in-2014/Deterring-hybrid-warfare/EN/index.htm>

PURTON, Simon a . Why half of winning an Irregular War is agreeing on what it is.... *NATO, Allied Commnad Transformation: Future Capabilities, Research and Technology* [online]. [cit. 2015-08-01]. Dostupné z:

<http://webcache.googleusercontent.com/search?q=cache:XmtTGmKPxEJ:ismor.cds.cranfield.ac.uk/26th-symposium-2009/whats-in-a-name-...-that-which-we-call-a-rose-by-any-other-name-would-smell-as-sweet.-or-why-half-of-winning-an-irregular-war-is-agreeing-what-it-is../%40%40download/presentation/Purton.ppt+&cd=1&hl=en&ct=clnk&gl=cz>

ŠEREMET, Pavel. *Ukrajinska Pravda: Российский военный эксперт: У России все готово для новой атаки* [online]. [cit. 2015-08-18]. Dostupné z:

<http://www.pravda.com.ua/rus/articles/2015/07/10/7074026/>

Updated List of Tasks for the Implementation of the Comprehensive Approach Action Plan and the Lisbon Summit Decisions on the Comprehensive Approach, March 4, 2011, pages 1-10. [cit. 2015-08-18]. Dostupné z:

[https://jatl.act.nato.int/NATO/data/NATO/lm_data/lm_12820/999/objects/il_0_file_35471/20111130_NU_NATO-IS-NSG-PO\(2011\)0529-Action-Plan-Comprehensive-Approach.pdf](https://jatl.act.nato.int/NATO/data/NATO/lm_data/lm_12820/999/objects/il_0_file_35471/20111130_NU_NATO-IS-NSG-PO(2011)0529-Action-Plan-Comprehensive-Approach.pdf)

VAN PUYVELDE, Damien. Hybrid war – does it even exist? *NATO Review magazine* [online].

2015 [cit. 2015-08-18]. Dostupné z: <http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/>

Top partneři

Generální partner
Pražského studentského summitu



Hlavní partner
Modelu OSN



Hlavní partner Modelu NATO



Ministerstvo zahraničních věcí
České republiky

Univerzitní partner



Hlavní partner Modelu EU



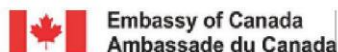
Partner jednání



Partner zahájení



Partneři Modelů



Mediální partneři

Hlavní mediální partner



Hlavní mediální partner



Mediální partner



Partner Chronicle



Za podpory





**Asociace
pro mezinárodní
otázky**
Association
for International
Affairs

Pražský studentský summit
projekt Asociace pro mezinárodní otázky