Hybrid Threats and Asymmetric Warfare:

What to do?

Stockholm 14-15 November, 2017

at

the Swedish Defence University, Stockholm, Sweden

Col (ret) Karl Hickman
Swedish Defence University
Dr Mikael Weissmann
Swedish Defence University
Dr Niklas Nilsson
Swedish Defence University
Dr Sascha-Dominik Bachman
Bournemouth University
Dr Håkan Gunneriusson
Swedish Defence University
Per Thunholm
Center for Asymmetric Threat Studies (CATS)

Conference proceeding

February 2018

Funded by:

RIKSBANKENS JUBILEUMSFOND
STIFTELSEN FÖR HUMANISTISK OCH SAMHÄLLSVETENSKAPLIG FORSKNING

Grant No: F16-1240:1

Co-funding has been received from the Swedish Armed Forces

The conference was organised by

Land Operations Section, Tactical Warfare Division, Dept. of Military Studies
Swedish Defence University (SEDU)

in collaboration with

Centre for Conflict, Rule of Law and Society, Bournemouth University

Center for Asymmetric Threat Studies (CATS), SEDU

Funded by:

RIKSBANKENS JUBILEUMSFOND
STIFTELSEN FÖR HUMANISTISK OCH SAMHÄLLSVETENSKAPLIG FORSKNING

Grant No: F16-1240:1

Co-funding has been received from the Swedish Armed Forces

Organising committee

Principal Investigator:
Dr. Mikael Weissmann, Assoc. Prof. in War Studies (military operations), Land Operations Section, SEDU.

Project Coordinator, Sweden:
Dr. Niklas Nilsson, Assistant Professor in War Studies, Land Operations Section, SEDU.

Project Coordinator, UK:
Dr. Sascha-Dominik Bachmann, Assoc. Prof. in Law, Bournemouth University, UK

Dr. Håkan Gunneriusson, Head of research & deputy head of Land Operations Section, SEDU

Per Thunholm, Senior Analyst at the Center for Asymmetric Threat Studies (CATS), SEDU

Hybrid Threats and Asymmetric Warfare: What to do?

The international security environment has seemingly departed from a post-cold war period of everlasting peace and has instead evolved into a volatile and increasingly grey area of war and peace. Security challenges arising from both hybrid wars and hybrid threats are high on security agendas in Sweden and Europe as well as internationally. However, despite the attention there is a lack of research that addresses how such "new" wars and threats should be handled. While studies do exist on specific issues, a comprehensive approach to how hybrid wars and threats are to be handled is still lacking. This is particularly the case when it comes to the sharing of experiences between states. This workshop constituted a first step towards developing such a comprehensive approach.

The workshop's aim was to be a bridge across disciplinary boundaries as well as between researchers and practitioners within and outside Sweden; integrating each group's extensive experiences and knowledge into a coherent whole. Besides producing and disseminating new knowledge, the intention of the workshop was to establish a foundation for long-term collaboration; the first step in the creation of a European Network on Hybrid Warfare Capabilities that can work across borders and link state of the art of research and practice.

Although mainly a scientific workshop, a number of practitioners were invited, with a mix of presentations by academics and practitioners. This was intended to foster innovative and reflective discussions across the academic-practitioner divide. The workshop also aimed to develop new ideas associated with hybrid threats/warfare in order to facilitate future cooperation

These proceedings include a summary of the key points made by the presenters, along with conclusions and policy recommendations derived from the ensuing discussions. Conference programme and a list of abstracts for the papers and presentations can be found in the appendix.

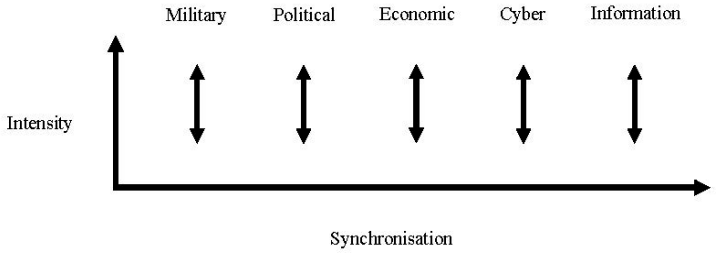
Summary of key points from the proceedings

SESSION 1: The role of the armed forces

Modelling hybrid warfare: a generic and holistic approach
Patrick Cullen, NUPI

- Academic analysis as to what constitutes Hybrid Warfare has yet to reach any consensus, although earlier definitions were too focused on non-state actors and kinetic means.

- There is general agreement that Hybrid Warfare does include both *multiple* and *synchronised* threats that aim to target state vulnerabilities at different levels of *intensity* over time:



Hybrid warfare in the mind of the Swedish officer: a multiple duality view of tactics and operational art
Michael Gustafson, SEDU

- Swedish Officer training is based on the 2015 curriculum and does not include Hybrid Warfare training.

- A survey of different officers demonstrated a wide variance in understanding of what Hybrid Warfare was and how relevant it should be for different parts of the Armed Forces.

- Perhaps most worryingly, none of those surveyed questioned whether the current model of Hybrid Warfare was correct.

Hybrid threats and warfare today and tomorrow: bringing the army (back) in

Mikael Weissmann, SEDU

- Hybrid Warfare blurs the distinction between civilian and combatant and both demands and permits all activities deemed necessary to achieve success. This could include full spectrum capabilities, including long distance weapons and Special Forces. The concept of strategic Key Terrain is also important, with increasingly potent Anti-Access Area Denial (A2AD) systems used to protect or threaten these areas.

- Whether the threat today can be described as peer vs peer or as superior vs inferior is, in the context of Sweden, dependent on whether Sweden operates alone or as part of a coalition.

- The role for the military in Hybrid Warfare will be varied, spanning the tactical to the strategic levels and including policing functions alongside more traditional military ones.

Mission Organised Constructs to counter Hybrid Threats

Scott Moreland, Naval Postgraduate School

- Hybrid Warfare is being used by various actors who do not believe in a rules based world order to achieve strategic symmetry with western states. They believe that they have both the opportunity and an imperative to do so.

- Hybrid Warfare capabilities include: the movement of conventional forces; nuclear force intimidation, economic and energy pressure; propaganda and disinformation, and cyber disruption and destabilisation. These capabilities

have been used as shaping instruments to create the conditions for conventional military intervention.

Session 1 Conclusions:

- *Rather than searching for consensus in defining and describing Hybrid Warfare, it is more fruitful to instead consider how Hybrid Warfare targets state vulnerabilities and how states should best organise themselves to meet the threat. Specifically:*
    - *States should conduct continual self-assessments to understand their current vulnerabilities.*
    - *States should enhance current threat assessments to understand how Hybrid Warfare capabilities are targeting those vulnerabilities (or not).*

SESSION 2: Cyber in a hybrid context

Theory of Strategic Culture – a tool to explain Russian cyber threat perception?

Martti J. Kari, University of Jyväskylä

- The determinants of Russian Strategic Culture include history, geopolitics, ideology and religion.
- Elements of Strategic Culture in Russia include:
    - Authoritarian Rule.
    - A sense of vulnerability.
    - Threat Perception.
    - A messianic mission to save Europe.

- A sense of being a Great Power.
- A Clausewitzian approach and a belief in the utility of force.
- The concept of being permanently in conflict.
- The use of asymmetric capabilities to conduct Hybrid Warfare.

- Russia believes that cyber threats to Russia are increasing and that they are not as technically capable as western states in this domain. This threat perception often leads to the establishment of offensive (hybrid) capabilities and activity (for example, perceived meddling in the Russian 2006 election may have led to the alleged Russian meddling in the US 2016 election).

Estonian defence league cyber unit as a hybrid national security actor

Rain Ottis, Tallinn University of Technology

- The Estonian Defence League was described as a useful tool in countering Hybrid Warfare threats.

- By drawing capability and talent from across Estonian society, whilst deliberately making assessment of the totality of that capability very difficult, the Estonian Defence League could serve as a useful example to other nations looking to expand their capabilities.

The silicon hat hacker: using reinforcement learning in hybrid warfare

Wayne Dalton, South African Military Academy

- Can we use machines with humans to reduce our vulnerability to hybrid threats? Machine learning, particularly the ability to analyse and learn from 'big data', has now matured to the point where machines can now outperform humans in a number of helpful tasks. This will:

- Allow humans to become more efficient and to be free to conduct more empathetic activities instead.
- Drive consensus faster in detecting and attributing Hybrid Warfare activity.
- Enhance cyber resilience by reducing cyber vulnerabilities.
- Offer the chance to overmatch Hybrid Warfare capabilities.

Session 2 Conclusions:

- *Individual states should adopt a progressive approach when building the capabilities necessary to counter hybrid threats, starting at the Joint level before moving to an Interagency and then Comprehensive Approach that also includes the private sector.*

- *In terms of states working together, multi-dimensional UN peacekeeping operations offer valuable lessons, including:*

    - *The importance of shared understanding, agreed Measures of Effectiveness and an agreed approach under unified command.*
    - *Demonstrating the proven ability of UN organisations such as the UNDP and the OCHA to interface and coordinate together.*
    - *The utility of having a Joint Mission Analysis Centre.*
    - *The utility of the EU Operations Centre as a possible coordinating body.*

- *If deterrence fails, then detection and attribution of Hybrid Warfare activity is extremely important in determining when and how states can respond.*

- *If action to counter Hybrid Warfare is taken to protect another state, then the role of the Host Nation as the sovereign actor cannot be underestimated. As sovereign nations acting within their territories, Host Nations will also be able to undertake activity that supporting states will probably not be able to.*

- *States should not underestimate and should instead seek to exploit the good will and significant capabilities within their civilian and private sectors.*

SESSION 3: Russia's neighbours

Cyber Component of Asymmetric Warfare: The Georgian Experience

Marina Malvenishvili, Chief specialist of development and foreign affairs section, Georgian Cyber Security Bureau, Ministry of Defence of Georgia

The August 2008 war against Georgia by the Russian Federation combined cyber and conventional attacks against governmental, media and financial institutions. Moreover, the increasing dependence on ICT clearly demonstrated that Georgia's national security could not be protected without the provision of cybersecurity.

In the period after 2008, Georgia started to develop these cybersecurity capabilities and improve its IT resilience through:

- Establishment of a relevant institutional framework, policy and legal base
- Creation of national CERT
- Establishment of a Cyber Security Bureau under the Ministry of Defence of Georgia
- Improved public awareness and the establishment of an educational base
- Capacity building of staff and the implementation of software and hardware solutions
- Establishment of international cooperation with NATO members and partner countries, as well as enhanced public-private partnership

Hybrid War and the Abkhazian Case

Kakhaber Esebua, Deputy Head of Defence System Analysis Division, Defence Planning and Development Department, Department of Defence of Georgia

- Russian "Gybrid Warfare" uses the normal Russian approach but with the elements used in different intensities. They are different portions of the same pie chart, used like a graphic equaliser but still with the traditional Russian aim of striking deeply over a broad front:

Dimensions	Actors	Actions (operations)
History and myth	Academia	Documentaries
Religion	Church	Historical Literature
Economy	State/Private	Local and International
Military	Army, Militia, Security	Pressure
Information	Service, Private Military	Direct, covert actions
Cyber	Companies	
	Media	
	Diplomatic	

SESSION 4: Russia and Hybrid Warfare

Key Note: Understanding Russia: military capability, reforms and threat perceptions

Daivis Petraitis, Independent Defence Analyst, Lithuania.

- The Russian Government arguably bases its thinking around four 'Russian truths':
    - 'War is eternal'.
    - War is fought by the state and not (just) the military of a state.
    - 'You fight your way, I fight mine'.
    - Victory does not require the capture or occupation of territory…'you have a territory, you have a problem … you have the king, you have the territory'.
- In completing its last 'Zapad' exercise this year, Russia was able to test all three of its strategic exercise objectives:
    - The conduct of a sudden attack.
    - The ability to defend and then terminate a conflict.
    - Wide scale state defence employing all the forces of the state; with the ability to escalate up to nuclear war in case of failure.

- Besides its existing brigades, Russia is also moving towards re-establishing a divisional level within its Armed Forces as a possible framework for the use of its combat brigades in larger scale operations. The new Russian Defence Management Centre is the main state command and control centre, allowing Russia the ability to analyse any situation and run operations continuously.

Asymmetric Measures in the Russian Security Strategy

Katri Pynnöniemi, University of Helsinki and National Defence University

- Some of the key concepts in the latest Russian National Security Strategy include sovereignty, independence and state and territorial integrity.

- Threats to Russian National Security include 'direct and indirect possible harm to the national interest'.

- From a Russian government perspective, the various colour revolutions are seen as regime changes organised by outside forces. The free flow of information championed by the West is also seen as information warfare and as part of a geopolitical struggle.

- A Russian asymmetric approach is characterised by flexibility and various asymmetric measures united by a common goal and actions, aimed at reducing the threat and eventually preventing it. The approach is defensive but includes both preventative and 'active' measures.

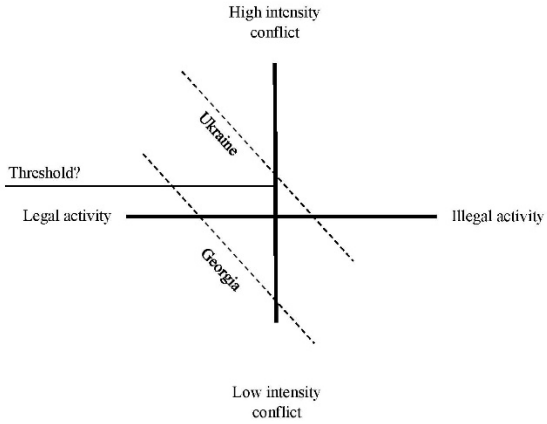
Hybrid Warfare – short or middle range theory?

Håkan Gunneriusson, SEDU

- Hybrid Warfare says more about the West than it does about Russia. Russia plays on the lack of desire on the part of western nations to engage in existential conflict due to their unwillingness to sacrifice their high standard of living.

- Western countries accept and even facilitate Russian 'tactical truths' because they *choose* not to call out disinformation as it would hurt their economic rationality. Meanwhile, Russia uses reflexive control to paint the West as weak.

- Where is the Western threshold in the context of conflict and legal/illegal activity?



-
- Russian disinformation is an interactive process that requires both the actor and the audience. Putin is an artist and we (the western states) are the consumer!

- In a sense, we are in an era of post-modern warfare, where war is only war if both sides say so. 'War' is therefore reduced to a matter of opinion.

The logic of Russian asymmetric warfare

Peter Mattson, SEDU

- Russia adopts asymmetric means because it has to.

- Its methods include technological means, will power, moral authority and organisational ability. The dimensions within which these methods operates vary:

    - Positive or negative.
    - Short or long duration.
    - Low or high risk.
    - Discrete or integrated.
    - Material or psychological.

Russian Hybrid Warfare in Georgia: lessons learned

Niklas Nilsson, SEDU

- Russia continues to exert economic leverage on Georgia today through the reopening of trade. Georgia is less vulnerable in the energy sector as 90 percent of the gas consumed comes from Azerbaijan.

- Politically, Russia can also use South Ossetia and Abkhazia as levers with Georgia. On the softer side, NGOs are also used by Russia to facilitate Russian-Georgian links.

- Russia aims to debunk the idea of Georgia as a beacon of democracy and to instead paint it as a traditional post-Soviet country. It also seeks to suggest that links with the West are damaging to Georgia. In particular, Russia plays on scepticism about whether the West will really 'deliver'.

- Currently, the picture in Georgia is one of increasing vulnerability. This may not be the reality but there is an increasing perception that this is the case, with increasing numbers susceptible to the messages described above.

Session 4 Conclusions:

- *Ukraine perhaps shows the limits of Russian Hybrid Warfare: once Western actors actively called out hybrid activity and named Russia as the aggressor, it became possible to apply real countermeasures (primarily in the form of economic sanctions).*

- *Seeking to 'fight' the results of Hybrid Warfare in a reactive manner plays to the strengths and not the weaknesses of the hybrid opponent. Instead, western nations should seek to retain the initiative and should continue to play to their very significant – perhaps even overwhelming - strengths (for example economic). They should also recognise and focus on the Centres of Gravity and vulnerabilities of hybrid opponents when countering the hybrid threat.*

- *Western nations should develop a more robust Command and Control structure to deal with transnational Hybrid Warfare. This should include partnering with organisations (like the EU) that have the ability to coordinate international responses to the threats, even if they remain dependent on national mechanisms for delivery.*

SESSION 5: Hybrid war and threats: the legal grey area

Key Note: Propaganda (as a component of hybrid warfare) and accountability

Anthony Paphiti, Brig (rtd) UK Army

- Propaganda is information, especially information of a biased or misleading nature. It is used to promote a political cause or point of view and to change perceptions. Misinformation is false or misleading information which is passed on in good faith. Disinformation is information known to be false and wilfully disseminated.

- Propaganda is an integral component of military deception and a critical tool of hybrid warfare. This fact is illustrated by recent developments in Libya, Syria and Iraq, as well as historical examples.

- A battle for the narrative is an essential component of hybrid warfare. Its objectives are multi-faceted: the "home" population; the enemy's military and the enemy's civilian population; and wider audiences of friendly nations from whom it is intended to garner international support.

- Media plays an increasingly important role in conveying government propaganda messages in pursuit of a military objective.

- Journalists can be embedded into military headquarters to control the information flow in return for force protection, coincidentally exploiting the journalistic pressure for a scoop.
- The pressure of 24-hour news channels and social media has arguably made it less likely that journalists will scrutinise unofficial sources and verify the facts contained in reports received from them. This, in turn, makes it easier to push out a false or misleading narrative through the media.

- In time of conflict, the media tend to support their government's line ("it's better to be viewed as a foot soldier for Bush than a spokeswoman for Al

Qaeda “, Irene Briganti, Fox News spokeswoman). The question is, how far should this go?

- To maintain credibility and integrity, media must scrutinize political statements and hold decision makers accountable.

- The legal provisions for countering propaganda are weak – the ICCPR prohibits propaganda for war, but most countries have entered reservations to this provision, citing freedom of expression. The Rome Statute of the International Criminal Court in practice only prohibits propaganda promoting genocide, crimes against humanity and war crimes. By contrast, this falls far short of the sort of provisions in domestic laws to cover e.g. hate speech and support for terrorism.

- There is a need for increased coordination between Western organizations on strategic communication.

- People frequently rely on misinformation/disinformation even after it has been retracted. This is a phenomenon known as “the continued-influence effect of misinformation”.

- People tend to continue to believe media statements that they have heard even when those statements have been retracted; ... unless people are suspicious about motives surrounding the events in question.

- The best way to counter propaganda is to tell the truth and demonstrate that this is indeed the case.

Beyond “passportisation”: when legal grey areas leave the door open to interventionism and rewriting post-1945 principles on international peace and security

Noelle Quenivet, UWE Bristol

- Russia’s practice of “passportization” is more than a policy – it is an important geopolitical tool for creating a buffer zone. In doing do, Russia is taking advantage of ambiguities in post-1945 international law by

reinterpreting legal grey areas and changing customary international law by practice.

- In Georgia, the provision of passports to residents in Abkhazia and South Ossetia allowed Russia to claim a right to protect nationals abroad and support these regions in declaring independence from Georgia. In other words, Russia has created legal 'facts', allowing it to claim the right to intervene in other states.

- Notably, however, these practices are not new and have been applied also by Western actors in a number of cases. This has attracted far less publicity in the West.

The use of force in an asymmetric conflict is not only limited to a soldier's right of self-defense

Mark Maxwell, Deputy Legal Counsel, US Africa Command

- Asymmetric warfare highlights the importance of legally distinguishing between self-defence and the scope of violence a soldier can use under the Law of Armed Conflict (LOAC).

- Self-defence is a natural law concept – we can protect our right to life at anytime, anywhere. States have different definitions of how broad this right of self-defence is, but it is based on direct threat and scopes and defines the right to use force by the soldier to negate the threat(s). When acting in self-defence, the legally authorized amount of force is limited.

- LOAC, however, allows states to assign soldiers the right to kill persons who do not present direct threats if identified as combatants. In asymmetric warfare, threats emerge among those who appear to be civilians. The concept of a civilian taking a "direct participation in hostilities" is important because it allows soldiers to target and kill those committing or preparing hostile or warlike acts against the State's war efforts.

- It is important to make this distinction because most liberal democracies cannot send troops into conflict with only the right of self-defence: soldiers need a clear understanding under the LOAC as to what status a civilian takes when that civilian is taking direct participation in hostiles. As one example, the LOAC defines proportionality very differently than its

definition within self-defence, giving the soldier much more discretion in using force against a civilian's hostile or warlike acts.

- Civilians directly participating in hostilities -- DPH -- can also be targeted under the concept of self-defence but this type of threat is limited to the soldier's person or that of the soldier's unit. However, violence inflicted based on the status assigned under LOAC versus that of self-defence profoundly changes the narrative of the conflict. Targeting someone under DPH is an offensive measure while self-defence is defensive in nature.

- It is important to understand the grey area between these concepts of law; and between the status of soldiers and the enemy combatants they are fighting, including civilians taking direct participation in hostilities.

Hybrid Warfare and Lawfare – the use of law as a weapon in the context of hybrid warfare

Sasha Bachmann, Bournemouth University

- The concept of hybrid warfare is not new as a concept of warfare but serves as a new platform that allows the discussion of threats beyond the concepts of war, peace and kinetic warfare. The definition of Hybrid warfare should remain open as a means to discuss other non-kinetic methods such as lawfare and information operations, both of which have the potential to become fully fledged new warfighting domains.
- Lawfare is a warfighting domain on its own. Lawfare refers to the use and/or abuse of the rule of law in a defensive and offensive capacity to achieve operational success without the need to employ kinetic methods of warfighting. There is no operational lawfare unit at NATO level but there are some member states which have such offensive/defensive capabilities.
- Russia is essentially mirroring the West when it comes to lawfare – arguing that they were responding to lawfare threats posed by the West.

Session 5 Conclusions:

- *Is there a need to address the problem of communicating with actors that will never recognize the law, such as Al Qaeda, ISIS and others? Should this be done and if so how?*

- *While these actors can be assigned the status of belligerents and thereby targetted, they exist worldwide and need to be addressed through broader approaches. We need to find ways to address the problem of sovereign states allowing violence on their territories according to different unified definitions of status. It is legally difficult to counter insurgent ideology. Some organizations can operate under the radar without consequences since hostile actions cannot be connected to them. Soldiers need training to know that they are exercising the status assigned to them by the state. Otherwise, we risk prolonging the war.*

SESSION 6: Total defence cooperation

Deterrence through resilience: NATO, the nations and the challenges of being prepared

Guillaume Lasconjarias, NATO Defence College

- We need to understand how NATO shifted from countering HW to enhance resilience. The shift from countering hybrid threats and warfare to enhancing resilience can nevertheless be questioned. From the Alliance perspective, how did we slowly evolve from hybrid threats to resilience, which at first glance seem to be very different from NATO's core tasks? The answer perhaps lies in the notion that the long-existing separation between defence and security has vanished, blurring responses and ensuring that they are not sufficiently holistic. For NATO, the countering of hybrid threats has largely been limited to "civilian preparedness".

- The journey from dealing with hybrid threats to instituting resilience mirrors the current evolution of NATO, and is also reflected by the EU's parallel course. The need to strengthen defence capabilities both at home and on Europe's frontline calls for a more comprehensive approach that has been more evident since 2014. Despite this, the main critique is that rather than going from strategic intention into the elaboration of ways and means, progress has been the other way around. First responses have been hampered by improvisation, with the emphasis on ad hoc solutions using existing conventional capabilities.

- If we really want to develop a deterrent against hybrid threats, we cannot only focus on "hardware" and "fixing" things. Because hybrid warfare entails a strong 'battle for the narrative', one of the future battlefields is our populations and elite's mindset and the harnessing of a new defensive spirit.

NATO and Hybrid Warfare
Hans Andersen, Allied Command Transformation, Virginia

- NATO: HW is not new. What is new is that it has moved from the operational to the strategic level, underpinned by new dimensions such as: globalization; complex geostrategic environment; advanced technologies (cyber); and information demand.
- Russia is always inside the western OODA-loop by being swift in its decision making. NATO needs an agreement between its member states to mitigate the organisation's long decision processes.

- **What is Hybrid Warfare? Characteristic include**:
    - Part of an overall **Strategic Plan**
    - Highly integrated (**synchronized**)
    - Combination of **conventional** and **unconventional** means
    - **Overt** and **covert** activities, military, paramilitary, irregular and civilian actors
    - Directed at an adversary's **vulnerabilities**
    - Complicating **decision making**
    - Across the full **DIMEFIL** spectrum
    - Creating **ambiguity** and **denial**
    - Both State and Non-State actor
    - Employed in conflict and confrontation that **fall short of** armed conflict.
    - **Globalization** and **technological advances** has led to increased vulnerabilities.
    - Increasingly sophisticated cyber-attacks
    - Far reaching **complex** p**ropaganda** and disinformation campaigns
    - Targeted and coordinated **political and economic pressure**.
    - **Moved to the Strategic Level**.

- The 3 pillars of NATO response vs hybrid: 1) Prepare, 2) Deter, 3) Defend.

- The EU is important for NATO as dealing with hybrid threats needs to be part of a collective effort.

Special Forces and hybrid scenarios: "Diplomat warriors" in small states and medium powers
Njord Wegge, NUPI

- Future warfare scenarios increasingly focus on how conventional and unconventional measures might be applied together. Special Operation Forces (SOF) have a particularly important role in different Hybrid Warfare scenarios in states of a small or middle power size.

- Small/medium size states like Norway and Sweden can, and should consider to develop SOF designated to counter warfare also in the political, societal and diplomatic domain. Such a development might demand the development of new legal mandates and involve parts of the emergency and contingency apparatus.

- Possibilities for life-time careers as SOF should be investigated and new career opportunities for the age 40+ should be developed.

Session 6 Conclusions:

- *Deterrence against hybrid threats requires a focus on the population's and elite's mindset and the harnessing of a new defensive spirit.*
- *NATO needs swifter coordination mechanisms to take control of the OODA-loop.*
- *Effective collaboration between EU and NATO is essential in efforts to counter hybrid threats.*
- *SOF should be considered an important component in a wide range of hybrid scenarios in small states.*
- *Find ways to make life-time careers as SOF possible.*

Appendix

Conference Programme

Tuesday, Nov 14

0840-0850	Introductory remarks, Col. Ronny Modigs, Head of the Department of Military Studies, Swedish Defence University
0850-0900	Welcome remarks by Mikael Weissmann, Swedish Defence University
SESSION 1: The role of the armed forces	
0900-1040	**Presentations:** 1. **Modelling hybrid warfare: a generic and holistic approach** Patrick Cullen, Norwegian Institute of International Affairs (NUPI) 2. **Hybrid warfare in the mind of the Swedish officer** Michael Gustafson, Swedish Defence University 3. **Hybrid threats and warfare today and tomorrow: bringing the army (back) in** Mikael Weissmann, Swedish Defence University 4. **Adapting mission organizational constructs to enhance civil-military coordination to counter hybrid threats** Scott Moreland, Center for Civil-Military Relations, Naval Postgraduate School, United States **Chair:** Håkan Gunneriusson
1040-1110	Coffee break

SESSION 2: Cyber in a hybrid context	
1110-1225	**Presentations:** 1. **Theory of strategic culture – a tool to explain Russian cyber threat perception?** Col. Martti J. Kari, University of Jyväskylä, Finland 2. **Estonian defence league cyber unit as a hybrid national security actor** Rain Ottis, Tallinn University of Technology, Estonia 3. **The silicon hat hacker: using reinforcement learning in hybrid warfare** Wayne Dalton, Stellenbosch University, South Africa **Chair:** Niklas Nilsson
1225-1325	Lunch
SESSION 3: Russia's neighbours	
1325-1425	*Cyber component of asymmetric warfare: the Georgian experience* Marina Malvenishvili, Chief specialist of development and foreign affairs section, Cyber Security Bureau, Ministry of Defence of Georgia **Hybrid war and the Abkhazian case** Kakhaber Esebua, Deputy chief of division, defence system analysis division, Defence Planning and Development Department, Ministry of Defence of Georgia **Discussion** **Chair:** Niklas Nilsson
1425-1455	Coffee break

SESSION 4: Russia and hybrid warfare	
1455-1720	**KEY NOTE: Understanding Russia: military capability, reforms and threat perceptions** Daivis Petraitis, Independent Defence Analyst, Lithuania **Presentations:** **1. Asymmetric measures in the Russian Security Strategy** Katri Pynnöniemi, University of Helsinki and National Defence University, Finland **2. Hybrid warfare – short or middle range theory?** Håkan Gunneriusson, Swedish Defence University **3. The logic of Russian asymmetric warfare** Peter Mattson, Swedish Defence University **4. Russian hybrid warfare in Georgia: lessons learned** Niklas Nilsson, Swedish Defence University **Chair:** Mikael Weissmann

Wednesday, Nov 15

SESSION 5: Hybrid War and Threats: the legal grey area	
0845-1045	**KEY NOTE: Propaganda (as a component of hybrid warfare) and accountability** Anthony Paphiti, Brig (rtd) UK Army. One of the founding members of the British Army Prosecuting Authority. **Presentations:**

	1. **Beyond Passportisation: when legal grey areas leave the door open to interventionism and rewriting post-1945 principles on international peace and security** Noelle Quenivet, UWE Bristol, United Kingdom 2. **The use of force in an asymmetric conflict is not only limited to a soldier's right of self-defense** Mark Maxwell, Deputy Legal Counsel, U.S. Africa Command, United States 3. **Hybrid warfare and lawfare – the use of law as a weapon in the context of hybrid warfare.** Sascha Dov Bachmann, Bornemouth University, United Kingdom **Chair:** Håkan Gunneriusson
1045-1115	Coffee break
SESSION 6: Total defence cooperation	
1115-1230	**Presentations:** 1. **NATO and Hybrid Warfare** Hans Andersen (LtCol), Allied Command Transformation, ACT, Virginia 2. **Deterrence through resilience: NATO, the nations and the**

	challenges of being prepared Guillaume Lasconjarias, NATO Defence College, Rome, Italy 3. **Special forces and hybrid scenarios: "Diplomat warriors" in small states and medium powers** Njord Wegge, Norwegian Institute of International Affairs (NUPI) **Chair:** Per Thunholm
1230-1245	**Conclusion**

Abstracts

Session 1

Modelling hybrid warfare: a generic and holistic approach

Patrick Cullen, Norwegian Institute of International Affairs (NUPI)

The verdict on hybrid warfare (HW) is clear. Despite an unsettled debate over the utility of the term, its conceptual boundaries and proper definition, a growing trans-Atlantic consensus from actors including NATO and the European Union is nevertheless in agreement that HW represents a security problem that must be addressed. This chapter, based on research conducted in the *Multinational Capability Development Campaign* (*MCDC*) *Countering Hybrid Warfare* project, moves beyond definitional debates to provide a security policy-oriented conceptual framework for understanding the whole of government/society security puzzle posed by HW. It discusses HW in generic terms by focusing on its exploitation of ambiguity and manipulation of its opponent's response thresholds, HW's emphasis on attacking its opponents at its seams (legal, organizational, etc.), and its creative use of non-military instruments of power. The chapter concludes with a discussion of the challenges HW poses for warning intelligence, and recommendations for mitigating these concerns.

Hybrid warfare in the mind of the Swedish officer: a multiple duality view of tactics and operational art

Michael Gustafson, Swedish Defence University

Understanding hybrid warfare is challenging because it comprises among other dimensions threats not belonging to the traditional military domain. Nevertheless, traditional military capabilities are said to exist in hybrid warfare, in parallel with irregular warfare: concepts such as guerrillas, terrorists, criminality and a dominant use of information and cyberwarfare. This article examines standpoints among Swedish officers studying at the two-year higher staff education regarding tactics and operational art in so-called hybrid warfare. The study is a sociological mapping of statements inspired by Pierre Bourdieu field theory, addressing the question of *"How can field theory explain contemporary military thought on tactics and operational art in hybrid warfare?"*.

The results show that military views on hybrid warfare can be distributed as a field with opposite opinions of the same challenge. This field can be expressed in the following way; a larger group of officers stated preferences for infantry unit concepts in a blended military and civilian context. A smaller group argued preferences to ranger unit concepts in a mainly military context. Even more varied thought was expressed by a smaller, group of officers, highlighting mechanized unit concepts in a regular warfare context. Finally another group preferred mechanized tactics and operation in a blended military and civilian context. Also with in each tactical type Different views also appeared within each tactical type. A multiple duality of views can thus be argued to exist in this field, with a potential of shaping different preconditions for collaboration, comprehensive approaches, leadership, planning and execution of operations.

Hybrid threats and warfare today and tomorrow: bringing the army (back) in

Mikael Weissmann, Swedish Defence University

The aim of this article is to outline what the hybrid/asymmetric threats and warfare scenarios are for Sweden today and tomorrow. It is argued that Sweden needs to prepare for and act against asymmetric warfare and hybrid warfare scenarios (alleged on-going and in the future, violent and nonviolent). The focus is on the role and challenges of the Swedish army, who are arguably a key target/actor hybrid warfare scenarios.

The paper will focus on 1) how the threats are perceived by the Swedish armed forces in general and the army in particular, 2) what can the army do, and 3) what should the army be able to do (and not do)? To make the picture as comprehensive as possible, the study combines analysis of official discourse in official documents, including doctrines and the ongoing public debates among pundits and experts, with qualitative and structured interviews with army officers. The focus in the interviews will be on operationalisation: what CAN the army do, what SHOULD the army be able to do, what should it NOT BE ABLE TO DO, and HOW does it get to where it want to be?

Adapting mission organizational constructs to enhance civil-military coordination to counter hybrid threats

Scott Moreland, Center for Civil-Military Relations, US Naval Postgraduate School

Hybrid threats exploit operational, informational, and legal ambiguities and vulnerabilities across all domains. National organizations and regional security consortiums, including NATO and the European Union, seek more effective responses to these increasingly difficult challenges. The *comprehensive approach* is an important conceptual framework for 'whole of society' security cooperation. Although not uniformly defined or perfectly understood, the basic principles of a comprehensive approach can be successfully applied to current and future operations involving military, civilian, and private sector components.

Hybrid threats depend on our perceived lack of agility, flexibility, and resolve. Contemporary missions - including peacekeeping, cyber security, and maritime security - have developed modestly effective models for the practical application of a comprehensive approach; these can be adapted and applied to counter hybrid threats. Through existing and evolving organizational models, collective capabilities must be better coordinated via mutual trust and understanding, enhanced interoperability, and unassailable transparency.

Session 2

Theory of strategic culture: a tool to explore russian cyber threat perception?

Col. Martti J. Kari, University of Jyväskylä, Finland

The interest in cyber warfare has generated the need for theoretical tools to research cyber threats and our responses to these threats. This paper reviews how the Cold War theories on the use of nuclear weapons, such as zero- sum game theory, theory of strategic culture and deterrence theory, can explain state behaviour in a cyber environment. I argue in this paper that the theory of strategic culture is suitable for exploring and explaining Russia's cyber threat perception. The theory of strategic culture seeks to identify factors which are characteristic of decision making and state practice; and to study how and why these factors influence the state´s decision making and practices. Factors influencing the strategic thinking of a state, i.e. determinants of strategic culture might for example be historical, geopolitical, religious or ideological. Elements of Russian strategic culture, including a sense of vulnerability, the idea of Russia as besieged fortress, the mythology of permanent war and technological inferiority can also be identified in Russia's cyber threat perception.

Estonian defence league cyber unit as a hybrid national security actor

Rain Ottis, Tallinn University of Technology, Estonia

Estonian national defence relies on a combination of a professional military, conscription-based reserve component and a volunteer organization called Defence League (*Kaitseliit*). In 2011 the Defence League gained a new capability in the form of the Cyber Unit (CU), which focuses on the cyber security aspects of national defence. While the term Hybrid Threat has received ominous and negative undertones in recent years, the Defence League in general and the CU in particular can serve as positive examples of Hybrid Actors in the context of national defence. This paper provides an overview of the role of the CU in Estonia and discusses its properties and capabilities against the backdrop of hybrid warfare.

The silicon hat hacker: using reinforcement learning in hybrid warfare

Wayne Dalton, Computer Information Systems Department, Faculty of Military Science, Stellenbosch University, South Africa

Computers today can learn things, on their own. 20 years ago, computers were capable of mastering human-like behaviour, but needed a lot of human expertise to guide their performance. Today, advances in machine learning have made it possible for computers to master very complex problems without relying on the encoding of human expertise into their algorithms. Recently, machine learning has successfully enabled computers to learn things that their human programmers themselves are unable to do; like discover new molecules that might lead to new drugs (Markoff, 2012).

Computers are also vulnerable to being exploited by hostile third-parties for a wide range of reasons, including cybercrime and cyber warfare. This endangers the safety and security of individuals, corporations and nation states in ways that are hard to protect against using conventional methods. Some companies have proverbially "set a thief to catch a thief" by employing large numbers of ethical hackers and other professionals to "pen test" their own critical infrastructure. Their goal is finding and fixing vulnerabilities in their systems before hostile attackers can exploit them.

This paper proposes that a computer can, in a self-sufficient and proactive manner, determine whether critical infrastructure is vulnerable to known cyber security exploits. The goal would be to remedy these exploits before anyone else can make use of them. The "*silicon-hat hacker*" is a machine-learning program that can explore and exploit vast quantities of data and consequently make high-confidence predictions on the existence of security exploits. This paper introduces the reader to reinforcement learning and how it might be used in cyber security. Finally, the paper will propose an architectural framework on how to accomplish this application of reinforcement learning to cyber security. In hybrid warfare, the complementary collaboration between Man and Machine will enhance capability and ultimately security and peace.

Session3

Cyber Component of Asymmetric Warfare: Georgian Experience Marina Malvenishvili, *Chief specialist of development and foreign affairs section, Cyber Security Bureau, Ministry of Defence of Georgia*

In August 2008, Russia perfectly demonstrated its doctrinal vision of warfare in the information age. Large-scale cyber-attacks against Georgia, conducted simultaneously with the kinetic war, presented the first application of the new "Russian hybrid" – mutually supporting efforts of information, cyber and kinetic operations. The Georgian case is significant in that it was the first instance where cyber means were used in direct connection with and in and support of major military operations as part of a state to state conventional war. This makes Russia's cyber-attacks against Georgia a unique case in the cybersecurity sphere. Russia, for the first time in history, tested Georgian cyber capabilities, using numerous attacks against both the public and private sectors. Importantly, the preparation for war started not in August, but months and even years earlier. Georgia has always been in Russia's "sphere of privileged interests".

Hybrid War and the Abkhazian Case

Kakhaber Esebua, Deputy chief of division, defence system analysis division, Defence Planning and Development Department, Ministry of Defence of Georgia

Hybrid Warfare has dozens of definitions and most of them are contradicting. The purpose of this paper is not to define the term in general but to talk about its Russian version. Hybrid Warfare is quite similar to the Russian notion of regular war; it consists of exactly the same components. The difference is that those components are employed in significantly different proportions and intensity. For a better understanding of Russian warfare we need to define (1) the **dimensions** (battlespaces) of Russian warfighting; (2) the **actors** employed; and (3) the **actions** (types of operations) conducted. Usually, the battlespaces of Russian warfare are: **History and Myths, Religion, Economy, Military, Information and Cyber**. War is fought in all those dimensions either simultaneously, in combinations, or alone, depending on the environment or the desired end state. Russian warfare is highly flexible and there are

no clear lines between its different forms – Hybrid and conventional. Hybrid is a comparably new type of Russian warfare, which is partially based on the concept of the Soviet Deep Battle. It means that Russia is operating in the entire depth of the enemy defence but not only in the military but other dimensions as well. The so-called Gerasimov Doctrine, which is widely seen as a bible of Russian Hybrid War is also talking about multidimensional war and underlines that this is not a Russian invention. Indeed, Hybrid War is neither entirely Russian, nor did it begin in Donbass. This paper analyses Russian Hybrid Warfare during the conflict in Abkhazia in the 1990s, which is still widely referred to as a separatist conflict. Yet in reality, it was an instance of Russian Hybrid Warfare against Georgia.

Session 4

Asymmetric measures in the Russian Security Strategy

Katri Pynnöniemi, University of Helsinki and National Defence University, Finland

Since the 2014 Crimean operation, Western military analysts have reviewed Russian military thinking in an attempt to both distinguish novel features and traditional patterns in the Russian ways of war. This research has drawn attention to concepts of 'nonlinearity', full-spectrum war, an 'asymmetric approach', and more recently to 'strategic deterrence'. Two of these concepts appear in the National Security Strategy, namely the *asymmetric approach* and *strategic deterrence*. In fact, the strategy ties these two concepts together in a way that tells a lot about the Russian approach to conflict. The 'asymmetric approach' has a rich history in Western military thought.[1] What I argue here is that its current usage in the Russian context can be traced to lessons drawn by the retired army general and the President of the Academy of Military Science, Makhmut Gareev after Russia's "five day war" with Georgia. The

[1] B. H. Liddlell Hart, *Strategy: Second Revised Edition*, NY: Penguin Books, 1991.

paper will discuss the evolution of this 'asymmetric approach' in the national security strategy (2009 and 2015).

Hybrid warfare – short or middle range theory?

Håkan Gunneriusson, Swedish Defence University

What is new about Russian hybrid warfare is that the West EU/NATO accepts the narrative that Russia is not at war in Ukraine. There are several reasons for this but one important thing to understand is that it is more about the West than about Russia. Russia is using reflexive control so that the West opts out from calling out Russia as a warring party in Ukraine. Why so? Because in a globalized Post-Cold War world there is no economic rationality in waging an existential war; and certainly not against a locally strong adversary that also possesses nuclear weapons and gives the impression of standing its ground if push comes to shove. Stating that Russia is at war with Ukraine would lead the West to act in accordance with the convention against War of Aggression. This would escalate the conflict and no one is interested in this outcome.

Yet there is more to this than Russia's relative strength and the West's focus on economic rationality. Each of these factors can be seen in the terms of Fernand Braudel as a *Courte Durée* (that Russia's relative military might will equal that of the West) and a *Moyenne Durée* (that the West's positivistic economic pursuit might one again become balanced by a more autonomous political rationality). However, there is further a current change in the perception of singular truth in society, which makes the interpretation of war and the relativisation of war easier. This is not a temporary (*Courte*) change.

The Logic of Russian Asymmetric Warfare

Peter Mattson, Swedish Defence University

Correlation of forces has always had a significant importance in Russian military thinking. In comparison to American military economy and power, Russia is not even close to being superior. Russia cannot meet the overwhelming American military capabilities with its own military weakness. This explains why the Russian military strategic logic includes asymmetric objectives, means and methods. Asymmetry is to do something different than one's adversaries in order to exploit an opponent´s weaknesses and to use one's own capabilities in a smart way to maximize own

strength. In Russia, all national power domains are coordinated under a military command in the National Defense Management Center (NDMC). The asymmetric approach can be used on the political-strategic, military-strategic and operational levels, or as a combination of all of them. Asymmetry can include different methods, technologies, values, organizations, time separation, or a combination of some of them. Strategic vulnerabilities usually include national leadership, the elite of the administration, as well as some strategic infrastructure.

Russian hybrid warfare in Georgia: lessons learned

Niklas Nilsson, Swedish Defence University

This paper shows how Russia has established a range of pressure points vis-à-vis Georgia that have incrementally circumscribed the Georgian government's political room for manoeuvre, both internationally and domestically. These pressure points have included: the use of military force or the threat thereof; leveraging geopolitical realities on the ground as means to exert diplomatic pressure; and the exploitation of economic dependencies. They have also encompassed subversive elements, including: co-optation and subversion aimed at inserting agents of influence in Georgia's political elite and society; cyber-attacks; and a concerted effort in the informational sphere to promote a narrative of Georgia that is favourable to Russian interests, both in the country itself as well as among its key partners in the West.

Georgia stands out as a particularly important case study of Russia's deployment of hybrid tactics. The country's longstanding conflict with Russia has made it a target of the full spectrum of hybrid tactics that Russia currently deploys in Ukraine and elsewhere. In fact, Georgia can be said to have functioned as a testing ground for many of these tactics, making Georgia's experience relevant far beyond the confined regional context.

Session 5

Propaganda (as a component of hybrid warfare) and accountability

Anthony Paphiti, Brig (rtd) UK Army.

From ancient Greece to Syria, the use of deception has been a key component of military strategy. Sun Tzu summed it up, in the Art of War, when he said that "All warfare is based on deception".

Within the realm of deception sits the concept of information operations or, more colloquially, propaganda. Of all the forms of hybrid warfare, propaganda ops are, perhaps, one of the most effective, as they may be used to change the perceptions of both friend and foe. In the former case, to win support for a cause. In the latter case, to confuse and sow seeds of doubt and fear.

In the Second World War, the allies used deception to great effect to protect the plan for the Normandy landings (operation OVERLORD) from being discovered, and employed a number of deception ops (Operation BODYGUARD) to disguise their real intent. As Churchill remarked at the Tehran Conference, in November 1943, "In wartime, truth is so precious that she should always be attended by a bodyguard of lies".

In more recent times, we have seen how disinformation and half-truths have won nations support for war in Iraq, Kosovo, Libya and Syria. On all of these occasions, the media and political establishment has played its part in disseminating the narrative. No one has been taken to task for some of the egregious claims made, for example, in the case of propaganda promoting WMD in Iraq.

In Syria, in the battle for East Aleppo, it became evident eventually that the reports being broadcast every evening by western media lacked independence, as their sources were Nusra jihadist activists within the militant-held part of the city. Images of children were used to win the sympathies of world viewers, and social media was employed to great effect to promote fake news or skew the truth. The truth had become a casualty. Propaganda had had a major impact on perceptions from outside Syria and wooed the famous and the powerful to the Islamists' cause: Islamists who were proscribed terrorist organizations listed by, inter alia, the United States and United Kingdom.

Where leaders, be they military or political, press a narrative for war, or journalists promote reports which they know or believe to be from a partisan and proscribed terrorist source, whether or not intentionally to support that biased narrative, is there any legal accountability? Does the law – international or domestic – make propaganda for war an offence, or is that a step too far and one which offends the right of freedom of expression and a free press?

The answer, it seems, is that there are few legal constraints on propaganda which falls short of incitement, or aiding and abetting etc. genocide, war crimes, or crimes against humanity, where the intent required in relation to a consequence of the narrative is that the person means to cause that consequence or is aware that it will occur in the ordinary course of events. In spite of the palpable bias in some quarters of the media, it is doubtful that any journalist has crossed that Rubicon. Which means that the use of propaganda remains a key tool of hybrid warfare.

Beyond passportisation: when legal grey areas leave the door open to interventionism and rewriting post-1945 principles on international peace and security

Noelle Quenivet, UWE Bristol, United Kingdom

By exploring Russia's activities from the fall of the Soviet Union until the present day, this paper examines how Russia uses nationality (understood in a wide sense of the term) as a political, economic, and cultural tool to justify expansionism. Russia, so it seems, is using grey areas in international law to implement a policy whose legal implications are in breach of the key principles of the UN Charter relating to international peace and security. It is argued that the policies and tools (e.g. conferral of nationality, support for the right of self-determination, protection of nationals abroad, etc.) developed and used by Russia are not necessarily unlawful *per se;* they can indeed in some instances be justified under international law as they fall within the grey areas of international law. That being said, the situations created as a result of this policy are often unlawful (e.g. recognition of a State that is part of the territory of another State, occupation and annexation, etc.). The paper concludes that Russia, by using its 'nationals' abroad and legal grey areas, is attempting to rewrite the rules carefully crafted post-1945, thereby allowing for interference in neighbouring States to become an established international custom.

The use of force in an asymmetric conflict is not only limited to a soldier's right of self-defense

Mark Maxwell, Deputy Legal Counsel, U.S. Africa Command, United States

There is a disturbing confusion among soldiers and their leaders in an asymmetric environment of what is the difference between the scope of authority to use lethal force under individual self-defence and the scope of authority to use lethal force under the law of armed conflict (LOAC). From the moment of a soldier's induction into the military, he or she is trained on the use of force in individual self-defence scenarios. Soldiers are also trained on what force can be used under LOAC. Although the two concepts – individual self-defence and LOAC -- might result in the use of force to kill or wound an enemy belligerent, they are two very different authorities. On the one hand, self-defence is tailored to protect the soldier from harm posed by a threat. The enemy's threat can be neutralized by a soldier's force that is proportional to the enemy threat; so if the enemy is threatening the soldier's life or limb, then lethal force would be appropriate and authorized. But if the threat is something lesser than life or limb, than the corresponding force should be lesser. Individual self-defence is defensive: again, it responds to a threat. The use of force under LOAC, on the other hand, is the State giving the soldier the right to be its agent so that the State can win the armed conflict. The State's grant of authority to the soldier under LOAC is to kill individuals who have been given the status of an enemy belligerent. Historically, an enemy belligerent is a member of the enemy's military. In the modern-day asymmetric environment, the enemy is often a civilian – or an individual pretending to be a civilian – who takes a direct participation in hostilities. The civilian steps out of his protective status as a civilian and decides to become an enemy belligerent by taking direct participation in hostilities; that is, he can be targeted under LOAC, even if he is not a threat to the individual soldier.

In many scenarios, the soldier is able to use lethal force under both under both concepts: individual self-defence and LOAC's civilians taking direct part in hostilities. But the degree of force under each concept is profoundly different. For example, a civilian takes part in hostilities by shooting at a soldier. After shooting, the civilian drops his weapon and starts to run away. There is real dispute if a soldier can shoot the civilian under the concept of individual self-defence; the threat posed by the civilian has evaporated. However, there is no issue under LOAC: the soldier can shoot the civilian because the civilian has taken the status of an enemy belligerent. So the degree of force might be different depending on which authority the soldier applies; but also, there are scenarios where both concepts do not overlap. For example, an aggrieved father of an innocent victim attacks a soldier out of remorse – the soldier's

right to respond falls squarely under individual self-defence. To the other extreme, a civilian helping to place an improvised explosive device (IED) in a road used by civilians is taking direct participation in hostilities. The intent of the IED is to prevent governance by funnelling civilians away from government-provided services. Friendly forces are not in the area, so individual self-defence is not applicable; however, LOAC concepts of targeting still apply and the civilian can be lethally targeted; it is part of the military's mission accomplishment to the win the conflict.

Understanding both concepts have three long-term advantages that will assist both the nation and military to navigate the use of force in these type of asymmetric conflicts. First, on a strategic level, it would help educate the Nation and its polity who are sending troops into harm's way that there are delineations between defensive measures, which a soldier always possesses under self-defence, and offensive measures, which will allows the soldier to win the nation's armed conflict. Second, on an operational level, it would compel militaries to train and educate their military force on the conceptual difference between the defensive use of force under individual self-defence – which is inherent - and the offensive use of force under LOAC – which is granted by the State to the individual soldier; this training will solidify the soldier's understanding of what force he or she is able to use under both concepts. In turn and thirdly, on a tactical level, this training would help the soldier understand both his limits and the expanse of his authority to use force on the battlefield.

Hybrid Warfare and Lawfare – the use of law as a weapon in the context of Hybrid Warfare.

Sascha Dov Bachmann, Bornemouth University, SEDU and CEMIS, Stellenbosch University

Hybrid Warfare is an old, multifaceted method of war where different actors, state and non-state, aim to reach their political or military goals by using a mix of conventional and non-conventional, or irregular, methods, as well as kinetic and non-kinetic means. Hybrid Warfare has become increasingly sophisticated and deadly (often involving cyberwarfare, propaganda and non-state adversary), and the methods used has a long history of successful employment. Similarly, Lawfare (the use of law as a weapon) is defined as "the strategy of using or misusing law as a substitute for traditional military means to achieve an operational objective". Lawfare therefore encompasses both affirmative as well as malicious use and has a goal of manipulating law by changing legal paradigms (from

https://www.academia.edu/34320799/Briefing_paper_Lawfare_in_Hybrid_Wars_The_21st_Century_Warfare).

Session 6

From Countering Hybrid Threats to Developing Resilience: New (shifting) Priorities for NATO?

Guillaume Lasconjarias, NATO Defence College, Rome, Italy

For NATO, the Ukraine crisis has been called a "wake-up call" redefining not just the relationships to Russia but the whole idea of living in a Europe free and at peace. To deal with security challenges emanating from its Eastern and Southern neighborhood, NATO has adopted the concept of "hybrid warfare", designing the combination of means that could undermine a government's and nation's ability to properly protect and rule over its population. Because these threats tackle domains that are outside the purely defensive area of responsibility, there's a need of a holistic response. For NATO, countering of hybrid threats has therefore been extended to increasing "civilian preparedness", packaged in the rejuvenated concept of resilience. For the Allies, it underlines the enduring ability to keep functioning in the face of internal or external change. This "resilience pledge" has been endorsed at the Warsaw summit in July 2016 which further proves the slow shift from countering hybrid threats and warfare to enhancing resilience.

Special forces and hybrid scenarios "Diplomat warriors" in small states and medium powers

Njord Wegge, Norwegian Institute of International Affairs (NUPI)

Future warfare scenarios increasingly focus on how conventional and unconventional measures might be applied together in what has been labelled "Hybrid Warfare". In such scenarios an opponent tries to reach his political goals through the synchronized use of different instruments of power tailored to vulnerabilities within the whole of society, while not going above what has traditionally been described as the threshold of war (e.g. a NATO article V scenario).

This research project investigates the potential role of Special Operation Forces (SOF) in Hybrid warfare scenarios in states of a small or middle power size. Based on research on the advantages of SOFs in future hybrid warfare scenarios, combined with insight into two relevant cases, Norway and Sweden, potential new roles of SOFs in Hybrid Threat scenarios will be analysed.

The Project concludes by first by supporting the idea that small/medium size states like Norway and Sweden can, and should, develop SOFs designated for warfare also in the political, societal and diplomatic domain; while secondly also pointing out that such a development might demand development of new legal mandates and a reorganization of parts of the emergency and contingency apparatus.