



NORTH ATLANTIC TREATY ORGANISATION



Supreme Allied Commander, Europe
B-7010 SHAPE
Belgium

Supreme Allied Commander, Transformation
Norfolk, Virginia 23551-2490
United States of America

1500/CPPCAM/FCR/10-270038

5000 FXX 0100/TT-6051/Ser: NU0040

TO: Director General, International Military Staff

SUBJECT: Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats

DATE: 25 August 2010

REFERENCES: A. IMSM-0292-2010, Hybrid Threats Description and Context, dated 31 May 10.
B. SG(2010)0425-REV1, Preparations for the Lisbon Summit, dated 29 Jun 10.
C. MCM-0056-2010, NATO CD&E Process, dated 6 Jul 10.

1. In response to the request at Reference A, the SCs developed their "Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats" at Enclosure 1.
2. Based upon collaborative work with NATO and national subject-matter experts, the Concept focuses on outlining the challenges posed by hybrid threats and provides an initial framework for countering them. Supporting the reflection on emerging security challenges (Reference B), it also identifies key implications for NATO and offers some potential approaches for addressing them.
3. The SCs recommend that the MC:
 - a. Endorses this Concept and forwards it to the NAC to note.
 - b. Guides the SCs to use this Concept to inform the current cycle of the NATO Defence Planning Process, and pursue further concept development (in accordance with Reference C) in order to provide analysis of requirements and possible solutions. This will also drive an analysis of the impact on current and future concepts, doctrine, planning processes, education and training.
4. Should the MC task and resource further development, it is anticipated that the SCs' products would be ready in July 2011, supported by the conduct of seminars, war games and experimentation. Should the nations request it, the SCs will also assist them in analysing the impact of this concept on their own capability development. We would anticipate providing regular update briefings to the MCWG (SP&C).

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

5. The Bi-SC points of contact for Countering Hybrid Threats are LTC Bernard Tourneur, HQ SACT FCRT (NCN 555-4332) and LTC Carlo Cavalli, SHAPE CPP CAM (NCN 254-6716).

FOR THE SUPREME ALLIED COMMANDERS, EUROPE AND TRANSFORMATION:



Karl-Heinz Lather
General, DEU A
Chief of Staff



R G Cooling
Vice Admiral, GBR N
Chief of Staff

ENCLOSURE:

1. Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats.

COPY TO:

External -

ASG(DI)-Emerging Threats and Challenges
ASG(DPP)
COS JFC HQ Brunssum
COS JFC HQ Naples
COS JFC HQ Lisbon

Internal -

SHAPE:

OPI
CPP
FOR
SPT
MIC
JEWCS
SRM
INA
LEG
MED
POL
DSO

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

STC
FIN
PRM
ASN
PAO
ODA
HIS
DOM (for distribution to NMRs)

HQ SACT:

Lists I, II, III, V, VI, VII (HQ SACT DIR 35-1)

ENCLOSURE 1 TO
1500/CPPCAM/FCR/10-270038
5000 FXX 0100/TT-6051/Ser: NU0040
DATED: 25 AUG 10

**BI-SC INPUT TO A NEW NATO CAPSTONE CONCEPT FOR THE
MILITARY CONTRIBUTION TO COUNTERING HYBRID THREATS**

PART I – INTRODUCTION

I.1 **BACKGROUND**

1. The scale and complexity of conventional and non-conventional future threats was highlighted in the Final Report¹ of the Allied Command Transformation (ACT) Multiple Futures Project (MFP). In response, the International Military Staff (IMS) directed² that the Bi-Strategic Commands (Bi-SC) commence development of an overarching Concept for the NATO *Military Contribution to Countering Hybrid Threats (MCCHT)*. A comprehensive internal review of current Policy, Strategy and the existing NATO Operational Framework³ has also underlined a conceptual shortfall and the need for the development of a hybrid threats concept.

2. This concept paper, developed in response to the identified gaps and guidance above, is the result of an extensive literature review⁴ and detailed analysis by ACT, SHAPE, National Representatives, NATO Centres of Excellence and other external NATO and non-NATO SMEs. The results are supported by external war gaming⁵ and will need to be validated further by events planned in 2011. A finalised description and context for hybrid threats (Part II) were also developed in collaboration with the nations, via the Military Committee Working Group (Strategic Plans and Concepts)⁶.

I.2 **AIM**

3. To articulate the parameters of hybrid threats facing NATO and identify areas that might drive the development of future capabilities. The Concept will also inform higher-level political authorities and lower-level military commands of the potential implications within their own domains.

I.3 **SCOPE**

4. The MCCHT is a Capstone Concept⁷ and provides the overarching framework for other subject related documents that have been addressed independently.

¹ MFP final report (April 2009) recognised the need for NATO to adapt to new security challenges of a hybrid nature. Allied Reach 2009 Final Report also emphasised the key elements of the hybrid threats as identified in this paper and made specific recommendations supporting NATO's potential response.

² IMSM-0423-2009 Development of a Military Concept for Countering Hybrid Threats, dated 23 July 09.

³ Annex A – Documents (A-U).

⁴ Annex A – All documents listed.

⁵ JIW2010 – CHT draft AAR June 2010.

⁶ IMSM-0292-2010 Hybrid threats description and context, dated 31 May 2010.

⁷ MC 0583: A Capstone Concept is an overarching concept with the purpose of leading force development and employment primarily by providing a broad description of how to operate across significant portions of the complete spectrum of operations and describing what is required to meet strategic objectives.

5. This Capstone Concept articulates the unique challenges posed by current and future hybrid threats and explains why these challenges may require NATO to adapt its strategy, structure and capabilities accordingly. It discusses both a general approach for dealing with hybrid threats as well as a framework for the Alliance to deliver an effective response. The paper also suggests broader implications for NATO's military component.

6. The concept paper also stresses three underlying themes throughout. Firstly, whilst the existing NATO policy, strategy and doctrinal framework remain valid, there are new threat areas which potentially have grown beyond the current remit; secondly, that the division between military and civilian responsibilities will become less defined in the changing security environment; thirdly, that there will be a need for the Alliance to make far greater use of partnerships and to build better cooperation beyond its borders.

PART II – HYBRID THREATS

II.1 DESCRIPTION⁸

7. Hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives.

II.2 CONTEXT

8. Countering hybrid threats is not a new problem for NATO Nations as adversaries have sought regularly to operate up and down a scale of action, both in military and civil environments, depending on their level of expertise. Hybrid threats involve adversaries (including states, rogue states, non-state actors⁹ or terrorist organisations¹⁰) who may employ a combination of actions¹¹ in an increasingly unconstrained operating environment in order to achieve their aims.

9. Hybrid threats do, however, now present a significant challenge for the Alliance and its interests, whether encountered within national territory, in operational theatres or across non-physical domains¹². They will apply pressure, across the entire spectrum of conflict, with action that may originate between the boundaries artificially separating its constituents. They may consist of a combination of every aspect of warfare and compound the activities of multiple actors. Experience from current operational theatres has demonstrated that adversaries can now conduct hostile actions through a broad array of conventional or non-conventional means and methods, and have a favourable outcome against a force that is superior, both technologically and militarily.

⁸ Description development is to be coordinated with ongoing work on AJP-1.

⁹ Hybrid threats could be perpetrated by singular actors or a combination of states and non state actors with shared and diverse objectives, acting with different degrees of co-operation against NATO.

¹⁰ MC 472 NATO Military Concept for Defence Against Terrorism.

¹¹ Potentially against both military objectives and civilians/civilian objects who/which may be protected by the law of armed conflict.

¹² May include but not limited to cyber, information/media and financial environments.

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

10. Against a backdrop of regional instability (which may be facilitated by, but not limited to, one or more of the following factors: state failure, resource scarcity, extreme climate change, economic migration, natural or human disaster and ideological extremism), hybrid threats may be more challenging than at any previous juncture¹³. Hybrid threats will have fewer physical or political boundaries, particularly due to the effects of globalisation and increased access to international resources and modern communication enablers. As such, hybrid threats will be characterized by highly interconnected individuals and groups who:

a. Find Greater Opportunity for Collaboration. The increasing interconnectedness of the globalised environment will provide greater opportunity for potential adversaries to communicate and work together in previously unexpected ways. The future environment is likely to be characterised by the forming of unexpected relationships and a lack of clearly defined tactical, operational and strategic levels among actors.

b. Frequently Use Misinformation in the Media for Strategic Effects. Adversaries will exploit further the globalised environment and the pervasiveness of the media cycle (supported by near-instantaneous information systems and networks) to create effects that transit between domains at much greater tempo.

c. Use of Diverse Means and Ways. Hybrid threats may contain both non-lethal and lethal fusions of conventional weaponry, chemical, biological, radiological and nuclear (CBRN) materials, terrorism¹⁴, espionage, cyber attack and criminality, supported by maliciously designed information operations and legitimate business organisations.

d. Exploit NATO's and Nations' Rules and Laws. Due to their complexity, hybrid threats will potentially exploit different interpretations and national restrictions in areas such as (but not limited to) international law and lethal engagement.

11. Hybrid threats will have elements that are relevant to defence. Their character is not purely military but military capabilities may contribute to aspects of their prevention, resolution or consequence management. Their breadth will demand that NATO be better able to provide a coordinated response¹⁵ between Alliance members¹⁶ and also with the international community in the framework of a wider civil-military response¹⁷.

12. Hybrid threats are comprised of, and operate across, multiple systems/subsystems (including economic/financial, legal, political, social and military/security) simultaneously and will therefore prove problematic for NATO's

¹³ NATO Strategic Concept Seminar 1 Oct 09; Summary (new threats).

¹⁴ MC 0550 Para 9 – Potential threats posed to NATO by Terrorism and WMD.

¹⁵ Any future hybrid threats scenario is likely to require far greater integration with (and support to) other international and local actors – at all levels of command, NATO's action will be more closely integrated with the civilian response.

¹⁶ Adversaries may potentially seek to generate hybrid threats that do not elicit an Article V reaction from NATO, thereby preventing a full NATO military and political response.

¹⁷ C-M(2008)0029-COR1 NATO's Contribution to a Comprehensive Approach.

response which would initially focus upon a military/security line of operation. Hybrid threats can expand and contract these lines of operation rapidly to accomplish their objectives.

II.3 KEY CHALLENGE AREAS

13. Analysis of hybrid threats indicates that there are potentially four key *Challenge Areas* that the Alliance will need to address if it is to provide an effective military response to the changing security environment:

a. Environmental Understanding. Hybrid threats may be encountered in a complex, cluttered and potentially urban¹⁸ environment which could encompass a wide range of ethnic groups and cultures, systems and structures that must be understood. Local populations and authorities may be indifferent or sympathetic to NATO's opponents, whilst being one of the Alliance's target Centres of Gravity (CoG). Components of a hybrid threat may cooperate based on perceived common objectives, creating an opposition that could be adaptive over time and difficult to define. Creating and maintaining a detailed comprehension of this environment and its components will be greatly challenging but may be critical in order for NATO to work alongside (and in partnership with) other military and non-military actors in countering hybrid threats.

b. Communication of Action. Hybrid threats may include multiple state and non-state actors with regional/international media access¹⁹ who may seek to discredit NATO's role, legitimacy, credibility and conduct whilst undermining the position of members' national governments. They may be able to exploit the legal complexity of situations where hostilities, terrorism and criminal activities overlap or complement each other and have mutually reinforcing effects. The Alliance could be portrayed as a foreign intervention force with little or no regional or cultural understanding of what is important to the indigenous population, local leaders, and government. The speed at which the adversary uses media against forces and the extent to which misinformation will be used to de-legitimize NATO action may therefore be problematic to disrupt and to counter.

c. Increasing Access to High-end Technology and CBRN Materiel for Non-state Actors. Whilst some adversaries generating hybrid threats could continue to use low-technology methods, the increasing availability of specialist, off-the-shelf and high-end technologies may allow NATO's adversaries to develop their capabilities²⁰ across a wider domain than the conventional battle space, particularly in the areas of space and cyberspace. Identifying the source of the threat will continue to be a challenge for NATO forces. A state actor's ability to

¹⁸ The ability of adversaries to utilize Littoral and Maritime environments must not be underestimated, as was seen during the recent Mumbai attacks (November 2008). An explanation of hybrid threats and implications for Confined Shallow Waters (CSW) can be found within document 28 listed at Annex A; CSW COE 2010 report on countering hybrid threats.

¹⁹ This includes regular media channels and web based enablers.

²⁰ Includes; Electronic Warfare (EW), Laser Technology, Bio Technology, Electro Magnetic Pulse Technology (EMP), Cryptographic systems.

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

sponsor surrogate²¹ organisations could also enable the latter to conduct precise and lethal attacks against NATO and its partners (whilst evading an effective military response). High-value targets²² are now potentially well within the scope of multiple and smaller actors. NATO may face a growing demand for expensive force and infrastructure protection whilst engaging adversaries that are constantly growing in terms of technological ability. The potential availability to such organisations of portable CBRN materiel and weapons will also add a critical dimension.

d. Adaptability and Agility of Actors. Hybrid threats may demand a highly agile response. The ability to engage a conventional adversary remains key but forces may face a rapidly shifting environment that includes the challenge of smaller (potentially *ad hoc*), coordinated and well resourced non-conventional actors. The ability of forces to operate in urban environments is critical - opponents may also be hardly distinguishable from local populations and lack a discernable force structure. They will not consider themselves constrained by international law nor recognise the law of armed conflict; they may be ready to choose from the full range of terrorist, criminal, conventional and irregular means and methods available to them.

PART III – COUNTERING HYBRID THREATS

III.1 TAKING A COMPREHENSIVE APPROACH

14. The Alliance must enhance its ability to participate in a comprehensive approach to countering hybrid threats. Their complexity necessitates a more holistic response with a broader community committed to a common cause. In some aspects, Nations may also need to assume the lead role in countering the threat with the NATO military component in a supporting role²³.

15. Hybrid threats will seek to exploit gaps in both the broader security environment and within NATO's security policy across the entire spectrum of conflict. NATO has a robust policy framework for the physical joint environment, but it should enhance this in partnership with other organisations to provide a more effective response to broader threats (including but not confined to, virtual/cyber, information, financial, psychological). Creating synergy through this comprehensive approach to a hybrid threats response could pose the greatest challenge for NATO and may need substantially increased focus.

16. A NATO military response will be tempered by cultural and social reality within the theatre of operations. It will need to focus on concise and realistic objectives with the requisite resources and sustainment to achieve those objectives (as well as the recognition that NATO may need to adapt rapidly to significant setbacks and elements of mission failure).

²¹ State actors can potentially supply and sustain non state actors through porous international borders and the globalised financial network - evidence from current NATO deployments suggests that weaponry used for hybrid threats against NATO forces has been supplied by states outside the immediate theatre of operations.

²² Potentially including: senior personnel, C2 nodes, computer networks, GPS, radio operating frequencies, capital platforms, social and energy infrastructures).

²³ Example: Defence Against Terrorism Draft Concept Paper and NATO Cyber Defence Policy - specifically for Anti Terrorism as well as in dealing with cyber attacks, NATO offers to assume a supporting role to Nations.

17. NATO may not master every aspect of hybrid threats²⁴. It should however avoid transforming its methods purely to confront a number of identifiable challenges. Adversaries may adapt quickly and the Alliance should ultimately look to impose comprehensive strategic, operational and tactical solutions rather than just attempting to keep pace. It should not rely on a solution that meets the threat on its own terms but must seek to counter by means and methods beyond predictable conventional or non-conventional military responses. Where possible, NATO should also look to negate the need for an actor to become a potential adversary to NATO. This may include utilizing broader political, military and economic incentives.

18. NATO should facilitate a more effective systems approach in the way it conducts its operations; understanding the broader implication of each military action in a complex environment will be key. A singular military action may have far-reaching social or economic consequences for a region or local population. In addition, the Alliance may need to consider unorthodox approaches to partnerships. It must choose its partners²⁵ strategically, focusing on those who will provide genuine and enduring support for the mission.

19. Since hybrid threats arise from a blend of simultaneous actions which may be considered to have one or more different legal parameters, the legitimacy and legality of any NATO response to them will need to be both nested in prudent assessment of the legal dimension of the operating environment and based on relevant international law, including - but not limited to - the law of armed conflict. It is unlikely that a single or generic legal framework will be sufficient to support each different hybrid scenario; hence each one will need to be addressed based on its own factors. In addition, NATO must also be aware and be prepared to counter the likelihood of opponents utilising the legal domain to disrupt and exploit an effective Alliance response.

III.2 A FRAMEWORK RESPONSE

20. This paper proposes that hybrid threats necessitate a holistic framework from which NATO can contribute to a sustainable, effective, and unified response on the basis of a sustainable consensus concerning the legitimacy and legality of Alliance action²⁶. The framework contains four inter-related elements²⁷ but all four may not always be applicable or in the outlined sequential order. They may overlap and/or be relevant before, during, and after military operations. All four may also be in use simultaneously once military forces have been deployed.

III.3 FRAMEWORK ELEMENTS

21. Framework Element I – Building Partnerships and Knowledge

- a. Strategic²⁸ Intent: Reduce potential for conflict; in conjunction with other relevant stakeholders, NATO should identify problematic regions and actors

²⁴ There are certain domains that it will not be able to dominate due to their scale and complexity.

²⁵ Such as non-NATO allies, private contractors, NGOs, IOs, regional nations.

²⁶ This framework aims to support the sovereignty of the HN, enhance the Rule of Law and to protect the population

²⁷ The tasks would be completed by NATO independently or by other actors which NATO would support.

²⁸ A combination of all political, military economic, social and information activities.

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

(state and non-state) that could present a threat in the event of destabilisation²⁹; it builds on any existing regional diplomatic footprint, informs the actors of NATO's (as well as the nations') concerns and objectives, and encourages agreement to tailored NATO and/or NATO Nations' support as appropriate. The Alliance would seek to identify and engage prominent actors (including International Organizations, Private Organizations³⁰, key empowered individuals³¹ and Non-governmental Organizations (NGOs)) whilst developing its own regional (and cultural) understanding.

b. Example Military Contribution: A holistic assessment of the region through the Knowledge Development process which should include: a cultural and intelligence as well as a military-legal assessment of the region (engagement with regional intelligence services); detection and monitoring of likely opponent groups, their leadership and broader cooperation including financing mechanisms; visible support to diplomatic effort by increased Military Assistance; where appropriate, support to the local infrastructure and humanitarian programmes; support to local and regional socio-economic development; low-visibility support to HN SOF; support for capacity enhancement and consolidation of regional Security Sector activities, based on the Rule of Law.

22. Framework Element II – Deterrence

a. Strategic Intent: Deter opponents from aggression and demonstrate NATO capabilities; to communicate to the region, local populations and international audience NATO's intent (in close partnership with others) to deliver a unified, balanced and (if necessary) military response to any threat³² to the Alliance or its supporters' territories, populations and forces.

b. Example Military Contribution: High-visibility military activity and presence; strategic communication to coerce opponents' leadership and alert them to their international vulnerability³³ and lack of own security; where necessary and appropriate, support to disruption of hybrid threat finance activities; detailed intelligence assessment of all potential aggressors and their courses of action; visible effort to track and locate CBRN material; consensual deployment of expeditionary military infrastructure into HN; developing close partnerships with other security providers and relevant stakeholders; support preparations for lawfully authorised economic blockade; robust defence of information networks; on request, support to civilian CBRN Consequence Management assets; isolation of adversaries in areas where there is a high density of disaffected population.

²⁹ This may include the potential dissolution of a nuclear state or one of political or economic significance – the collapse of which may have a direct or indirect effect across all elements of NATO's security.

³⁰ Any co-operation with private contractors should be guided by relevant international law as reflected in relevant NATO Policy.

³¹ Many regions and states have key individuals who are potentially empowered due to economic, political or ethnic status – NATO should also consider such prominent persons within their approach.

³² The current NATO legal and policy framework comprises, among others, NAC-approved Partnership and Cooperation Programmes as well as Non-Article 5 Crisis Response operations or, as the case may be, the invocation of Article 5 of the North Atlantic Treaty. Military responses may include the deterrence of an aggressive cyber campaign against critical Alliance infrastructure, as appropriate.

³³ Could include potential for criminal prosecution outside own country.

23. Framework Element III – Engage the Threat

a. Strategic Intent. Use of NATO military component to force a solution; in addition to active military and security force engagement, NATO - in cooperation with other actors - must contribute to a continued diplomatic and political solution.

b. Example Military Contribution: Military options include but are not limited to: deployment of full combat-capable forces in destabilized regions; operations to stop or contain use of force in support of law-enforcement agencies; comprehensive information operations campaign (to inform and protect local population and influence the adversary); neutralisation of potential tactical and strategic CBRN threats; interdiction of border violations; non-kinetic and kinetic measures against adversary key personnel and leadership³⁴; imposition of selective blockades; disruption of adversary networked systems; further support for capacity enhancement of regional Security Sector activities.

24. Framework Element IV – Stabilization

a. Strategic Intent. Stabilise the area of concern; NATO would support the regional and international community in implementing a sustainable and sufficient solution (and, if applicable, securing a viable end to hostile action), a comprehensive military and political approach based on continuous cooperation with the UN and other non-NATO civilian actors.

b. Example Military Contribution: Reconstruction and stability operations; increased emphasis on regional infrastructure support; monitoring and closure of borders; support to Disarmament, Demobilisation, Reintegration and Reconciliation programmes as well as other arms-control activities; continued consolidation of regional Security Sector activities and support to indigenous security forces; strategic communication to inform the international audience of the progress of NATO's mission; partnering and increased co-operation with regional/local authorities, agencies and International Organisations³⁵; supporting the empowerment of legitimate sub-national leadership³⁶.

25. To counter hybrid threats, Fig 1 demonstrates that NATO must utilise a framework through which it can both support the international community and generate early partnerships (Elements: Build partnerships and Stabilise) whilst engaging adversaries (Elements: Deter and Engage) across all domains (political, military, economic, social and information).

³⁴ Includes; Detainee Operations; kinetic operations will, as a rule, primarily be directed against opponent personnel exercising command and control functions as well as other combat functions.

³⁵ Potentially including Indigenous Capacity Building and Population Protection.

³⁶ Where legally appropriate and on request from international organizations, this may include assisting the apprehension of adversary leadership to facilitate extra theatre or international criminal proceedings.



Fig. 1

III.4 FURTHER CONSIDERATIONS

26. Prevention and deterrence should be the Alliance’s primary focus. Whilst current Policy and Strategy remain relevant³⁷, the threats that NATO currently faces and is likely to experience in the future indicate that the Alliance must consider how it can be more effective in prevention and deterrence. In particular it should explore new, less conventional measures to prevent and dissuade those actors³⁸ unmoved by the capabilities in NATO’s current kinetic and non-kinetic arsenal.

27. Hybrid threats may not be sufficiently reduced in the short term. The Alliance must deliver early and robust measures with an understanding of the need for a long-term comprehensive commitment. As the threats may be adaptable, diverse, and complex, each manifestation will be specific to context. Consequently, NATO may also find it difficult to measure its levels of success, particularly regarding its ability to implement a comprehensive approach and the visible results of its deterrence measures.

28. NATO will need to better understand what constitutes effectiveness against hybrid threats and how it can ascertain a sustainable end to hostile action³⁹. The Alliance must attempt to prevent and contain hybrid threats well before they occur, or respond very rapidly in the aftermath. This may become a measurable as the adversary reduces its activity due to NATO preventative measures and unpredictable counter-measures. This could signify success from a broader perspective because it

³⁷ Annex A; documents 1- 7.

³⁸ Particularly, less easily definable non state actors that consider themselves less vulnerable to a NATO response or not accountable to international law.

³⁹ Strategic Perspectives Journal; *Winning the Counter Insurgency*: Major General Y Amidror; notes the potential use of the term *sufficient victory* in fighting terrorism – when a viable and sustainable end to hostile action has been achieved. Ceasefires against Northern Irish Terrorism and Basque Separatism have also been described as a *repressed quiet*. These may be useful perspectives for NATO in understanding how it determines and assesses a sustainable outcome.

demonstrates that an adversary's ability to pass from intention to action is considerably reduced.

PART IV – KEY IMPLICATIONS FOR NATO

29. The current NATO Policy and Strategy framework⁴⁰ continues to provide a valid structure for dealing with some of the key challenges identified as hybrid threats by this concept paper. It is also noted that positive developments have been made in the strategic environment but that security of the Alliance remains subject to uncertainty⁴¹ and an array of threats that are multi-directional and often difficult to predict (and with potentially great impact on NATO citizens and those of its Allies).

30. Whilst it may be expected that the Alliance's new Strategic Concept will improve NATO's ability to deal with the key challenges identified as hybrid threats, its military implementation will need to ensure a sufficient framework particularly regarding the engagement of multiple and well-resourced non-state actors⁴². NATO's current military guidance⁴³ does not provide adequate depth for security environments for which its forces will need to be better prepared, but are currently insufficiently skilled or proficient⁴⁴.

31. There is no significant doctrinal gap concerning the need to counter most elements of hybrid threats⁴⁵, although there remains a general lack of cohesion across Allied Joint Publications as to how the whole paradigm should be engaged and in some of the definitive terminology.

32. Analysis of hybrid threats and the current strategic and operational frameworks has indicated that the following implications may now need to be considered if NATO is to effectively counter its growing security challenges.

IV.1 ENVIRONMENTAL UNDERSTANDING

33. Implication.

a. The complexity of hybrid threats may necessitate that NATO (military and civilian) education and training programmes now *"prepare their graduates with the ability to think critically and creatively in the conduct of both traditional and unconventional military operations, essentially of blended nature"*⁴⁶. The Alliance will need to engage adversaries that have a greater understanding of the environment in which it is operating⁴⁷.

⁴⁰ Alliance Strategic Concept 1999, MC 400/2, Comprehensive Political guidance 2006, MC 550 Guidance for the Military Implementation of the CPG (supported by Allied Reach 2009 Final Report).

⁴¹ Uncertainty and instability in and around the Euro-Atlantic area and the possibility of regional crises at the periphery of the Alliance, resulting from serious economic, social and political difficulties, territorial disputes or ethnic and religious rivalries which could spill over into neighbouring NATO countries.

⁴² With potential links to terrorism or organised criminality.

⁴³ MC 0550; Guidance for Military Implementation of the CPG.

⁴⁴ Examples; CBRN forensics, Law Enforcement, Cyber Defence, assistance to HN and Local Governance, Joint Operations requiring greater dispersion of forces and command structures.

⁴⁵ Identified specifically as "hybrid" only in AJP-01 (D) RD.

⁴⁶ SACT letter to SG and CMC - MFP 2009 page 4 (not emboldened in original text).

⁴⁷ Hybrid threats will demand that NATO personnel be better educated and informed concerning all aspects of the areas in which it operates; meaning it will need to do more than just speak the language and understand the customs; but develop and execute a plan that protects local customs without weakening NATO's own position.

b. The security environment will change as adversaries adjust their methods and tactics to expose NATO vulnerabilities and circumvent an effective response; this will necessitate that the Alliance and nations adopt flexible and adaptable 'Lessons Learned' processes. NATO may therefore need to support nations in standardizing necessary core skill sets that are needed for countering hybrid threats as well as assisting in the enhancement of interoperability⁴⁸.

c. The complexity of a response to counter a hybrid threat will also demand an environmental understanding through all levels of command and a flexible and agreed decision-making process whenever the nature of threats are not conducive to standard planning processes. The complex threat will necessitate more efficient collection, processing, sharing and fusion of all sources of intelligence⁴⁹ within and between nations, regional and international organizations, NGOs and partners⁵⁰. In addition to traditional military intelligence, this will include the collection, analysis and sharing of information on the social and human elements of the environment and the sharing of intelligence in certain civil areas such as crime (including cyber crime) and proliferation of CBRN materials. Geo-environmental intelligence will also be key. Adversaries may have the opportunity to achieve greater and quicker tactical situational awareness than NATO due to their closer proximity to the population.

IV.2 COMMUNICATION OF ACTION

34. Implication.

a. The ability of potential adversaries to exploit the information medium⁵¹ may demand that NATO adopts a more robust communication policy and a better understanding of what its actions communicate. In some operations, communication of action may be more critical than achieving physical objectives.

b. Against hybrid threats, no one actor controls the information medium. NATO may need to embrace a change of mindset (both operational and in broader cultural terms) by which communication of its action becomes a principal line of operation⁵² as opposed to a supporting action, with increased capacity to inform⁵³ opinions of all actors and stakeholders and facilitate early 'bridge building' and negotiation. NATO will also face difficulty in

⁴⁸ Interoperability for countering hybrid threats must extend beyond the military component and address all aspects of a comprehensive approach.

⁴⁹ Successful HUMINT may become a critical element of the intelligence gathering structure.

⁵⁰ Particularly with regards to cyber space, criminality and CBRN. Increased requirement for the sharing of intelligence may also demand that NATO reviews its current warning systems so that it extends beyond that of just terrorism.

⁵¹ Lebanon 2006 – Hezbollah's use of media and Internet proved problematic for Israel's communication strategy.

⁵² "Contribute positively and directly in achieving the successful implementation of NATO operations, missions, and activities by incorporating Strategic Communications planning into all operational and policy planning" (NATO Strategic Communications Policy). Alliance's communication must project unity and confidence.

⁵³ NATO must avoid accusations of coercion which will destroy trust with partners, stakeholders and target populations - relevant actors should be provided with the information required so they may properly understand and assess Alliance actions and intentions; a vital requirement that promotes Alliance Transparency and Integrity.

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

communicating its actions to less easily definable and more elusive non-state actors that are unconcerned by international accountability. NATO leadership will also face increased pressure to respond effectively in a high-tempo environment where tactical decisions may have rapid impact on both operational and strategic communication of action.

IV.3 INCREASING ACCESS TO HIGH-END TECHNOLOGY AND CBRN MATERIEL FOR NON-STATE ACTORS

35. Implication.

a. Increasing evidence of the potential for cyber attacks upon NATO network systems⁵⁴ combined with Alliance and Nations' growing dependence on superior information and communications technology means that NATO's military is increasingly vulnerable to this aspect of hybrid threats⁵⁵. A growing requirement for partnerships will create a larger cyber footprint which will (by default) require enhanced cyber protection measures. Whilst NATO has a policy⁵⁶ and a concept on Cyber Defence⁵⁷, consideration should be given to developing a concept on the full spectrum of cyber operations and protection⁵⁸.

b. The growing availability of sophisticated off-the-shelf (OTS) weapon technology for non-state actors⁵⁹ will increase NATO's vulnerability significantly. Strikes against high-value targets (civilian and military) could have potentially catastrophic consequences and may necessitate that NATO enhances force protection for military and essential non-military components⁶⁰ most at risk.

c. CBRN⁶¹ attacks will continue to be an area of critical concern, including the potential for action against large-scale civilian industrial/chemical facilities. The threat from rogue states will be exacerbated by geopolitical shifts and broader state sponsorship of non-state actors. Current NATO deterrence and defence are structured primarily to prevent CBRN attacks from state actors but may need to be reassessed to assist in the prevention of proliferation amongst multiple lower-level non-state actors⁶² such as terrorists and criminal networks.

IV.4 ADAPTABILITY AND AGILITY OF ACTORS

36. Implication.

⁵⁴ A broad and complex array of cyber attacks on Estonia's public and governmental networks systems in 2007 were largely unprecedented in scale and provide proof of the vulnerabilities of NATO members to such threats. NATO / NATO-led operations are facing a growing number of increasingly sophisticated cyber attacks, as well.

⁵⁵ Cyber technology has also developed to such an extent that the existing legal framework within NATO is insufficient to counter the threats posed by current and future cyber attacks.

⁵⁶ NATO Cyber Defence Policy 2007.

⁵⁷ NATO Cyber Defence Concept 2008 – MC 0571.

⁵⁸ Includes; protection of Financial, Business, Transport, Energy Supply nodes and Communication networks.

⁵⁹ NATO Strategic Intelligence Estimate 2009. Reduced costs of technology means access has and will devolve further to non state actors and individuals.

⁶⁰ In Operational theatres this may include key infrastructure, economic or other targets assessed as critical to the campaign.

⁶¹ NATO Strategic Intelligence Estimate 2009.

⁶² MC 0550 Para 21. NATO should look to develop Concepts and doctrine for the full spectrum of CBRN Counter proliferation operations

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

- a. NATO's underlying assumption is that it has a collective dominance of the majority of the conflict spectrum. Hybrid threats, however, could constitute a warping of the spectrum of conflict in which periods of high-intensity conventional operations could be encountered in an otherwise low-intensity environment and against a seemingly non-conventional opponent, potentially with state sponsorship and access to high-tech weaponry and resources.
- b. The breadth of threat domains may necessitate that NATO extend its traditional area of military competency and its ability to cooperate with organizations and nations beyond that for which it is currently configured. The Alliance may need to decide which core competencies it wants to focus upon and those for which it may need to rely on non-NATO entities.
- c. The high tempo of multiple hybrid threats may circumvent NATO's planning and execution process. NATO's operational command and control design with a hierarchical decision-making process is not configured to effectively counter such threats in a realistic timescale. This may necessitate that NATO adopts an operational command and control structure that is more dispersed and pushes authority down to lower levels."
- d. NATO should potentially be able to deploy with a 'toolbox of capabilities' and consider more imaginative use of existing forces to anticipate, adapt and achieve rapid operational and tactical superiority. NATO may need to look at how it might improve interoperability of conventional forces⁶³ with specialists⁶⁴. However, a proper balance within the Alliance between specialisation and general flexibility must still be achieved.
- e. Evidence from operational theatres⁶⁵ has also shown that adversaries are able to control large sections of an indigenous population by asserting religious, political and economic influence at the community level. The exploitation of financial networks and legitimate businesses may also mean that NATO needs to improve awareness at all levels concerning *threat finance*.
- f. A cluttered and complex environment will also require that NATO develops more efficient competencies for the detection and attribution of hostile action.

PART V – CONCLUSIONS

37. This Capstone Concept has offered a rigorous analysis of the developing security environment facing NATO; it has found that the complexity of future challenges will necessitate the Alliance adjusts its structures, processes and capabilities in a number of primary areas if it is to provide an effective response to the proliferation of hybrid threats.

⁶³ Analysis of Interoperability shortfalls by JALLC (presented to NATO EWG(I) 12 May 10) listed key shortfall areas which included the following; English language skills, CIS networks, Administrative Procedures, C2 and Situational Awareness, Friendly Force Tracking, Force Capability and Readiness Reporting Standards, Tactical Communications.

⁶⁴ SOF; CIMIC; PRTs; OMLTs.

⁶⁵ Joint Centre for Operational Analysis (US JFCOM) – Journal Volume XI issue supports current ISAF lessons learned regarding Taliban ability to influence and control whole rural communities that are within ISAF AOOs.

38. What is clear is that there is no preclusive view of a NATO response to counter hybrid threats. The range and dimensions of the challenge do, however, stress the need for the enhancement of a comprehensive approach. Many elements of any response to counter a hybrid threat will likely depend on factors outside the current remit of the NATO military sphere; this particularly includes the problematic issues surrounding cooperation with non-military actors and a thorough understanding of the civil-military interfaces required to achieve unity of effort. Therefore it will be necessary to seek guidance from the political domain as to their aspirations for the scope of the military contribution to countering hybrid threats. Consequently, developing policy consensus among NATO Nations in areas beyond the accepted paradigm of military contribution will remain a prominent issue, as will dealing with the broader consequences of rapid technological development.

39. The paper has made observations that will need development in approach due to current constraints and sensitivities; however, as an intellectual discussion of future security challenges, the issues raised are meant to sit 'outside' accepted parameters. It is hoped that it will subsequently provoke debate on emerging hybrid threats and inform decisions on which areas of the Alliance now need to transform. Whilst all challenges and implications discussed in this paper are of significance for NATO, the Alliance must decide in the short and medium term how and what it wishes to adapt.

ANNEX:

A. Documents Reviewed

ANNEX A TO
ENCLOSURE 1 TO
1500/CPPCAM/FCR/10-270038
5000 FXX 0100/TT-6051/Ser: NU0040
DATED: 25 AUG 10

DOCUMENTS REVIEWED

- A. Washington Treaty
- B. Alliance Strategic Concept (1999)
- C. Allied Reach Final Report (2009)
- D. MC 400/2 Guidance for the Military Implementation of Alliance Strategy
- E. Comprehensive Political Guidance (November 2006)
- F. MC 0550 Guidance for the Military Implementation of the CPG
- G. Multiple Futures Project Findings and Recommendations April 2009
- H. NATO's Comprehensive Strategic Level Policy for Preventing the Proliferation of WMD and Defending against CBRN Threats
- I. AJP-3(A) Allied Doctrine for Joint Operations
- J. AJP-3.2 Land Operations
- K. AJP-3.4 Non-Article 5 Crisis-Response Operations
- L. AJP-3.4.4 RD2 Counter-insurgency
- M. AJP-3.5 Special Operations
- N. AJP-3.10 Information Operations
- O. AJP-3.14 Force Protection
- P. AJP-01 (D) RD
- Q. NATO Strategic Concept Seminar 1; Fundamental Security tasks - Summary of Principal Ideas and Issues (October 2009)
- R. NATO Strategic Concept Seminar 2; NATO's Engagement in an era of Globalisation - Key Messages and Conclusions (November 2009)
- S. NATO Strategic Concept Seminar 3; Transatlantic Cohesion NATO and EU (December 2009)
- T. NATO GOE Seminar 4 Summary Report (March 2010)
- U. NATO COTC Final Analysis Report (December 2009)
- V. NATO Strategic Intelligence Estimate (2009)
- W. IMSTAM(INT)-0038-2010
- X. Significant Technological Developments and Military Implications MC165/07
- Y. MC 0571 NATO Cyber Defence Concept April 2008
- Z. Bi-SC Defence Against Terrorism Draft Concept Paper (February 2010)
- AA. HUMINT COE CHT Research Paper (February 2010)
- BB. CSW COE CHT Research Paper (February 2010)
- CC. JCBRN COE CHT Research Paper (March 2010)
- DD. CJOS COE CHT Research Paper (February 2010)
- EE. HQ SACT Intelligence Paper on CHT (March 2010)
- FF. HQ SACT C4ISR CHT Workshop Report (March 2010)
- GG. HQ SACT JET Paper on CHT (March 2010)
- HH. Euro-Atlantic Partnership Work Plan January 2010