SPRING 2014
9th EDITION

The Journal on Terrorism and Security Analysis

JTSA

SATSA
STUDENT ASSOCIATION ON
TERRORISM & SECURITY ANALYSIS

Terrorism and Cyber Attacks as Hybrid Threats: Defining a Comprehensive Approach for Countering 21st Century Threats to Global Peace and Security

By Dr. Sascha-Dominik Bachmann and
Dr. Håkan Gunneriusson

Abstract

Multimodal, kinetic and non-kinetic threats to international peace and security, including cyber-attacks, low intensity asymmetric conflict scenarios, global terrorism, piracy, transnational organized crime, resources security, retrenchment from globalization and the proliferation of weapons of mass destruction, were identified by NATO as 'hybrid threats,' which state actors are ill-equipped to handle. This interdisciplinary article predicts that military doctrines, traditional concepts of war and peace, and legal perceptions will be challenged by the nature of these threats.

Introduction and Overview

The drastic global changes since the end of the Cold War had a permanent impact on military operations and doctrine. The last quarter century saw state actors adopt several distinct approaches to dealing with threats. The collapse of the Soviet Union in 1991 removed the original *raison d'etre* of the Warsaw Pact: the specter of repelling a Soviet attack on the West through the Fulda gap in Germany.[1] The end of the balance of power that existed after the Second World War led to a proliferation of armed conflicts around the globe. Recently, it appeared the global community condoned the use of inter-state force highlighted by the 'War on Terrorism', the Russian-Georgian conflict of summer 2008, and the Libyan Intervention of 2011. However, if any state or non-state actor wanted to target a Western European state by using conventional means of warfare, they would face significant risks of retaliation.

New potential threats arose from both state and non-state actors with the advent of new technologies, the growth of the Internet, and the proliferation of privately owned computer hardware. These increasingly sophisticated threats include the use of cyber[2] as a means of warfare and have further blurred the traditional distinction between war and peace. Such a distinction was replaced by the recognition of the need to counter 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 the modern Western way of life within the context of the present 'steady state' environment at home (and before the backdrop of the ongoing asymmetric conflicts in Afghanistan, Pakistan, Mali, Somalia, and Yemen).

This article aims to introduce this form of security threat under inclusion of aspects of cyber-terrorism and cyber-warfare. It presents the findings of an ongoing hybrid threat experiment that was undertaken by the Swedish National Defence College. It briefly reflects on how hybrid yhreats may impact on military thinking in the developed world. Additionally, it argues that the 2010 ICC Review Conference in Kampala's codification of the crime of aggression does not necessarily reflect these new forms of 21st century threats.

This article[3] consists of three parts: First, it introduces the notion of 'hybrid threats' as a new threat definition and its (at least temporary) inclusion in NATO's new comprehensive defense approach with a reflection on the use of cyber capabilities. Second, inclusion is highlighted at the

1 Referring to the German lowlands between Frankfurt am Main and the former East German border, which was regarded as the most likely terrain for a Soviet led attack by the Warsaw Pact.

2 The term "cyber" is used in a wider sense, referring to the use of computer technology and the Internet for operations outside the four traditional arenas of land, sea, air, and space. Cyber operations, cyber war, and cyber-attacks are examples of such operations. For a classification of cyber conflicts, see Michael Schmitt, "Classification of Cyber Conflict," 17 (2) JCSL (2012), 245-260.

3 The authors have undertaken some prior work in that field: See Sascha-Dominik Bachmann and Gerhard Kemp "Aggression as 'Organized Hypocrisy' – How the War on Terrorism And Hybrid Threats Challenge The Nuremberg Legacy," *Windsor Yearbook of Access to Justice* (2012); Sascha Bachmann "NATO's Comprehensive Approach to Counter 21st Century Threats – Mapping The New Frontier of Global Risk and Crisis Management, 88 *Amicus Curiae* 2012; and Sascha Bachmann and Håkan Gunneriusson "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.

multinational level through case study examples of NATO and UN initiatives and inclusion is examined at the state level through a case study of the Swedish National Defense College. Third, it addresses potential implications for military doctrine arising from hybrid threats and the associated legal consequences. The article concludes with a brief outlook on the new dimensions of possible future threats to peace and security as challenges to our present concept of war and peace, and then reflects on possible responses.

New Security Challenges: *The Emergence of 'Hybrid Threats' as Challenges to Peace and Security*

Multimodal, low intensity, kinetic as well as non-kinetic threats to international peace and security including cyber war, asymmetric conflict scenarios, global terrorism, piracy, transnational organized crime, demographic challenges, resource security, retrenchment from globalization, and the proliferation of weapons of mass destruction were identified and labelled by NATO as 'Hybrid Threats', as threats 'posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives'.[4]

Having identified these threats, NATO undertook work on a comprehensive conceptual framework, a Capstone Concept, which was to provide a legal framework for identifying and categorizing such threats within the wider frame of possible multi-stakeholder responses. In 2011, NATO's Allied Command Transformation (ACT) supported by the U.S. Joint Forces Command Joint Irregular Warfare Centre (USJFCOM JIWC) and the U.S. National Defence University (NDU) conducted specialized workshops related to 'Assessing Emerging Security Challenges in the Globalized Environment (Countering Hybrid Threats [CHT]) Experiment'.[5] These workshops took place in Brussels, Belgium, and Tallinn, Estonia, and aimed at identifying possible threats and to discuss some key implications when countering such risks and challenges. The findings of the workshops were published in the ACT's final report and recommendations in 2011.[6]

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.[7] Such a comprehensive response will have to be in partnership with other stakeholders such as international and regional organizations as well as representatives of business and commerce.[8] However, due to a lack of financial resources in general, and an absence of the political will to create necessary 'smart defense' capabilities among its member states, NATO decided in June 2012 to cease work on CHT at its organizational level while encouraging its member states and associated NATO Excellence Centers to continue working on hybrid threats.

Case Studies

Prior to the ACT's report and recommendations, NATO held a summit in Lisbon, Portugal. The participants discussed general challenges to the alliance's present role in the face of falling national defense budgets. It was at this summit that the Lisbon Summit Declaration of 2010 was drafted. New threat scenarios were addressed in the Declaration, threats which differed from traditional 'state on state' armed conflict scenarios, and were discussed in reaction to increased globalization.[9] As a consequence, NATO adopted a new Strategic Concept. The Strategic Concept set out its vision for the immediate future, and called for "NATO's

4 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, dated 25 August 2010.

5 See NATO's *Transnet* network on Countering Hybrid Threats (CHT), *https://transnet.act.nato.int/WISE/Transforma1/ACTIPT/JOUIPT.*

6 Assessing Emerging Security Challeges in the Globalized Environment," *NATO Allied Command Transformation, https://transnet.act.nato.int/WISE/CHTIPT/Newsletter/JanuaryCHT/file/_WFS/CHT%20Newsletter%20-%20Edition%201%20-%20final.pdf.*

7 See "Updated List of Tasks for the Implementation of the Comprehensive Approach Action Plan and the Lisbon Summit Decisions on the Comprehensive Approach," March 4, 2011, 1-10, *https://jadl.act.nato.int/NATO/data/NATO/lm_data/lm_12820/999/objects/il_0_file_35471/20111130_NU_NATO-IS-NSG-PO(2011)0529-Action-Plan-Comprehensive-Approach.pdf.*

8 Michael Miklaucic, "NATO Countering the Hybrid Threat," September 23, 2011, *http://www.act.nato.int/multimedia/archive/41%E2%80%90top%E2%80%90headlines/747%E2%80%90nato%E2%80%90countering%E2%80%90the%E2%80%90hybrid%E2%80%90threat.*

9 North Atlantic Treaty Organization Public Diplomacy Division, "Lisbon Summit Declaration," last modified November 20, 2010, *http://www.nato.int/nato_static/assets/pdf/pdf_2010_11/2010_11_11de1db9b73c4f9bbfb52b2c94722eac_pr_cp_2010_0155_eng-summit_lisbon.pdf.*

evolution, so that it [could continue] to be effective in a changing world, against new threats, with new capabilities and new partners".[10]

NATO's main objective, however, remained the capability to counter any threats faced by its member states. But this understanding changed to include threats posed by traditional external security threats as well as internal security threats from new sources, including terrorist attacks in the context of 'homeland security.' NATO's original role of protecting its member states from the threat of aggression, and doing so by all political and military means necessary, has slowly been amended to reflect new threat scenarios, including acts by non-state actors in response to the attacks on September 11, 2001.[11]

In the autumn of 2012, the Swedish National Defense College conducted a hybrid threat experiment, using similar situations to those contemplated by NATO.[12] The experiment scenario centered on an imaginary island kingdom in the middle of the Baltic Sea, which faced growing economic, social, and political challenges. The situation in the fictional kingdom had deteriorated to the point that neighboring states, including Sweden, were directly affected by a mix of traditional and hybrid threats. The experiment participants were asked to pretend to be a committee of advisers for the Swedish government and were tasked with advising the Swedish Government on how to handle the issues presented by its fictional neighbor. The participants were instructed to represent the industries that they worked for in real life. The experiment participants included members of the Swedish armed forces, Swedish national support agencies, the university sphere, the pharmacological industry, the banking industry and the internet security industry.

The experiment participants were given a wide range of new and threatening situations to contemplate and provide solutions for the Swedish Government. The situations created by the imaginary hostile state included (1) cyber threats, including defacing government sites; (2) threats to hack and stop the pacemaker of a high ranking Swedish government official; and (3) the destruction of a turbine in a nuclear power station using a computer worm, similar to the "Stuxnet" attack in Iran.[13] Traditional threats were also contemplated, and included (1) the attempt to sink a hijacked oil tanker in the middle of a sensitive maritime environment zone; (2) inserting a small group of Special Forces Operatives into Swedish territory; and (3) hiring Somali pirates to hijack Swedish vessels just off of the Horn of Africa.

The experiment reflected both the strengths and weaknesses of Swedish democratic society when facing multimodal threats. The experiment showed that the existing Standard Operation Procedures (SOPs) allowed for efficient responses to certain threats, by addressing how Swedish government agencies and even certain NGOs should react in times of emergency. This was mostly due to a previously established command and control, as well as communication and coordination assets within the central authority. However, the experiment also showed the existence of shortcomings within Swedish society when countering multi modal threats. This was due to the absence of a nationally defined comprehensive approach for joint inter-agency cooperation. This lack of comprehensive joint action and coordination was highlighted by the fact that the Swedish Government did not have the authority to direct and control the work of autonomous subordinate agencies.

The participants of the Swedish experiment recognized that modern conflicts with hybrid elements would lead to new levels of threat and response complexity. They noted that to combat these new complexities, there needed to be an active, uniform and collective leadership - some- thing beyond the standard operation procedures.[14] The participants identified that a major weakness was the lack of a comprehensive coordination and response between agencies, including the armed forces, the civil defense assets, and other civilian actors – such as IT specialists and

10 North Atlantic Treaty Organization, "Active Engagement, Modern Defence," last modified November 19, 2010, *http://www.nato.int/cps/en/natolive/official_texts_68580.htm.*

11 North Atlantic Treaty Organization, "Statement by the North Atlantic Council," last modified September 15, 2001, *http://www.nato.int/docu/pr/2001/p01-124e.htm.*

12 Juhapekka Rautava, "Countering Hybrid Threats: CHT Seminar" lecture, Swedish National Defence College, 2012.

13 Jonathan Last, "How Stuxnet is Scaring the Tech World Half to Death," *The Weekly Standard,* last modified September 30, 2010, *http://www.weeklystandard.com/blogs/how-stuxnet-scaring-tech-world-half-death.*

14 Regarding details for the SNDC-symposium, contact Håkan Gunneriusson at *hakan.gunneriusson@fhs.se.*

pharmaceutical experts [15]

Recently, the shortcomings addressed by the Swed- ish study were proven to be accurate. Swedish counter-terrorism and intelligence agencies failed to cooperate and operate jointly when facing a recent national threat. The country was left vulnerable to acts of terrorism, causing the director and deputy director of the National Center for Counterterrorism to resign in protest.[16] With a shrinking defense budget, the downscaling of national agencies and society's inability to accept the existence of such threats as future possibilities, it seems unlikely that these shortcomings will be addressed in the near future.

NATO's Comprehensive Approach to Countering Hybrid Threats: *Challenges and Missed Opportunities*

The 2011 "Jasmine Revolution" in North Africa exemplified the types of problems addressed in the Swedish study, and showed how such threats could become a reality. It also demonstrated a range of new, multimodal hybrid threats, including (1) failed state scenarios; (2) civil unrest; (3) the proliferation of sophisticated weaponry systems to regional extremist groups;[17] (4) the threat of proliferation of weapons of mass destruction; and (5) the prospects of mass migration into Europe.

The novel concept of hybrid threats first gained recognition when Hezbollah had some tangible military success against the Israeli forces during the Second Lebanon War in 2006. Ironically, the definition of 'hybrid' then was that a non-state actor showed military capabilities originally only associated with state actors.[18] Since then, the idea of hybrid threats has become associated with a new threat dimension including 'cyber' attacks, 'bio- hacking'[19], the 'abuse' of nanotechnology, and plain acts of global terrorism.[20] If any state or non-state actor wanted to target a Western European state by using conventional means of warfare they would face significant risks of retaliation.

The military engagement by NATO in the Libyan conflict highlighted how quickly the organization could be drawn into military combat operations, when requested to contribute militarily to peace enforcement combat operations and/or 'stability operations'[21]. Libya also showed how NATO can contribute militarily to a UN authorized 'use of force' peace enforcement operation in the context of the UN's emerging 'R2P' responsibility.[22] 'Operation Unified Protector' also showed an apparent rift among NATO's member states in terms of willingness and ability to commit military assets: only half of NATO's 28 states actually committed military assets to the operation.

Since then, the UK and France have been discussing changes to voting procedures in NATO as well as new bi-national military cooperation agreements in order to overcome acute mission shortcomings in the future. Canada stopped participating in the NATO AWACS program altogether as a direct consequence to Germany's decision to halt its participation in AWACS operations during the conflict. The present situation in Syria seems to constitute more or less a repeat of these rifts and differences among the alliance's member states (with perhaps the exception of the position towards Turkey and its request for NATO

15 Ibid.

16 Sveriges Radio, "Spy Executives leaves cooperative body in protest," last modified November 04, 2012, *http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=5334446.*

17 Harel Amos and Avi Issacharoff, "Hamas boosting anti-aircraft arsenal with looted Libyan missiles," *The Free Republic,* last modified October 26, 2011, *http://www.freerepublic.com/focus/news/2798512/posts.*

18 See e.g. Matt M. Matthews, "We Were Caught Unprepared: The 2006 Hezbollah-Israeli War," (Combat Studies Institute Press, Fort Leavenworth, 2008).

19 An unnatural high percentage of children got Nacrolepsy in Scandinavia by birdflue vaccine, some genes was sensitive, *http://birdflu666.wordpress.com/2012/02/24/5740/.*

In 2010, the town Östersund was affected by Cryptosporidium, a parasite which uses humans (and other animals too) as hosts for its reproduction. *http://www.smittskyddsinstitutet.se/nyhetsarkiv/2010/smittskyddsinstitutets-arbete-med-det-vattenburna-utbrottet-av-cryptosporidium-i-ostersund/.*

20 Hakan Gunneriusson, "Nothing is taken serious until it get serious," *Defence Against Terrorism Review*, no. 1 (2012).

21 For a definition US Army Field Manual (FM) 3–07, see *Stability Operations*, defined broadly as "the Army's approach to the conduct of full spectrum operations in any environment across the spectrum of conflict," *http://www.fas.org/irp/doddir/army/fm3-07.pdf.*

22 Also referred to as 'RtoP', describing the international responsibility to protect humans from genocide and crimes and humanity and manifest in UN GA Resolution A/RES/63/308 on the Responsibility to Protect.

PATRIOT missiles to enhance its defence capability towards any Syrian air attack).

Pre-dating these events was NATO's Lisbon Summit Declaration of 2010, which discussed general challenges to the alliance's present role before the backdrop of falling national defence budgets. New threat scenarios, which differ from traditional 'state on state' armed conflict scenarios were discussed, often in the context of increasing globalization.[23] As a consequence, NATO adopted a new strategic concept which sets out its vision for the immediate future and calling for "NATO's evolution, so that it continues to be effective in a changing world, against new threats, with new capabilities and new partners".[24] The alliance's main objective, however, remains the capability to counter any threat arising for any of its member states posed by both traditional external security threats as well as internal security threats from a new source, including terrorist attacks in a 'homeland security' type of context. This original role of protecting NATO's member states from aggression or the threat of it, by all political and military means necessary, is slowly being amended to reflect on new threat scenarios, which include acts by non-state actors, as NATO's response to '9/11' highlights.[25]

If NATO had decided to adopt the comprehensive approach as part of its strategic framework, then this would also have been beneficial for shaping the alliance's future role. NATO faces the prospect of changing mission roles, shrinking national defense budgets and general identity issues surrounding organization its existence: its traditional role as provider of military capabilities for its member states, as part of a collective self-defense effort, or for the U.N., in cases of U.N. Charter Article 51 authorizations, would have been complemented by tasks of global risk and crisis management. Countering new hybrid threats and taking the lead in future joint multi-stakeholder threat-based responses could have resulted in a new role for NATO as a facilitator of peace and stability operations.

Of particular relevance in the context of hybrid threats is the danger of the proliferation of advanced weapon systems by non-state actors (NSAs) associated with radical Islam, as well as their increasing use of new technologies. 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 Fajr (Dawn) 5 rocket's capability to reach both Tel Aviv and Jerusalem has once more shown the vulnerability of Israel as a state when it comes to conventional kinetic threats.

Such conventional military and security threats are supplemented by the use of new communication technologies, which are used to influence the Western opinion in favor of Hamas – the newest Gaza conflict is thus an excellent example of how multimodal threats, asymmetric terror, and warfare are supplemented by terrorist disinformation campaigns. Hamas has been employing tools and strategies of disinformation normally associated with clandestine psychological operations of traditional military state actors, such as sending emails and text messages with hoax news updates, as well as propaganda slogans to Israeli and non-Israeli Internet addresses and cellphones and the use of the Internet to disseminate propaganda.[26] Text messages during the eight days of conflict were sent, which warned that "Gaza will turn into the graveyard of your soldiers and Tel Aviv will become a fireball".[27] It is likely that hybrid and 'joint' operations of non-state actors, terrorist organizations will become more frequent.

Additionally, the capacity for non-state actors to copy the command and control structures of conventional mili- tary has increased with the readily 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

23 NATO Lisbon Summit Declaration, *http://www.nato.int/cps/en/natolive/official_texts_68828.htm.*

24 "Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organization" of 19 November 2010, *http://www.nato.int/cps/en/natolive/official_texts_68580.htm and Lisbon Summit Declaration of November 20, 2010.*

25 NATO invoked Article 5 of the Washington Treaty, the Alliance's collective defence clause, see *NATO*, "Collective defence," *http://www.nato.int/cps/en/natolive/topics_59378.htm;* See also "Statement by the North Atlantic Council of 12 Sept 2001," *http://www.nato.int/docu/pr/2001/p01-124e.htm.*

26 L. Marcus, "Explosive New Arab Music Video: 'Strike a Blow at Tel Aviv,'" *Jewish Press,* November 19, 2012, *http://www.jewishpress.com/.*

27 Jaber Hala, "Hamas goes underground to avoid drones," *The Sunday Times,* November 25, 2012, 27.

an AK-47 and the insurgents' morale were traditional 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 used to be also weaker in terms of available weaponry and utilization of technology.

Thus, 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."[28] Even a mainly conventional war will have a 'hybrid' element such as a cyber-attack or bio-hacking. 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' for carrying out or controlling hybrid threats.

The Role of "Cyber" in Hybrid Threat Scenarios

Such conventional military and security threats are supplemented by the use of new technologies. The advent of 'Cyber conflict' and 'Cyber War' serves as examples for the use of new technologies within the scope of hybrid threats. Cyber War[29] refers to a sustained computer based cyber-attack by a state (or non-state actor) against the information technology infrastructure of a target state. An example of such hostile action occurring 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 Second World War Soviet memorial from the center of the city of Tallinn.[30] This incident was followed by the employment of sophisticated cyber operations against Georgia in 2008.

The most recent report of sophisticated cyber weaponry was Stuxnet, a virus that sabotaged Iran's nuclear weapons program. Presumably employed by Israel, it highlighted the technical advancement possibilities, as well as the potential of such means in the fifth dimension of warfare.[31] The continuing and intensifying employment of cyber attacks by China against the United States, NATO, the European Union and the rest of the world has led the U.S. to respond by establishing a central Cyber War Command, the United States Cyber Command (USCYBERCOM) in 2010[32] to "conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure U.S./allied freedom of action in cyberspace and deny the same to their adversaries."[33] 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 NATO Transnet network on Countering Hybrid Threats (CHT).[34]

'Cyber' in the context of armed conflict does not necessarily establish genuinely new categories of conflict; rather it constitutes another and improved tool of warfare. The military will find new ways to conduct its operations using 'cyber' as a force multiplier and operational capability enhancer, and will continue to operate on the tactical, operational or strategic level. The increasing use of cyber by non-state actors to further their economic, political and other interests, and the present problem of clear accreditation of the originators of cyber activities makes it increasingly hard to identify and counter such threats. Terrorist nation state actors (or terrorist proxies of a state sponsor such as Iran and Syria) are increasingly using cyber capabilities to augment their attack capabilities.

Apart from the above mentioned use of 'cyber' as a means of disinformation during the last Israel-Gaza conflict, another example for the role of social media as a enhancer for terrorist activities can be found in the Mumbai attacks in India in 2008. Terrorists from Pakistan attacked the city,

28 SNDC Hybrid Threat Workshop, Swedish Armed Forces representative.

29 See generally, Jenny Döge "Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime," *Archiv des Völkerrechts,* (2010): 486.

30 See Ian Traynor, "Russian accused of unleashing cyberwar to disable Estonia," *The Guardian*, May 17, 2007, *http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.*

31 Christopher Williams, "Stuxnet: Cyber-attack on Iran 'was carried out by Western powers and Israel,'" *The Telegraph,* Jan. 21, 2011, *http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html.*

32 With the decision taken in 2009, and initial operational capability as of 2010, see United States Strategic Command *http://www.stratcom.mil/factsheets/Cyber_Command/.*

33 Ibid.

34 See NATO Transformation Network, *https://transnet.act.nato.int/WISE/Transforma1/ACTIPT/JOUIPT.*

with a particular focus on the Taj Mahal hotel.[35] Tactical intelligence during the raid was gathered from social media and the exploitation of existing mass media such as cable-TV, while home electronic equipment and cell phones were used as means of 'command and control'. Handlers directed the terrorists on the ground; they stood in permanent cell phone contact with the field operators in Mumbai, and were able to use both Internet and major television channels for updates 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 operation's handlers 'data mined' and compiled this information in real time and communicated operation relevant information directly to the terrorists through the use of smart phones. For example, the terrorists received the information from their handlers that the antiterrorist commander in charge of Mumbai security had been killed in action. This had been data mined from open live sources and communicated directly to the terrorists who had little knowledge about this early 'success' of their action. The terrorists also got reports that people panicked and were running for their lives, something everyone saw on the television.

Consequently, the terrorists received direct instructions to add to the panic by detonating hand grenades at regular intervals. After television reports indicated that there were three Indian ministers in the hotel, the terrorists were ordered by their handlers to kill or capture them.[36] The terrorists were also informed of tactical developments outside the hotel and instructed to attack specific targets among the police and security forces. When an anti-terrorist squad landed on the roof, warnings were issued and the terrorists subsequently engaged the squad.[37]

The Mumbai example illustrates 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 globalization and technical advancement. Moreover, the volume of publicly available electronic information is staggering. In urban areas, one can find tactical information by simply tapping open sources or into closed, protected sources such as CCTV (closed-circuit television), or documents in 'data cloud' solutions.

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 'backdoor' Trojan for the purpose of later data theft.[38] Using the Google server, hackers bypassed any firewall used by the 'target.' Another example of using an otherwise 'innocent' host like Google took place in late 2012 when hackers defaced Pakistan's Google domain along with other official Pakistan websites.[39]

To summarize these present 'cyber' hybrid threats, one can state that it is new and readily available technology that makes these threats so potent. Command and control capabilities may be established in relatively short notice and with little effort. The media can be used for influencing the public opinion as a means of psychological operations (PSYOPS), both at home and abroad. Cyber threats strike at the core of modern warfare by affecting command and control abilities, which have become increasingly vulnerable to cyber-attack. Such cyber threat capabilities also strike at the core of our post-industrial, modern society. The use of 'cyber' as a threat category on its own or as an aiding tool for carrying out other multi-modal attacks is highly likely to increase, and consequently its overall role within the context of hybrid threats will rise.

Countering Hybrid Threats – Implications for Military Doctrine

Military doctrine intentionally centers on a military perspective that reflects the particular necessities and capabilities of the armed forces. NATO's inability to formulate a binding comprehensive approach to hybrid threats (which would combine conventional threat elements with unknown, 'hybrid' threat elements as a potential trigger for a NATO

35 Some of the following content derives from Swedish National Defence College sources which are on file with the authors.

36 See *http://islamicterrorism.wordpress.com/2009/01/07/chilling-phone-transcripts-of-mumbai-terrorists-with-their-lashkar-handlers/.*

37 See *http://www.rediff.com/news/2009/mar/18sld4-book-extract-of-mumbai-attacked.htm.*

38See *http://securityaffairs.co/wordpress/10454/malware/malware-hides-cc-server-communications-using-google-docs-function.html.*

39 See *http://tribune.com.pk/story/470924/cyber-vandalism-hackers-deface-google-pakistan/.*

Article 5 response) is a testament to the perseverance of an overwhelmingly conservative military doctrinal approach. The danger in this approach is that the failure to prepare for 21st century threats by adhering to traditional concepts of counterinsurgency (COIN) and traditional international conflict scenarios, might lead to a lack of preparedness and vulnerability in the future. This failure of defining a NATO policy on countering hybrid threats is even more unfortunate given that the U.S. has a national military security strategy in place that recognizes certain hybrid elements as threats to its national security.[40]

This failure to adapt at NATO's organizational level may stem from a continuing Cold War rooted psychology among the political actors. During the Cold War, the world was locked into an intellectual doctrinal approach, which viewed all conflicts in the context of the global ideological struggle coded political paradigm of its time. Once the Cold War came to an end in 1991, new national conflicts arose along once pacified conflict lines. This new era manifested itself in the terrible conflicts in the Balkans as a conse- quence 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 exclu- sively 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 U.S. led West versus the Soviet led East. This division made potential threats more foreseeable and even 'manageable.'

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' of post 9/11 as parallel tracks; with the latter challenging Western positivistic materialism's paradigm.[41] 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 it will in its turn 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 integrated protection from conventional interstate aggression as well as from new hybrid threats. One such example is the recent suggestion by the United Nations that states should be more proactive when it comes to fighting the use of the Internet by terrorists.[42] Only society as a whole can protect itself, a task that is not limited to the military. This is even more important in times of shrinking military budgets, which will likely continue for the foreseeable future. An integration of the capabilities at an interstate level, something NATO refers to as 'Smart Defence', and increased defense cooperation, may be the only way to counter the multitude of evolving threats in the future.

Hybrid threats challenge Clausewitz's dogma of war, which constituted "a mere continuation of [state] politics by other means," and might degrade his definition of a permanent state of war. 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 defense strategies that respond to existent threats and prepare for evolving new threats. Such preparation reminds us of Sun-Tzu when he provided: "victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win." [43]

40See e.g. *The National Security Strategy of the United States of America*, September 2012, *http://nssarchive.us/NSSR/2002.pdf.*

41 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.

42 See United Nations Counterterrorism Implementation Task Force, "The Use of the Internet for Terrorist Purposes," *http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.*

43 Sun-Tzu, *The Art of War*, (Simon and Brown, 2011): ch. 4.

Concluding Observations on Future Military Challenges within a Political and Legal Context

This article was written with the intention to introduce the 21st century "hybrid threat" to a wide audience, despite NATO's decision not to adopt a comprehensive approach. This failure does not reduce the dangers of this category of global risk. On-going debate and academic engagement with the topic and rationale of the hybrid threat, such as the Swedish experiment in 2012, will hopefully lead to heightened awareness and eventual preparedness.

This submission concludes with a sobering prediction: the present legal concepts on the use of military force - the *jus ad bellum* - have become relatively anachronistic and partially outdated, which will not suffice when dealing with the present security threats and challenges of the 21st Century. The U.S. National Security Strategy of 2002 was designed to authorize U.S. President George W. Bush's administration to take pre-emptive action whenever the "United States cannot remain idle while dangers gather,"[44] and was meant to counter threats which involve the use of weapons of mass destruction[45] by rogue states and terrorist non-state actors, such as al-Qaeda. The emergence of new threats makes an extension of this doctrine not unlikely.

With such changes to traditional military doctrine, 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 prohibition of the use of force, with its limited exceptions under Articles 2(4), 51 of the U.N. Charter and Article 5 of the NATO Treaty. Also, future direct intervention in failed state scenarios will require flexibility with choices of military assets and objectives. The present concept of crisis management response can easily develop into a more pronounced military engagement of an increasingly 'forceful' nature.[46]

Future responses to multimodal threats will include the kinetic force options directed against – most presum- ably – non-state actors. They will affect our present views on the legality of the use of force in international relations, as enshrined in Articles 2 (4) of the U.N. Charter with the limited exceptions available under Article 51 of the U.N. Charter, namely individual and collective self-defense,[47] as well as Security Council authorization. Already, the continued use of 'UAVs' (Unmanned Aerial Vehicle, or 'drones') for targeted killing operations effectively emphasizes the legal challenges ahead. The ongoing kill operations in the tribal areas of Waziristan/Pakistan demonstrate how quick the critical threshold of an armed conflict can be reached and even surpassed. These operations clearly fall within the scope of 'armed conflict', as defined by the International Criminal Tribunal for the Former Yugoslavia in *Prosecutor v. Dusko Tadic*.[48] Thus, these operations give rise to the applicability of the norms of the law of armed conflict, the body of international humanitarian law governing conduct in war.

However, the 'lawfulness' of such operations requires the existence of either a mandate in terms of Article 51 of the U.N. Charter[49] or the existence of an illegal armed attack in order to exercise a right to national or state self-defense in terms of Article 51. Whether such military operations are within the scope of these categories remains open to discussion. Indeed, highly relevant to this context is the newly codified Article 8*bis* of the Rome Statute of the International Criminal Court, which criminalizes acts of aggression, and excludes the non-state actor as a possible target/victim. Consequently, such kinetic operations against non-state actors[50] remain outside its scope of applicability and may lead to accountability issues.

Certain legal considerations are important in regard to

44 The White House, "The National Security Strategy of the United States of America," *National Security Strategy Archive*, September 2002, *http://nssarchive.us/NSSR/2002.pdf.*

45 "Weapons of mass destruction" refer to nuclear, biological and chemical weapons.

46 The 2004 Tsunami disaster relief saw civil relief efforts complemented by military efforts and assets to enhance own relief efforts, and to provide military protection in terms of 'force protection.'

47 North Atlantic Treaty, Art. 5, April 4, 1949, 34 U.N.T.S., at 243.

48 Prosecutor v. Dusko Tadic, Case No. IT-94-1-A, 105 ILR 419, 488, Appeal Judgment, (July 19, 1999).

49 A Security Council Resolution authorizing the use of force in an Enforcement and Peace Enforcement Operation context.

50 Cf. the Israel Defense Forces' operations during the 2006 Second Lebanon War against Hezbollah and Operation Cast Lead against Hamas in 2008/2009 as well as the continuing use of UAVs/drones against enemy targets from the Taliban and al-Qaeda in Afghanistan and Pakistan.

hybrid threats, which may include kinetic threats but do not exclude non-kinetic threats such as cyber-attacks, as long as a military response is considered as a counter-option. Hybrid threats include threats stemming from transnational terrorism and other low intensity, asymmetric conflicts. In addition, post-9/11 transnational terrorism may have changed the perception that *jus ad bellum* was only applicable on inter-state international conflicts.[51]

Furthermore, the recent Kampala definition of the crime of aggression[52] may have to be amended when it comes to countering hybrid threats, as non-state actors do not fall within the definition on the crime of aggression, whether they are perpetrators or victims. The new Article 8*bis* of the Rome Statute at the Kampala Review Conference in June 2010[53] does not recognize the contemporary role which non-state actors play in the context of the aggression.[54]

Aggression under article 8*bis* is now a leadership crime.[55] The language seems to suggest a stricter approach than the Nuremberg process, where individual liability was framed with reference to individuals who could "shape or influence policy." "Effective control" under Article 8*bis* could limit individual liability to the exclusion of individuals who, for instance, merely influenced policy.[56] This view of 'leadership', combined with the state-centric approach to the crime of aggression, underscores the difficulty in extend- ing the crime of aggression to "post-bureaucratic forms of organization as represented, for example, by paramilitary or terrorist non-State actors," such as Hamas or Hezbollah.[57] The legal implications of the definition of aggression for the "post-9/11" world, as well as for possible military responses to new hybrid threats by non-state actors remain to be seen.

If NATO decided to adopt the comprehensive approach as part of its strategic framework, then this would also be beneficial for shaping its future role. NATO faces the prospect of changing mission roles, shrinking national defense budgets and general identity issues surrounding organization its existence: its traditional role as provider of military capabilities for its member states, as part of a collective self defense effort, or for the U.N., in cases of U.N. Charter Article 51 authorizations would have been complemented by tasks of global risk and crisis management. Countering new hybrid threats and taking the lead in future joint multi-stakeholder threat-based responses could have resulted in a new role for NATO as a facilitator of peace and stability operations.

NATO's Strategic Concept of 2010 was aimed at prevention, as well as deterrence, and aims at developing a holistic or comprehensive approach to a variety of new conflict scenarios of multimodal or hybrid threats: from kinetic combat operations to multi-stakeholder based non-kinetic

---

51 Pre-9/11 examples of engaging in military action against foreign terrorists led mostly to condemnation as a violation of Art. 2 (4) UN Charter, see the U.S. Operation El Dorado Canyon of 1986 against Libyan terrorist targets or the hot pursuit operations by SADF against ANC, MK and SWAPO, and more recently long range operations of the IDF against terrorist infrastructure in Khartoum, Sudan. For a legal analysis of the changing nature of asymmetric war, see Sascha-Dominik Bachmann, *Targeted Killings: Contemporary Challenges, Risks And Opportunities*, 18(2) J. Conflict Security and L. 259 (2013).

52 See Sascha-Dominik Bachmann and Gerhard Kemp, *Aggression as 'Organized Hypocrisy' – How the War on Terrorism And Hybrid Threats Challenge The Nuremberg Legacy*, 30 Windsor Y.B. Access Just. 233 (2012).

53 See Res.RC/Res.6, advance version, 16 June 2010 online: International Criminal Court <*http://www.icc-cpi.int*>.

54 The definition of "Crime of Aggression" to be included in the Rome Statute in 2017 reads:

Article 8bis. Crime of aggression. 1. For the purpose of this Statute, "crime of aggression" means the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a State, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations. 2. For the purpose of paragraph 1, "act of aggression" means the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations. Any of the following acts, regardless of a declaration of war, shall, in accordance with United Nations General Assembly resolution 3314 (XXIX) of 14 December 1974, qualify as an act of aggression.

55 Art 8bis(1) read with art 25 (3bis); see analysis of G. Kemp, *Individual Criminal Liability for the International Crime of Aggression* (Belgium: Intersentia, 2010) 236-237; Kai Ambos, *The Crime of Aggression after Kampala*, 53 German Y.B. of Int'l Law 463, 468 (2010).

56 Ambos, 53 German Y.B. of Int'l Law, 468; For a more nuanced view on "leadership," see G. Kemp, *Individual Criminal Liability for the International Crime of Aggression*, 236-237.

57 Ambos, 53 German Y.B. of Int'l Law, 492.

responses.[58] 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. The repercussions for international lawyers in terms of possible responses to such challenges are significant, and have not yet been discussed in terms of their full possible impact for the way we define war and peace within the concept of armed attack and individual and collective self-defense.

Conclusion

Hybrid threats will dominate the conflicts of the future, and will be no less serious than the conflicts of the 20th century. New roles are needed for national militaries, as well as for non-state actors, such as multinational corporations and non-governmental organizations. The "War on Terror" illustrated that the term "geography" has become obsolete; it created 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'. The use 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.

Again, the intention of this article is to introduce the 21st century 'hybrid threat' to a wider audience. Ongoing debate and academic engagement with the topic and rationale of 'hybrid threats,' such as the Swedish experiment in 2012, will hopefully lead to greater awareness. In addition, the authors believe that the definition of 'armed attack' will continue to change in the post-9/11 environment,[59] and will eventually give rise to a significant change in the present body of international law regulating *jus ad bellum* and *jus in bello*.[60] Reflecting on the current U.S. National Security Strategy, and on a recent analysis by Professor Dr. Heintschel von Heinegg[61] on the consequences of asymmetric warfare for the law of armed conflict, one likely consequence may be that nations will use military force to counter hybrid attacks (including cyber-attacks).

Hybrid threats as such are not new threats; new is the recognition that such multimodal threats command a 'holistic' approach, which combines traditional and non-traditional responses by state and non-state actors such as multinational corporations. Responses to hybrid threats must be proportionate and measured: from civil defence and police responses to COIN and the use of military force. The authors therefore predict that the emergence of hybrid threats and their recognition as potential threats to peace and security, the proliferation of low threshold regional conflicts (such as the Libyan 2011 conflict and Syria), and continuing asymmetric warfare scenarios (such as the ongoing operations in Afghanistan and Pakistan) will have a significant impact on the prevailing culture and prism of traditional military activity, which is still influenced by concepts from the last century.

Hybrid threats pose not only security challenges but also legal difficulties. Only time will tell how Western states, through military doctrinal reform, will adapt within their existing legal and operational frameworks.

58 See 2010 NATO Strategic Concept, *http://www.nato.int/cps/en/natolive/topics_82705.htm.*

59 U.N. Security Council Resolutions 1368 of September 12, 2001 (U.N. Doc. S/RES/1368 (2001) and 1373 of September 28, 2001 (U.N.Doc. S/RES/1373 (2001), both affirming the right of the US "of individual or collective self defence in accordance with the Charter".

60 Cf Article 49 of the First Additional Protocol to the Geneva Conventions.

61 Dr. Wolff Heintschel von Heineggl, "Max Planck Encyclopedia of Public International Law: Asymmetric Warfare," *Oxford University Press, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1809?rskey=TOSNYw&result=5&prd=EPIL.*