HYBRID WARS: THE 21st-CENTURY'S NEW THREATS TO GLOBAL PEACE AND SECURITY

Sascha-Dominik Bachmann,
Bournemouth University, UK[a]
Håkan Gunneriusson
Swedish Defence University[b]

Abstract

This article discusses a new form of war, 'hybrid war', with inclusion of aspects of 'cyber-terrorism' and 'cyber-war' against the backdrop of Russia's 'Ukrainian Spring' and the continuing threat posed by radical Islamist groups in Africa and the Middle East. It also discusses the findings of an on-going hybrid threat project by the Swedish Defence College. This interdisciplinary article predicts that military doctrines, traditional approaches to war and peace and their perceptions will have to change in the future.

Introduction

The so-called 'Jasmine Revolution' during the Arab Spring of 2011 challenged the political order in the Maghreb and the whole Middle East. While some of the protests led to actual regime changes and a move towards freedom and democracy – such as in Tunisia – events in other states in the region, such as Bahrain and Syria, had been less successful and saw the

Scientia Militaria, South African Journal of Military Studies, Vol 43, No. 1, 2015, pp. 77 – 98.
doi : 10.5787/43-1-1110

[a] Assessor Jur, LLM (Stel) LLD (UJ), Associate Professor in International Law (Bournemouth University, UK). Outside academics, he has served in various capacities as lieutenant colonel (army reserve), taking part in peacekeeping missions in operational and advisory capacities The author took part as NATO's Rule of Law Subject Matter Expert (SME) in NATO's Hybrid Threat Experiment of 2011 and in related workshops at NATO and national level.

[b] PhD in Modern History, Associate Professor in War Studies, head of research ground operative and tactical areas Department of Military Studies, War Studies Division, Land Operations Section, Swedish Defence University.

return of the 'old order' of autocratic governments. The collapse of Muammar Gaddafi's regime in Libya, the on-going civil unrest in Egypt between supporters of the ousted hard-line Muslim brotherhood and the military government, the on-going brutal Syrian conflict and the collapse of Iraq after the withdrawal of the USA have all significantly contributed to the proliferation and the ascent of evermore powerful and murderous terrorist groups and organisations across the region.

The use of 'cyber'[1] and kinetic responses to international terrorism have increasingly blurred the traditional distinction between war and peace. Such a distinction was replaced by the recognition of a notion of new, multi-modal threats, which have little in common with past examples of interstate aggression. These new threats to global peace and security seriously threaten our modern Western way of life within the context of the present 'steady-state' environment at home (and against the backdrop of the ongoing asymmetric conflicts in Afghanistan, Pakistan, Mali, Somalia, Kenya and Yemen). These new wars "along asymmetric lines of conflict"[2] constitute "a dichotomous choice between counterinsurgency and conventional war"[3] and challenge traditional concepts of war and peace.

This article[4] firstly reflects on the new notion of so-called 'hybrid threats' as a rather new threat definition and its (temporary) inclusion in the North Atlantic Treaty Organization's (NATO) new comprehensive defence approach with a reflection on the last Swedish experiment. Secondly, it discusses the use of 'cyber' in the context of 'hybrid threats' before it, thirdly, addresses some implications for military doctrine arising from such threats. The article concludes with a brief outlook on new dimensions of possible future threats to peace and security by highlighting the evolvement of the concept of 'hybrid threats' into 'hybrid war' by reflecting on security issues arising.

'Hybrid threats' as challenges to peace and security

The novel concept of hybrid threats first gained recognition when Hezbollah had some tangible military success against the Israeli Defense Forces (IDF) in Lebanon 2006 during the Second Lebanon War.[5] Ironically, the definition of 'hybrid' then was that a non-state actor showed military capabilities one originally only associated with state actors.[6] Multimodal, low-intensity, kinetic as well as non-kinetic threats to international peace and security include cyber war, asymmetric conflict scenarios, global terrorism, piracy, transnational organised crime, demographic challenges, resources security, retrenchment from globalisation and the proliferation of weapons of mass destruction. Such (multi-)modal threats have become known as 'hybrid threats'.[7] Recognised in NATO's Bi-Strategic Command

Capstone Concept of 2010, hybrid threats are defined as "those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives".[8] Having identified these threats, NATO undertook work on a comprehensive conceptual framework, as a Capstone Concept, which was to provide a legal framework for identifying and categorising such threats within the wider frame of possible multi-stakeholder responses. In 2011, NATO's Allied Command Transformation (ACT), supported by the US Joint Forces Command Joint Irregular Warfare Centre (USJFCOM JIWC) and the US National Defence University (NDU), conducted specialised workshops related to Assessing Emerging Security Challenges in the Globalised Environment (Countering Hybrid Threats [CHT]) Experiment'.[9] These workshops took place in Brussels (Belgium) and Tallinn (Estonia) and were aimed at identifying possible threats and at discussing some key implications when countering such risks and challenges. In essence, hybrid threats faced by NATO and its non-military partners require a comprehensive approach allowing a wide spectrum of responses, kinetic and non-kinetic, by military and non-military actors. In a 2011 report, NATO describes such threats as,

> Admittedly, hybrid threat is an umbrella term, encompassing a wide variety of existing adverse circumstances and actions, such as terrorism, migration, piracy, corruption, ethnic conflict etc. What is new, however, is the possibility of NATO facing the adaptive and systematic use of such means singularly and in combination by adversaries in pursuit of long-term political objectives, as opposed to their more random occurrence, driven by coincidental factors.[10]

The same report underlines that hybrid threats –

> … are not exclusively a tool of asymmetric or non-state actors, but can be applied by state and non-state actors alike. Their principal attraction from the point of view of a state actor is that they can be largely non-attributable, and therefore applied in situations where more overt action is ruled out for any number of reasons.

The findings of the two workshops were published in the ACT's final report and recommendations in 2011. However, due to a lack of financial resources in general and an absence of the political will to create the necessary 'smart defence' capabilities among its member states, NATO decided in June 2012 to cease work on CHT at its organisational level while encouraging its member states and associated NATO Excellence Centres to continue working on hybrid threats.

In 2012, the Swedish National Defence College as a Partnership for Peace (PfP) partner[11] conducted its own hybrid threat experiment.[12] The scenario dealt with a fictitious adversary in the East, not very dissimilar to Belorussia, except that it was an island kingdom in the Baltic Sea. The situation deteriorated to the point where neighbouring states were directly affected by a mix of conventional military and hybrid threats. More traditional threats arose from the attempt to sink a hijacked oil tanker in the middle of the sensitive maritime environment zone, launching a small group of Special Forces operatives (SFOs) in Swedish territory and hiring Somali pirates to hijack Swedish vessels off the Horn of Africa. The latter showed how a conflict could spread from being very local in one part of the world to involve remote hotspots in Africa. In this case, the problems at the Horn of Africa could legitimise actions and events, which originally had their roots in Northern Europe. The participants of the experiment acted as a committee of advisers for the Swedish government, and their individual roles represented their normal functions: from members of the armed forces and national support agencies to the university sphere, the pharmacological industry, banking and internet security. The experiment showed that existing and established standard operation procedures (SOPs) made responding to specific threats rather efficient. This was mostly due to already established command and control as well as communication and coordination assets and abilities. The experiment did however also show the existence of shortcomings when countering multi-modal threats due to the absence of a nationally defined comprehensive approach for a joint interagency approach. With SOPs in place and lacking a uniform command and control structure, it can also become harder to respond in a tailored and united way for government agencies, as all contributing agencies have their respective tasks and procedures. This lack of comprehensive joint action and coordination is highlighted by the fact that the government in the scenario did not have the authority to direct and control the work of subordinate but autonomous agencies.[13] The participants of the hybrid threat experiment did recognise that a coming hybrid conflict would lead to new levels of threat and response complexity and that there was a need for active, uniform and collective leadership beyond SOPs.[14] The participants identified as a weakness the lack of a comprehensive response and coordination between agencies such as the armed forces, the civil defence assets and other civilian actors, such as IT specialists and pharmaceutical experts.[15] With a shrinking defence budget, the downscaling of agencies and an obvious lack of civil society to accept the potential existence of such threat in the future, it seems unlikely that these shortcomings will be addressed in the near future.

In an African and Middle Eastern context, one cannot generalise as these states differ in terms of stability and strength regarding the capacities of their security assets. A state such as South Africa should and could rely very much on SOPs in order to have a constant high readiness against unsuspected threats. Other countries with weaker infrastructures and resources cannot expect their agencies to react swiftly when faced with ad hoc security challenges. The recommendation should then be to have very able actors (rather than structures, which the SOP demands) at key positions (at ministerial level and the level below) who can understand the threat and swiftly tailor a suitable response with the resources the state has at hand itself and with allied states. The latter is important in general and certainly so in Africa. As the borders have a colonial past, one should expect hybrid threats stemming from non-state actors (NSAs), which will eventually encompass a number of states.

Worrying – and of particular relevance in the context of hybrid threats – is the danger of proliferation of advanced weapon systems by NSAs associated with radical Islam, as for example the Islamic State of Iraq and al-Sham (ISIS) in Syria and Iraq as well as the increasing use of new technologies by NSAs. The last Israel–Gaza conflict highlights these developments: new technologically advanced rocket systems, supplied by Iran to their terrorist proxy Hamas, were used against Israel. The capability of the Fajr (Dawn) 5 rocket to reach both Tel Aviv and Jerusalem has been shown and has once more shown the vulnerability of Israel as a state when it comes to conventional, kinetic threats.

Against the backdrop of the on-going conflict in Ukraine and the classification of the conflict as a 'hybrid war' by Ukraine's national security chief,[16] NATO's decision to discontinue working on the hybrid concept as an organisational objective might turn out to have been made too early.[17]

The role of 'cyber-space' in hybrid threat scenarios in post-Cold War security

Despite NATO's failure to agree to a joint and comprehensive approach in countering hybrid threats, there is little doubt that "hybrid threats are here to stay".[18] Even a mainly conventional war will have a 'hybrid' element such as for example a 'cyber-attack', 'bio-hacking', and even 'nano-applications'.[19] Old threats, such as nuclear threats, can these days be reconsidered as within reach for state actors. Warnings have already been made that some university courses in nuclear technology might be in danger of being used by terrorist organisations.[20] Future attackers will rely increasingly on technological and scientific ways to execute their

operations, and one of the documented examples is the use of 'cyber-space' for carrying out or controlling 'hybrid threats'.

'Cyber-conflict' and 'cyber-war' serve as examples of the use of new technologies within the scope of hybrid threats. Cyber-war[21] basically refers to a sustained computer-based cyber-attack by a state (or NSA) against the IT infrastructure of a target state. An example of such hostile action taking place in the fifth dimension of warfare is the 2007 Russian attempt to virtually block out Estonia's internet infrastructure as a unilateral countermeasure and retribution for Estonia's removal of a WWII Soviet War Memorial from the centre of Tallinn.[22] Governmental and party websites as well as businesses were severely obstructed by this incident of cyber warfare, when Russian military operations were augmented by cyber operations against Georgia. This incident was followed by the employment of cyber measures in connection with the Russian military campaign in Georgia in 2008. Russia once again acted in a way which utilised the potential of the hybrid threat as a military strategy and modus operandi, this time in the Crimea.

Another example of how multi-modal threats, asymmetric terror and warfare are supplemented by terrorist (dis)information campaigns can be seen in the Israel–Gaza conflict. Then and now, Hamas has been employing tools and strategies of disinformation normally associated with clandestine psychological operations (PsyOps) of traditional military state actors, such as the sending of emails and text messages with hoax news updates as well as propaganda 'news flashes' sent to Israeli and non-Israeli email addresses and cell phones and the use of the internet to disseminate their propaganda.[23] During the eight days of conflict, text messages were sent which warned, "Gaza will turn into the graveyard of your soldiers and Tel Aviv will become a fireball."[24]

The (reported) use of a sophisticated computer worm to sabotage Iran's nuclear weapons programmes, called Stuxnet, by presumably Israel, has highlighted both the technical advancement, possibilities as well as potential of such new means of conducting hostile actions in the fifth dimension of warfare.[25] The continuing and intensifying employment of such cyber-attacks by China against the USA, NATO, the European Union and the rest of the world has led the USA to respond by establishing a central Cyber War Command, the United States Cyber Command (USCYBERCOM) in 2010[26] to "conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to their adversaries".[27] Following these developments – and perhaps supplementing the work of USCYBERCOM – NATO set up a special hybrid threat study group, which is studying possible responses to

such threats, the so-called NATO Transnet Network on Countering Hybrid Threats (CHT).[28] 'Cyber' in the context of armed conflict does not necessarily establish genuinely new categories of conflict per se; it rather constitutes another and improved 'tool' of warfare, namely 'cyber warfare'. The military will find new ways to conduct its operations by militarising 'cyber-space' as a force multiplier and operational capability enhancer, and will continue to operate at the tactical, operational or strategic level. The increasing hostile use of 'cyber-space' by NSAs to further their economic, political and other interests, and the present problem of clear accreditation of the originators of cyber activities make it increasingly hard to identify and counter such threats. Terrorist NSAs (or terrorist proxies of a state sponsor such as Iran and Syria) are increasingly using cyber capabilities in the wider sense to augment their attack capabilities. Apart from the above-mentioned use of 'cyber-space' by Hamas as a means of disinformation during the last Israel–Gaza conflict, ISIS (Islamic State in Iraq and the Levant) has been successful in utilising the 'cyber-space' for self-promotion and as a means of psychological warfare in its operations in Iraq and Syria.

One such example of the role of the internet and social media as an enhancer and force multiplier for terrorist activities can be found in the Mumbai attacks in India in 2008. Terrorists from Pakistan attacked the city, with a particular focus on the Taj Mahal Hotel.[29] Tactical intelligence during the raid was gathered from social media and the exploitation of existing mass media such as cable TV. Readily available home electronic equipment and cell phones were used as means of 'command and control'. Terrorist operatives on the ground were directed by their handlers in what can only be described as a classic war (situations) room in Pakistan. They were in permanent cell phone contact with the field operators in Mumbai, and were able to use both internet and major television channels for a situation update on the evolving situation on the ground, comparable to a situation report (SITREP) used by conventional armed forces. Live coverage of the attacks was made available by news channels, and as a novelty, by the social media, such as Flickr, Twitter and Facebook. The handlers of the operation 'data mined' and compiled this information in real time and communicated operation-relevant information directly to the terrorists through the use of smartphones.[30] What one could observe in the Mumbai example was the amazing readiness, availability and affordability of using new technologies for setting up an effective and workable system of 'command and control'.

This observation is a post-Cold War reality and a direct result of globalisation and technical advancement. The ways of accessing information in cyberspace are changing rapidly and are becoming increasingly hard to counter. One

recent example of an ingenious way of 'hacking' into otherwise protected sources involved the use of Google programs for inserting a so-called 'backdoor' Trojan for the purpose of data theft later.[31] Using the Google server, which already had access to the information of interest, hackers bypassed any firewall used by the 'target'. Another example of using an otherwise 'innocent' host like Google for carrying out 'cyber attacks' took place in late 2012 when hacker 'vandals' defaced Pakistan's Google domain along with other official Pakistan websites.[32] Other examples are the use of Thingbots – such as TVs, media players, routers and even a refrigerator – to send out spam in a coordinated and prolonged fashion.[33] While spam is mostly used for phishing activities, it also could be used for DDoS attacks (distributed denial of service attacks).

To summarise, one could state that the combination of new technology and the availability of these 'cyber'-supported or 'cyber'-led hybrid threats is what make these threats so potent. Command and control capabilities can be established in a relatively short time and without too much effort, and the media could be used for influencing the public opinion as a means of 'PsyOps', both at home and abroad. 'Cyber threats' in general strike at the core of modern warfighting by affecting command and control abilities, which have become vulnerable to such 'cyber attacks'.

Hybrid threats and military doctrines

Military doctrines provide guidance for the military logic of operational practice. It is therefore alarming that most Western military doctrines are apparently unprepared when it comes to hybrid threats. It seems as if NATO's inability and perhaps unwillingness to formulate a binding comprehensive NATO approach to hybrid threats is a testament to the perseverance of an overwhelmingly conservative military doctrinal approach. Time will tell whether this is to change. Latvia regards the 2014 events in Ukraine as clear evidence that NATO is unwilling and unable to provide protection at all if Russia was to repeat its Crimean operation in the Baltic States. A suggestion was made to change NATO's Washington Treaty so that Article 5 can deal with this kind of hybrid threats.[34] This is of course very unlikely as few of the NATO member states have anything at all to gain from military confrontation with Russia. It does however send a message to all states within the Russian interest sphere that there should be no doubt about Russia's strength and, correspondingly, NATO's weakness in this part of the world.

The failure of defining a NATO policy on countering hybrid threats is even more unfortunate given that the USA has a national military security strategy in

place, which recognises certain hybrid threats as part of new and existing threats to its national security.[35]

This failure may have its cause in a continuing Cold War-rooted psychology and thought among the political actors. During the Cold War, the world was locked in an intellectual doctrinal approach which viewed all conflicts in the context of the global ideological struggle coded by the laws and political paradigm of its time. Once the Cold War had come to an end in 1991, new national conflicts arose along once pacified conflict lines. This new era manifested itself in, for example, the bloody conflicts in the Balkans in the 1990s as a consequence of the breakup of the old communist regime, and the various conflicts on the territory of the former Soviet Union. While the Cold War was not necessarily only about the conflict between two opposing superpowers, nor exclusively about ideological confrontation, it nevertheless led to a strict division of the world and its conflicts into two major ideological spheres with only few exceptions, namely the spheres of the US-led West versus the Soviet-led East. This division made potential threats more foreseeable and even 'manageable'.

Since the end of the so-called 'Cold War', the world has changed dramatically and it is clear that this is also affecting military operations and doctrines. While the collapse of the Soviet Union and the Warsaw Pact in 1991 removed the original *raison d'être* of the Alliance, the prospect of having to repel a Soviet-led attack by the Warsaw Pact on Western Europe, the end of the Cold War also ended the existing balance of power after World War II and led to a 'proliferation' of armed conflicts around the globe. It seems as if the use of inter-state force has once more become 'acceptable',[36] as highlighted in the two 'War on Terrorism' campaigns, the Russian–Georgian conflict of the summer of 2008, the NATO-led Libyan Intervention of 2011, and Russia's recent operations in the Crimea and Ukraine proper. This potential for future interstate conflict adds to the above-discussed proliferation of 'hybrid conflict' where non-state actors have become very successful actors, aggressors respectively, in an inter- and intrastate conflict setting.

The end of the Cold War gave rise to a new way of thinking, which was no longer based solely on technological capabilities and/or sheer numerical superiority. It is possible to view the European postmodernism and the 'fourth generation warfare' following 9/11 as parallel tracks, with the latter challenging the paradigm of the Western positivistic materialism.[37] While military academics in the Western world do not lack warnings about the new challenges brought by these changes, it

will eventually be up to politicians to 'drive' new initiatives, a prospect often marred by 'Realpolitik', which will determine any policy in the end.

How does that affect military (and) security doctrines? Doctrinal changes for the military will depend on how the laws of war and the use of force will be shaped and this, in turn, will be shaped by the practice of those who should adhere to it. This has been highlighted by examples where legitimacy has been ignored on behalf of Realpolitik, as the operations in Afghanistan and Iraq show. What one can hope for in military doctrine is an integration of the rest of society in the common effort to protect itself from all forms of threats, conventional interstate aggression as well as new hybrid threats. One such example is the recent suggestion by the UN that states should and ought to be more proactive when it comes to fighting the use of the internet by terrorists.[38] Only society as a whole can protect itself, a task which is not limited to the military only, but which, on the other hand, cannot take on this huge task alone. An integration of the capabilities at interstate level, something NATO refers to as 'smart defence', and increased defence cooperation may be the only way forward to counter the multitude of ever-evolving threats in the future.

The capacity of NSAs to copy the command and control structures of conventional military has increased with the ready availability of mass-produced information technology and the possibility to tap into open sources for 'data mining'. These developments have changed the traditional view of asymmetric warfare, where an AK-47 and the insurgent's morale were traditionally the only and often most important factors in achieving victory. The asymmetric warfare concept used to be an idiom to describe war against opponents who also used to be weaker in terms of available weaponry and utilisation of technology.

Hybrid threats as such are not new threats; what is new is the recognition that such multi-modal threats command a 'holistic' approach, which combines traditional and non-traditional responses by state and NSAs as well, such as multinational companies. Responses to hybrid threats have to be proportionate and measured: from civil defence and police responses to counterinsurgency (COIN) and military measures. On the other hand, even NATO has something to win on the lack of codification. There will be a grey area of conflict where all actors can act – states, as well as non-states. Not that this seems to be the recipe for a bright future, but at least the possibilities for action will be there, even for Western states.

Hybrid threats and their possible responses challenge Carl von Clausewitz's dogma of war as constituting "a mere continuation of [state] politics by other means"[39] and might degrade the definition by Clausewitz into an early modern/modern *moyenne durée* definition of armed conflicts to use Fernand

Braudel's term,[40] namely that of a permanent state of war and conflict of varying intensity. NATO followed this rationale in its approach to countering hybrid threats, as they wanted a conventional threat element in the hybrid threat definition in order to ensure the operational usefulness of its conceptual approach. NATO's failure to formulate a comprehensive response strategy to asymmetric and 'hybrid' threats is an omission which will come at a cost in the future. International cooperation on capabilities is the *sine qua non* of future counter-strategies in order to respond to such threats and to be prepared for evolving new threats. This necessity of being prepared reflects on Sun-Tzu when he said, "Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win."[41]

Conclusion: From hybrid threats to hybrid war

Russia and Ukraine

Russia's offensive policy of territorial annexation (of the Crimea), the threat of using military force and the actual support of separatist groups in the Ukraine have left the West and NATO practically helpless to respond.[42] NATO seems unwilling to agree on a more robust response; thus, revealing a political division among its member states. This unwillingness can partly be explained by Europe's dependency on Russian gas supplies but also by the recognition of legal limitations and considerations, such as NATO's Article 5 (which only authorises the use of collective self-defence in cases of an attack on a NATO member state). It does not seem far-fetched to see the events of spring 2014 as the emergence of a new power balance in the region. As it was the case with the two historical examples, the overall outcome will be different from what was initially expected. The recent events have also brought Russia back into the region as the main player. Russia's (re-)annexation of the Crimea in April 2014 is a fait accompli and unlikely to be revised anytime, and the on-going support of separatist groups in the eastern parts of the Ukraine where the Russian-speaking minority is in the majority, such as Donetsk and Luhansk, has seen an increase in open military combat.[43] Ukraine is already a divided country, with fighting taking place along its ethnic lines. The break-up of the old Yugoslavia in the 1990s and its ensuing humanitarian catastrophe may serve as a stark reminder of things to come. Yet, it is the prospect of such a civil war that has also removed the necessity for open Russian military intervention. Russia has begun to fight the war by proxy, by using covert military operatives and/or mercenaries.[44] Reflecting these developments and having nothing further to gain from an invasion, Russia announced the temporary withdrawal of regular combat troops from the border in June.

After adopting a 'retro' USSR foreign policy,[45] Putin needed and found new strategic allies: in May 2014, he entered into a gas deal with China,[46] which has the potential not only to disrupt vital energy supply to Europe but also to question the emergence of a future long-term cooperation based on mutual economic interest and trust. Whether these developments herald the coming of a new 'cold war' remains to be seen. What is evident, though, is that the Cold War's 'Strategic Stability' dogma, which prevented any direct military confrontation between NATO and the Soviet-led Warsaw Pact, does not exist in the 21st century. New technologies in 'cyber-space'[47] and the use of 'new wars' along asymmetric lines of conflict – 'hybrid war' will see to it. Russia's operation has also shown that the hybrid approach can be adopted by states as well and not only by NSAs in an asymmetric context. In fact, it seems as if a resourceful state can wage hybrid war very effectively against opponents who lack the same resources. For example, one can look at the media advantage, which Russia had against Ukraine, a media advantage that is very much the backbone of the Russian new way of waging war. Once again, we have to remind ourselves that this media component is not a mere side-effect any more but the very core of post-industrial warfare.

The failure to agree on effective and far-reaching economic sanctions against Russia has also highlighted the weakness of the globalised economical system as such. But does the Crimean scenario teach something new about warfare? Some researchers have focused on the conventional part of the operation.[48] But it seems that the use of a term like 'semi-covert operations' in such texts is just a placeholder for a more accurate term such as 'hybrid war'.[49] Others have focused on what is new in Russian warfare, something about which Russia is very explicit. Among a host of features of the new war, there are some worrying elements we would like to consider: the non-declaration of war, the use of armed civilians, non-contact clashes like the blockade of military installations by 'protestors', the use of asymmetric and indirect methods, simultaneous battle on land, air, sea, and in the informational space, and the management of troops in a unified informational sphere.[50]

Why bother with all these methods, as Russia can be strong enough to take on whatever Russia is interested in within its sphere of interest? Seen from the perspective of hybrid warfare, it is all about muddling Clausewitz's dictum of war as the continuation of politics with other means: no war was to be declared officially and civilians were to be used instead of combatants. What we have seen in the Crimea is that Russia acted very much in this way, actually denying the existing of a state of war but defining military action in a holistic way with armed as well as unarmed civilians, supported by regular combat elements, doing the actual military

manoeuvre acting. The nature of the conflict remains undefined to a certain extent: war or civil unrest, interstate aggression or intrastate conflict. The latter was especially true in eastern Ukraine where the situation was very unclear when it came to whether Russia actually was active or not in an instrumental way. Against that backdrop, the following has become reality:

> With the advent of hybrid threats we will redefine what war is and we will most likely go into an era when we must get used to war and all its implications on society, there will possible be no difference between mission area and at home anymore, nor will the boundary between war and peace be well defined. 'Normality' will thus be redefined accordingly in a radical way.[51]

The international community and *jus ad bellum* are oriented towards limiting the possibilities of action in regular conflicts as we have come to know them in the 20th century. The hybrid logic of practice effectively amends the rules of war. Further, the practice of not acknowledging one's own actions makes the legal liability a difficult issue.

Africa

In Ukraine and the Crimea, we have seen Russia utilising the hybrid approach. This is a bit of a novelty as when the term emerged at first it was a way of describing a non-state approach, namely Hizbollah in Lebanon in 2006. One could argue whether the term 'hybrid threats' can still be applied on NSAs, if one lays claims, that what we have seen in the Ukraine, is a hybrid conflict between Ukraine and the Russian separatists. On the other hand, one has to look at the logic of practice in every conflict in order to determine what the indicators are. It is of course important to note whether an actor is a state or not.

But which kind of indicators do we find in Boko Haram and Al-Shabaab that we can see as rather new and within the discussion of hybrid threats? For radical Islamists, the religious and political representations of the West do not match the attitude of their own culture towards a non-material rationality breaking through in the West with the Enlightenment. The Western world and its secularisation serve more like a warning example for these groups. In any case, the rise of the radical Muslim movements can be seen as a reaction to modernism. Is an upsurge of Islam a form of neo-conservatism? This is an empirical question which will have to wait for now. But many of the insurgents in Boko Haram and Al-Shabaab come from

countries where there is little room for anything else than radicalisation when it comes to political room within which to manoeuvre.

Something that should be taken into consideration is that it is rather prejudiced to view all forms of religion as a quest for the past. It is possible and often the case, that religion defends the past. But it is also possible to imagine a progressive religious movement that, much like postmodernism, embraces and builds on – rather than repels – the movement that it reacts to, a concept which will be further explored later on when presenting examples of contemporary Islamist movements. Either way, both Islamism and postmodernism can be seen as reactions to a modernism that culminates in a globalisation and weakened national states. The trigger of this culmination was the end of the Cold War. Religion can provide existential comfort in an ever-changing world in a more striking way than postmodernism.

Which similarities between the events in the Crimea and the African theatres of terrorism can we then identify? Are there any similarities of Russia's conduct of operations and NSAs such as Boko Haram and Al-Shabaab? The most important similarity is the urge for media recognition, as proper media attention is crucial in the age of modern mass media communication. Is there something in common between the Crimean and Kenyan/Nigerian scenarios? Is it the same, and are both hybrid wars? In our perspective, 'hybrid threats' is a term which should be the litmus test of what future conflicts are to present to us as our immediate future reality. Yes, that is true, both scenarios use media as an integral part of warfare, not just as a collateral effect of the belligerent actions. But in the African radical Islamist cases, we see the same pattern as we have seen in, for example, Iraq both now under ISIS and under the insurgency against the USA. The difference in the use of media is fundamental. Radical Islamists use media as a 'force multiplier' for their terrorist agenda. In the Crimean case, we saw a plethora of misinformation: from the tactical level up to the Russian president, trying their best to communicate strategically that they were not involved in the operations while actually being caught red-handed. Even when three tanks crossed the border from Russia to Ukraine, none of the actors stated that they were the perpetrators and Ukraine did not push the point against Russia either.[52] The common denominator is the use of media in a very central role. The difference is that Boko Haram and Al-Shabaab try to translate tactical success into terror, while in the Crimean and Ukrainian examples, Russia tried the opposite while denying being an active agent. In the former case, *jus ad bellum* is ignored; in the latter, it is evaded.

This article was written with the intention of making 'hybrid threats' as a 21st-century security threat known to the wider audience despite NATO's decision not to adopt a comprehensive approach. This failure does not reduce the dangers of this category of global risks. Ongoing debate and academic engagement with the topic and rationale of 'hybrid threats', such as the Swedish experiment in 2012, will hopefully lead to further awareness and eventually preparedness. This submission concludes with a sobering prediction: it is the opinion of the authors that the present legal concepts on the use of military force, the *jus ad bellum*, have become relatively anachronistic and even partially outdated, something that will not suffice when dealing with the security threats and challenges of the 21st century. The authors predict that the emergence of hybrid threats and their recognition as potential threats to peace and security as such, the proliferation of low-threshold regional conflicts (such as the 2011 Libyan conflict, Syria and now Iraq), as well as continuing asymmetric warfare scenarios (such as Syria, Iraq, Afghanistan and Pakistan) will have a significant influence on the prevailing culture and prism of traditional military activity, which is still influenced by concepts from the previous century. With such a change of military doctrines, a change of legal paradigms will be inevitable: new adaptive means and methods of 'flexible responsiveness' through escalating levels of confrontation and deterrence will question the existing legal concept of the prohibition of the use of force with its limited exceptions, as envisaged under Articles 2(4) and 51 of the UN Charter and Article 5 of the NATO Treaty.[53] Future direct intervention in failed state scenarios will require flexibility in terms of choice of military assets and objectives. Future responses to multi-modal threats will always include the kinetic force option, directed against – most likely – NSAs. They will also affect our present concepts of the illegality of the use of force in international relations, as enshrined in Article 2(4) of the UN Charter with limited exceptions available under Article 51 of the UN Charter, namely individual and collective self-defence (*cf.* Article 5 of the NATO Treaty) as well as UN authorisation. Already today, the continuing use of UAVs (unmanned aerial vehicles, or drones) for 'targeted killing' operations effectively emphasises the legal challenges ahead: the ongoing 'kill' operations in the so-called 'tribal' areas of Waziristan/Pakistan are kinetic military operations, which demonstrate how quickly the critical threshold of an armed conflict can be reached and even surpassed. These operations clearly fall within the scope of the definition of 'armed conflict' by the International Criminal Tribunal for the former Yugoslavia in the appeal decision in *The Prosecutor v Dusko Tadic*[54] and therefore giving rise to the applicability of the norms of the so-called 'Law of Armed Conflict', the body of international humanitarian law governing conduct in war. The 'lawfulness' of such operations does, however, require the existence of either a mandate in terms of Article 51 of the

UN Charter (in the form of a United Nations Security Council [UNSC] Resolution authorising the use of force in an enforcement and peace enforcement operation context) or the existence of an illegal armed attack in order to exercise a right to national or state self-defence in terms of Article 51 of the UN Charter. Whether such military operations are within the scope of these categories remains open to discussion.

NATO's Strategic Concept of 2010 was aimed at prevention as well as deterrence in general and at developing a holistic or comprehensive approach to a variety of new conflict scenarios of multi-modal or hybrid threats, from kinetic combat operations to multi-stakeholder-based non-kinetic responses. Even with the failure to formulate a binding comprehensive approach to such threats at the supranational level, the findings of NATO's hybrid workshops have shown the significance of such threats and the need to respond in a flexible way.

New roles of states, their militaries and their politicians but also NSAs, such as multinational corporations and non-governmental organisation (NGOs), are needed. Geography as a term has already become obsolete as the 'war on terrorism' has shown: with its abstract categories of distinction into 'abroad', such as 'mission area', 'area of operations' and 'theatre of operation', and 'at home' having merged into one abstract universal 'battlefield' with an often-shifting geographical dimension. The dogma of 'flexible response', which has often been regarded as a tenet in military operational thinking and doctrine, has lost much of its meaning as a means of military force projection within the context of hybrid threats.

Hybrid threats pose not only security challenges but also legal ones and only time will tell how Western societies with their military will eventually adapt within their existing legal and operational frameworks.

Endnotes

[1] The term 'cyber' is used in a wider sense, referring to the use of computer technology and the internet for operations in the so-called fifth dimension; 'cyber operations', 'cyber war' and 'cyber attacks' are examples of such operations, depending on their intensity. For a classification of 'cyber conflicts', see Schmitt, M. "Classification of cyber conflict". *Journal of Conflict & Security Law* 17/2. 2012. 245–260.

[2] Lamp, N. "Conceptions of war and paradigms of compliance: The 'new war' challenge to international humanitarian law". *Journal of Conflict & Security Law* 16/2. 2011. 223.

[3] Hoffman, FG. "Hybrid threats: Reconceptualizing the evolving character of modern conflict". *Strategic Forum* 240. 2009. 1; also see Hoffman, FG. "Hybrid warfare and challenges". *Joint Forces Quarterly* 52. 1Q. 2009. 1–2; Hoffman, FG. "Hybrid vs. compound war: The Janus choice of modern war: Defining today's multifaceted conflict". *Armed Forces Journal* October 2009. 1–2.

[4] The authors have undertaken some prior work in that field, which reflects on various other aspects of the topic; *cf* Bachmann, S-D & Kemp, G. "Aggression as 'organized hypocrisy': How the war on terrorism and hybrid threats challenge the Nuremberg legacy". *Windsor Yearbook of Access to Justice* 30/1. 2012; Bachmann, S-D. "NATO's comprehensive approach to counter 21st century threats: Mapping the new frontier of global risk and crisis management". *Amicus Curiae* 88. 2011. 24–26; Bachmann, S-D & Gunneriusson, H. "Countering terrorism, asymmetric and hybrid threats: Defining comprehensive approach for 21st century threats to global risk and security". Swedish MoD – High Command, Internal Paper, releasable to the public some notions of this article were published prior in another context in "Terrorism and cyber attacks as hybrid threats: Defining a comprehensive approach for countering 21st century threats to global peace and security". *Journal for Terrorism and Security Analysis* 2014. 26–37.

[5] Hoffman, FG. *Conflict in the 21st century: The rise of hybrid wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007, 37.

[6] See for example Matthews, MM. "We were caught unprepared: The 2006 Hezbollah-Israeli War". The Long War Series Occasional Paper No 26. Fort Leavenworth, KS: US Army Combined Arms Center, Combat Studies Institute Press, 2008.

[7] (n 4) *supra*.

[8] *cf* BI-SC input for a new NATO Capstone Concept for the Military contribution to countering hybrid enclosure 1 to 1500/CPPCAM/FCR/10-270038 and 5000 FXX/0100/TT-0651/SER: NU0040, 25 August 2010.

[9] Miklaucic, M. "NATO countering the hybrid threat". 23 September 2011. <http://www.act.nato.int/nato-countering-the-hybrid-threat> Accessed on 7 May 2015.

10 For a thorough discussion of the concept of hybrid threats, see Sanden, J & Bachmann, S-D. "Countering hybrid eco-threats to global security under international law: The need for a comprehensive legal approach". *Liverpool Law Review* 33. 2013. 16. Copyright of the authors is acknowledged;

Aaronson, M, Diessen, S & De Kermabon, Y. "Nato countering the hybrid threat". PRISM 2/4. 2011. 115.

[11] A programme of practical bilateral cooperation between individual Euro-Atlantic partner countries and NATO.

[12] Försvarshögskolan. "Hur försvarar vi oss mot hybridhot?". 30 October 2012. <https://www.fhs.se/sv/nyheter/2012/hur-forsvarar-vi-oss-mot-hybridhot> Accessed on 27 January 2014.

[13] A recent example highlights the problem of failed coordination between the Secret Police, the National Defence Communication and Military Intelligence. The official in charge did leave office, as it was little to coordinate; Sverigesradio. "Spionchefer lämnar samarbetsorgan i protest". 4 November 2012. <http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5334446> Accessed on 27 January 2014.

[14] Feedback from scenario participants (answers to Gunneriusson's call for feedback by email): University representative 1; Medicine sphere representative 1; Armed Forces representative 3; Cyber security representative 1 and the Swedish Defence Materiel Administration representative 2.

[15] *Ibid.*

[16] Olearchyk, R & Buckley N. "Ukraine's security chief accuses Russia of waging 'hybrid war'". *The Financial Times*. <http://www.ft.com/cms/s/0/789b7110-e67b-11e3-9a20-00144feabdc0.html#axzz33DXeBUkR> Accessed on 6 May 2015.

[17] Bachmann, S-D. "Crimea and Ukraine 2014: A brief reflection on Russia's 'protective interventionism'". *Jurist*. <http://jurist.org/forum/2014/05/sascha-bachmann-ukraine-hybrid-threats.php> Accessed on 6 May 2015.

[18] SNDC Hybrid Threat Workshop, Swedish Armed Forces representative.

[19] On biohacking, see Ricks, D. "Dawn of the BioHackers". *Discover*. <http://discovermagazine.com/2011/oct/21-dawn-of-the-biohackers/article_view?b_start:int=2&-C=> Accessed on 27 January 2014 and Saenz, A. "Do it yourself biohacking". *SingularityHUB*. 28 April 2009. <http://singularityhub.com/2009/04/28/do-it-yourself-biohacking/> Accessed on 27 January 2014; Whalen, J. "In attics and closets, 'biohackers' discover their inner Frankenstein". *Wall Street Journal*. 9 May 2012. <http://online.wsj.com/article/SB124207326903607931.html> Accessed on 27 January 2014.

[20] *dn.se.* "Säpo: Högskoleutbildningar kan sprida kärnvapen". 10 April 2014. <http://www.dn.se/nyheter/sverige/sapo-hogskoleutbildningar-kan-sprida-karnvapen/> Accessed on 7 May 2015.

[21] See in general Döge, J. "Cyber warfare: Challenges for the applicability of the traditional laws of war regime" *Archiv des Völkerrechts* 48. 2010. 486.

[22] See Traynor, I. "Russian accused of unleashing cyberwar to disable Estonia". *The Guardian.* 17 May 2007. <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia> Accessed on 12 May 2015.

[23] Marcus, L. "Explosive new Arab music video: 'Strike a blow at Tel Aviv'". <http://www.jewishpress.com/special-features/israel-at-war-operation-amud-anan/explosive-new-arab-music-video-strike-a-blow-at-tel-aviv/2012/11/19/> Accessed on 15 May 2013.

[24] Jaber, H. "Hamas goes underground to avoid drones". *The Sunday Times.* 25 November 2012. 27.

[25] Halliday, J. "WikiLeaks: US advised to sabotage Iran nuclear sites by German thinktank". *The Guardian*. 18 January 2011. <http://www.theguardian.com/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear> Accessed on 6 May 2015; Kroft S. "Stuxnet: Computer worm opens new era of warfare". *60 minutes.* 4 June 2012. <http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/> Accessed on 6 May 2015; Williams, C. "Stuxnet: Cyber attack on Iran 'was carried out by Western powers and Israel'". *The Telegraph.* 21 January 2011. <http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html> Accessed on 6 May 2015.

[26] With the decision taken in 2009, and initial operational capability as of 2010, see US Strategic Command. "US Cyber Command". <http://www.stratcom.mil/factsheets/2/Cyber_Command/> Accessed on 6 May 2015.

[27] *Ibid.*

[28] See NATO. "Transformation Network". <https://transnet.act.nato.int/WISE/Transforma1/ACTIPT/JOUIPT> Accessed on 12 May 2015.

[29] Some of the following content derives from Swedish National Defence College sources, which are on file with the authors.

[30] Jagoindia. "Chilling phone transcripts of Mumbai terrorists with their Lashkar handlers". 7 January 2009. <http://islamicterrorism.wordpress.com/2009/01/07/chilling-phone-transcripts-of-mumbai-terrorists-with-their-lashkar-handlers/> Accessed on 27 January 2014.

[31] Paganini, P. "Malware hides C&C server communications using Google Docs function". 21 November 2012. <http://securityaffairs.co/wordpress/10454/malware/malware-hides-cc-server-communications-using-google-docs-function.html> Accessed on 27 January 2014.

[32] Baloch, F. "Cyber vandalism: Hackers deface Google Pakistan". *The Express Tribune*. 25 November 2012. <http://tribune.com.pk/story/470924/cyber-vandalism-hackers-deface-google-pakistan/> Accessed on 27 January 2014.

[33] *Proofpoint*. "Proofpoint Uncovers Internet of Things (IoT) Cyberattack". 16 January 2014. <https://www.proofpoint.com/us/proofpoint-uncovers-internet-things-iot-cyberattack> Accessed on 20 January 2014.

[34], Jānis. B. "Russia's new generation warfare in Ukraine: Implications for Latvian defense policy". Policy Paper No 02. Riga: National Defense Academy of Latvia, 2014, 9.

[35] See for example The White House. "The National Security Strategy of the United States of America" (hereafter NSS). September 2002. <http://nssarchive.us/NSSR/2002.pdf> Accessed on 15 May 2013, reaffirmed in NSS 2012.

[36] … and often questionable in terms of legality and legitimacy, and might qualify as the prohibited use of force in terms of Article 2(4) of the UN Charter. The planning and conducting of these operations would in the future fall within the scope of Article 8 *bis* of the ICC Statute (in its revised post-Kampala 2011 version and coming into force only after 2017, potentially leading to individual criminal responsibility).

[37] The ideas of the extreme Wahhabism (the religious fundament advocated by al-Qaeda), that man should live in the same technological conditions as Muhammad, is easily linked to the ideas behind fourth-generation warfare.

[38] UNODC. "The use of the internet for terrorist purposes". <http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf> 13 Accessed on 27 January 2014.

[39] Clausewitz, C. *On war* (Book I), transl Graham, JJ. London: N Trübner, 1873, 24; Braudel, F. *La Méditerranée et le monde méditerranéen à l'époque de Philippe* (Vol. II). Paris: Lib. A. Colin, 1949.

[40] *Ibid.*

[41] Sun-Tzu. *The art of war* (transl L Giles). New York: Barnes & Noble, 2012, Chapter 4.

[42] See Bachmann, S-D. "Russia's 'spring' of 2014". *OUPblog.* 9 June 2014. <http://blog.oup.com/2014/06/russia-putin-hybrid-war-nato/> Accessed on 6 May 2015 (copyright of OUP fully acknowledged).

[43] Varenytsia, I. "Fighting in Eastern Ukraine rages on overnight despite talks". *Time*. 14 April 2015. <http://time.com/3820764/ukraine-donetsk-russia-fighting-rebels-belarus-putin-shyrokyne/> Accessed on 7 May 2015.

[44] Roth, A & Tavernise, S. "Russian revealed among Ukraine fighters". *The New York Times.* 27 May 2014. <http://www.nytimes.com/2014/05/28/world/europe/ukraine.html?_r=0> Accessed on 7 May 2015.

[45] Patel, A. "Russia with Crimea: Back in the USSR". *Rusi*. 9 May 2014. <https://www.rusi.org/analysis/commentary/ref:C536CCA853F88D/#.U4irgkp-58E> Accessed on 7 May 2015.

[46] Lain, S. "Russia's gas deal with China underlines the risks to Europe's energy security". *The Guardian*. 26 May 2014. <http://www.theguardian.com/commentisfree/2014/may/26/russia-gas-deal-china-europe-energy-security-danger> Accessed on 7 May 2015.

[47] Roscini M. "Is there a "cyber war" between Ukraine and Russia?". <http://blog.oup.com/2014/03/is-there-a-cyber-war-between-ukraine-and-russia-pil/> Accessed on 6 May 2015.

[48] Sutyagin, I & Clarke, M. "Ukraine military dispositions: The military ticks up while the clock ticks down". Briefing Paper. *RUSI.* April 2014. <http://www.rusi.org/downloads/assets/UKRANIANMILITARYDISPOSITIONS_RUSIBRIEFING.pdf> Accessed on 6 May 2014; Norberg, J. "The use of Russia's military in the Crimean crisis". *The Global Think Tank*. 14 March 2013; Norberg J. "The use of Russia's military in the Crimean Crisis". *Carnegie Endowment for International Peace.* 13 March 2014. <http://carnegieendowment.org/2014/03/13/use-of-russia-s-military-in-crimean-crisis/h3k5?reloadFlag=1> Accessed on 6 May 2015.

[49] Norberg, J & Westerlund, F. "Russia and Ukraine: Military-strategic options, and possible risks, for Moscow". *IISS*. 7 April 2014. <https://www.iiss.org/en/militarybalanceblog/blogsections/2014-3bea/april-7347/russia-and-ukraine-3b92> Accessed on 6 May 2015.

[50] Changes in the Character of Armed Conflict According to General Valery Gerasimov, Chief of the Russian General Staff, listed in Jānis *op. cit.*, p. 4

[51] Gunneriusson, H. "Nothing is taken serious until it gets serious". *Defence Against Terrorism Review* IV/7. 2012.

[52] Moore, J. "Ukraine crisis: Three Russian tanks cross shared border". *International Business Times*. <http://www.ibtimes.co.uk/ukraine-crisis-three-russian-tanks-cross-shared-border-1452424> Accessed on 6 May 2015.

[53] See Bachmann & Kemp *op. cit*., n 4, for a detailed overview of possible legal challenges in the context of kinetic responses to hybrid threats.

[54] IT-94-1-A, 105 *ILR* 419,488.