

*Scientia Militaria, South African
Journal of Military Studies*, Vol
43, No. 1, 2015, pp. 77 – 98.

Muammar

-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.

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

In 2012, the Swedish National Defence College as a Partnership for Peace (PfP) partner¹¹ 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

such threats, the so-called NATO Transnet Network on Countering Hybrid Threats (CHT).²⁸

genuinely new categories of conflict per se; it rather constitutes another and
 warfare,
 to conduct its operations by militarising -space
 operational capability enhancer, and will continue to operate at the tactical,
 operational or strategic level. The increasing hostile use of cyber- 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
 -space Gaza
 conflict, ISIS (Islamic State in Iraq and the Levant) has been successful in utilising
 the cyber- 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 . 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
 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
 command and .

This observation is a post-Cold War reality and a direct result of
 globalisation and technical advancement. The ways of accessing information 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

Since the end of the so- , 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* 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

³⁶ as highlighted in

Georgian conflict of the summer of 2008, the NATO-led Libyan Intervention of 2011, the Crimea and Ukraine proper. This potential for future interstate conflict adds to the above- -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.

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

by _____, a prospect often marred
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 _____, 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

_____ tional 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-_____, 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.

³⁹ _____ and might degrade the definition by Clausewitz into an early modern/modern *moyenne durée* definition of armed conflicts to use Fernand

,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

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

,⁴⁵ Putin needed and found new strategic allies: in May 2014, he entered into a gas deal with China,⁴⁶ which has the

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 possibly be no difference between mission area and at home anymore, nor will the boundary

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 hybrid warfare is 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 concept can 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

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 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 integrale

This article was written with the intention of making as a
21st-
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

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.

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

-
- 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. 4 November 2012. <<http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5334446>> Accessed on 27 January 2014.
- ¹⁴ 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. *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- brief r protective i *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 yourself b. *SingularityHUB*. 28 April 2009. <<http://singularityhub.com/2009/04/28/do-it-yourself-biohacking/>>

²⁰ *dn.se*. Säpo: Högscoleutbildningar kan sprida kärnvapen

³⁰ Chilling phone transcripts of Mumbai terrorists with their Lashkar 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

Academy of

Latvia, 2014, 9.

³⁵

<<http://nssarchive.us/NSSR/2002.pdf>> Accessed on 15 May 2013, reaffirmed in NSS 2012.

³⁶ 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

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

⁴² See Bachmann, S- *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 rages on overnight despite t
Time

51

Defence Against

Terrorism Review IV/7. 2012.

52 Moore, crisis: Three Russian tanks cross shared b . *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.