Article

# Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats – mapping the new frontier of global risk and security management

by Sascha-Dominik Bachmann

## INTRODUCTION

The end of the so-called "Cold War" has seen a change in the nature of present threats and with it to the overall role and mission of NATO, the North Atlantic Treaty Organization. The collapse of the Soviet Union and the Warsaw Pact in 1991 also removed the original *raison d'etre* of the Alliance: the prospect of having to repel a Soviet led attack by the Warsaw Pact on the West through the so called "Fulda gap" in Germany (referring to the German lowlands between Frankfurt am Main and the former East German border, which were regarded as the most likely terrain for an armour led Soviet breakout) was replaced by the recognition of the need to counter new – often hybrid – threats, which have little in common with bygone acts of interstate aggression. These new, modern threats to global peace, prosperity and security seriously threaten the present steady state environment at home (before the backdrop of the ongoing asymmetric conflicts in Afghanistan, Pakistan and Iraq) and warrant a comprehensive, multi-stakeholder driven response.

Multimedal, low intensity, kinetic and non-kinetic threats to international peace and security including cyber war, low intensity asymmetric conflict scenarios, global terrorism, piracy, transnational organised crime, demographic challenges, resources security, retrenchment from globalization and the proliferation of weapons of mass destruction were identified by NATO as so called "hybrid threats" (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).

NATO's Bi-Strategic Command Capstone Concept describes these hybrid threats as "those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives." (See Hybrid Threats Description in 1500/CPPCAM/FCR/10-270038 and 5000 FXX/0100/TT-0651/SER: NU0040 dated 25 August 2010: (para 7)).

Having identified this kind of emerging threat, NATO is working on a comprehensive conceptual framework (the Capstone Concept) for identifying and discussing such threats and possible multi-stakeholder responses. 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 (see "Updated List of Tasks for the Implementation of the Comprehensive Approach Action Plan and the Lisbon Summit Decisions on the Comprehensive Approach," dated 4 March 2011, pp 1–10, para 1).

NATO 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) Experiment" in 2011(*cf* NATO's *Transnet* Network on Countering Hybrid Threats (CHT) at

https://transnet.act.nato.int/WISE/Transforma1/ACTIPT/JOUIPT). The workshops of the experiment took place in Brussels, Belgium and Tallinn, Estonia, and had the aim of identifying possible threats and to discuss some or the key implications that need to be addressed in countering such risks & challenges. Essential is the hypothesis that such a response will have to be in partnership with other stakeholders such as international and regional organisations, as well as representatives of business and commerce.

This short article introduces the reader to a new form of global threat scenario and the possibilities of response and deterrence within their wider legal and political context.

## NATO'S NEW COMPREHENSIVE APPROACH TO COUNTERING HYBRID THREATS – CHALLENGES AND OPPORTUNITIES

The events of the so-called "Jasmine Revolution" in North Africa during the so-called "Arab Spring" of last year shook the political landscape in the Maghreb, the Arab and the Mid-Eastern world. They generated also a variety of hybrid threats: from failed state scenarios, civil unrest, proliferation of sophisticated weaponry and even weapons of mass destruction (the Libyan conflict allegedly led to incidents of proliferation of sophisticated weapon systems to regional extremist groups such as Hamas in Gaza; *cf* Amos Harel and Avi Issacharoff, "Hamas boosting anti-aircraft arsenal with looted Libyan missiles" *Haaretz,* 27 October 2011) and the prospects of mass migration into Europe caused by the Arab unrest in general and the seven month NATO campaign in Libya in particular.

These events saw NATO in a more traditional role as supranational defence and security organisation. In late October 2011, the conflict in Libya had come to an end with its leader al-Gaddafi killed and a new transitional government, the National Transitional Council (NTC), in power. This outcome was largely achieved by the deployment of military force in a NATO led operation at sea and in the air (Operation "Unified Protector") in order to enforce United Nations Security Council Resolution 1973 (UN S/RES/1973 (2011)). The engagement in the Libyan conflict highlighted how quickly NATO and its member states can be drawn into military combat operations, unofficially referred to as "kinetic operations", when requested to contribute militarily to peace enforcement combat operations and/or so-called "stability operations" (see for a definition US Army Field Manual (FM) 3–07, *Stability Operations)*.

Whilst Libya demonstrated how NATO could contribute militarily to a UN sanctioned "use of force" operation in the context of UN's new "R2P" responsibility (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) it also showed an apparent rift among NATO's member states in terms of willingness and ability to commit military assets. Only half of the Alliance's 28 states actually committed forces to the operation and the UK and France are discussing changes to voting procedures in NATO, as well as new bi-national military cooperation agreements as a direct fallout of the operation.

In 2010, NATO issued its Lisbon Summit Declaration (press release PR/CP (2010) 0155) where general challenges to the Alliance's present role as well as potential responses before the backdrop of falling national defence budgets and new threat scenarios differing from traditional "state on state" armed conflict were discussed, often in the context of increasing globalisation. 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" ("Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation" of 19 November 2010, http://www.nato.int/cps/en/natolive/official_texts_68580.htm and Lisbon Summit Declaration of 20 November 2010, PR/CP (2010) 0155)).

Its 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 challenge. This original role of protecting NATO's member states from any such security threats by all political and military means necessary is supplemented by new competencies such as the successful crisis management of even the most "challenging crises" either by NATO directly or by reaching out to new actors and stakeholders such as non-NATO states as well as NGOs. Flexibility, cost effectiveness, and eventually adaptability to new threat scenarios, are key competencies in the new concept.

## CYBER ATTACKS AS AN HYBRID THREAT – A CASE STUDY ON THE APPLICABILITY OF A COMPREHENSIVE APPROACH

Cyber attacks resemble a kind of new hybrid threat which gained more publicity in recent years. Cyber threats resemble threats in the fifth dimension of warfare, as cyber warfare is often termed, and refer to a sustained campaign of concerted cyber operations against the IT – infrastructure of the target state, including and leading to mass web destruction, spam and malware infection. The intensity of these operations, their "success" in terms of disruption and denial of IT services as well as in terms of disinformation and defacement, and lastly their objectives which are political in nature and not just criminal (such as internet banking fraught etc) warrant their nature as cyber "warfare" and not just cyber crime.

Cyber warfare passes the threshold of other cyber activities such as hacking, spamming and phishing (see in

general Döge "Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime" 48 *Archiv des Völkerrechts* (2010) 486–501). Cyber attacks can be generated by state and non-state actor alike, but also by groups of highly expert individuals or multinational companies (consider the capabilities and opportunities available to Microsoft, Apple or individual "figureheads" of international IT): an example of cyber operations of recent years which came to our attention was the 2007 attempt by Russia to punish Estonia for its decision to remove a WW II Soviet War Memorial from the centre of Tallinn. Russian generated IT attacks virtually and literally "crashed" Estonia's internet infrastructure for a period of over three days, and as a consequence state and political party websites as well as banking and business websites were effectively disrupted ("Russian accused of unleashing cyber war to disable Estonia", *The Guardian* 17 May 2007, at http://www.guardian.co.uk/world/2007/may/17/topstories3.russia).

Russia used similar tactics in the 2008 Russian military conflict with Georgia, employing cyber attack measures against state and private targets in Georgia as part of the Russian military campaign. Another recent example is the use of Stuxnet, a sophisticated computer worm/virus which targeted Siemens control systems which were used in Iran's uranium enrichment centrifuges in order to set back Iran's nuclear weapons programmes ("Stuxnet: Cyber attack on Iran 'was carried out by Western powers and Israel'" *Daily Telegraph,* 21 January 2011 at http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.html). The potential of Stuxnet in terms of technical advancement, possibilities and capabilities is enormous: viruses which target industrial systems and actively disrupt industrial processes pose a significant threat to the infrastructure of any developed state. Such cyber threats posed by China and Russia as nation state originators and directed against the USA, NATO and the European Union, led the USA and the UK to respond by establishing a framework of possible counter techniques including the use of kinetic options.

In the USA, a central Cyber War Command, the United States Cyber Command (USCYBERCOM) was established in 2010 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 our adversaries" (see http://www.stratcom.mil/factsheets/Cyber_Command/). The UK followed suit and launched in November 2011 its own UK Cyber Security Strategy which identifies the importance of cyberspace for the UK and aims at protecting UK interests in the fifth dimension by enhancing cyber security. Whether this entails the capability to launch own cyber attacks, is not disputed by the government (see *Daily Telegraph*, "Britain prepares for cyber war", 25 November 2011 at http://www.telegraph.co.uk/news/uknews/defence/8915871/Britain-prepares-for-cyber-war.html) whether this will also entail kinetic options has to be seen.

These options are supplemented by "civil "law enforcement and crime prevention actions by national and international law enforcement agencies tasked with fighting cybercrime, such as the European Cybercrime Taskforce or the planned European Cyber Crime Centre. Other stakeholders in combating such cyber threats are specialised bodies and organizations such as the UN International Telecommunication Union (ITU) which in collaboration with other actors such as the International Multilateral Partnership Against Cyber Threats coordinate technical response mechanisms and coordinate crisis responses. All these measures, from kinetic to law enforcement to technical countermeasures form part of a holistic approach in combating hybrid threats, thus exemplifying the possible scope of countermeasures available under the "comprehensive approach."

## CONCLUSION

In conclusion, the author predicts 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 Libyan 2011 conflict and Syria), as well as 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. 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), 51 UN Charter and Article 5 NATO Treaty (See Bachmann and Kemp, "Aggression as 'Organized Hypocrisy' – How the War on Terrorism and Hybrid Threats Challenge The Nuremberg Legacy", 30/1 *Windsor Yearbook of Access to Justice* (2012) for a detailed overview of possible legal challenges in the context of kinetic responses to asymmetric conflict and hybrid threats).

Future direct intervention in failed state scenarios will require flexibility in terms of choice of military assets and objectives: the present concepts of "crisis management" responses can easily develop further into a more pronounced military engagement of an increasingly "forceful" nature (see the 2004 Tsunami disaster relief which saw civil relief efforts being complemented by military efforts and assets to enhance own relief efforts but also to provide military protection in terms of "force protection").

Future responses to multimodal threats will also include the kinetic force options; directed against – most

presumably – non-state actors. They will also affect our present concepts on the illegality of the use of force in international relations, as enshrined in Articles 2 (4) of the United Nations Charter with the limited exceptions available under Article 51 UN Charter, namely individual and collective self defence (*cf* Art 5 NATO Treaty) as well as UN authorization. Already today, the continuing use of "UAVs" (unmanned aerial vehicles, or drones) for "targeted killing" operations effectively emphasise the legal challenges ahead: the ongoing "kill" operations in the so called "tribal" Areas of Waziristan/Pakistan are kinetic military operations demonstrating 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* (IT-94-1-A, 105 ILR 419,488) 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 UN Charter (in the form of a UN SC 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. Whether such military operations are within the scope of these categories remains open to discussion. Interesting in this context is also the observation, that the newly codified Article 8 *bis* of the Statute of the International Criminal Court, which criminalises acts of aggression and which was codified in 2010 at the Kampala Review Conference, exclude the non-state actor as a possible target/victim; consequently such kinetic operations against non-state actors (*cf* the Israel Defence Forces' operations during the 2006 Second Lebanon War against Hezbollah and the operations of Cast Lead against Hamas in 2008/2009 as well as the continuing use of UAVs/drones against enemy targets from the Taleban and al-Qaeda in Afghanistan and Pakistan) remain outside its scope of applicability and may lead to later accountability questions.

NATO, assuming the organisational lead in countering hybrid threats, may also turn out to be favourable for shaping the Alliance's future role before the backdrop of the changing mission role and nature of the organisation: its traditional role as provider of military capabilities for its member states, as part of a collective self defence effort, or for the UN, in cases of Article 51 authorisations will be 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 lead to a new role for NATO as a facilitator of peace and stability operations.

NATO's new strategic concept of 2010 will focus on 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 responses. The comprehensive approach is promise and challenge at the same time; time will tell what legal and political challenges will arise and how successful the new approach will be.

**Sascha-Dominik Bachmann**

*Assessor Jur, LLM, LLD, Senior Lecturer in Law (School of Law, University of Portsmouth). The author's professional experience includes working in various capacities as an Army reserve officer and 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. The sources used in the article fall either under "NATO – non-sensitive information releasable to the public" or they are compliant with the so-called Chatham House rules. The author would like to thank Dr Peter Andrew for his insightful comments.*