



NORTH ATLANTIC TREATY ORGANISATION
HEADQUARTERS, SUPREME ALLIED COMMANDER
TRANSFORMATION
7857 BLANDY ROAD, SUITE 100
NORFOLK, VIRGINIA 23551-2490



Assessing Emerging Security Challenges In The Globalised Environment

The Countering Hybrid Threats (CHT) Experiment

First Impression Experiment Report (FIER)

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

TABLE OF CONTENTS

Executive Summary 3

1. Introduction 4

2. Experiment Overview 5

3. Achievement of Experiment Aim 6

4. Achievement of Experiment Objectives..... 6

5. Assessment of Experiment Execution 7

6. Initial Observations from Experiment 9

7. Preliminary Conclusions & Recommendations.....16

8. Reference Documents18

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

EXECUTIVE SUMMARY

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 the “Assessing Emerging Security Challenges in the Globalised Environment (Countering Hybrid Threats) Experiment”, at the Nordic Forum Hotel in Tallinn, Estonia from 09 – 13 May 2011.

The BI-SC input to a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats (MCCHT) provided the conceptual baseline for the event. Development of the Experiment background documents, scenario, aim, and objectives were also guided by the new NATO Strategic Concept and current work underway on the NATO Comprehensive Approach.

The Experiment Aim “To investigate the utility and feasibility of the MCCHT concept and develop with both military and civilian actors an understanding of potential NATO approaches in addressing the identified key challenge areas” was achieved. Experiment results also indicate that the Experiment generated key information that supports the utility of the draft BI-SC concept, and demonstrates the key issues and challenges raised within it.

A 2016 non-crisis scenario based within fictional Silver and Ivory Seas regions bordering NATO was developed for the event to reflect the range of current and emerging security challenges.

Participants for the experiment were chosen from a wide variety of government, military, and civilian backgrounds. Approximately two-thirds of the participants consisted of non-military personnel. Three panels, organized around the participants functional skill sets and organisational associations, were used to examine the security environment as well as the potential characteristics, capabilities, operating logics, and implications of hybrid threats.

The bulk of collected data requires further analysis and will be presented in the Final Experiment Report (FER); however ten initial overarching recommendations can be made at this point in the analysis:

- Recommendation 1. The concept of hybrid threats is a very useful intellectual model. However it needs further refinement to enable it to offer solutions to the challenges faced by both the NATO and non-NATO stakeholders.
- Recommendation 2. Understanding all the elements of a hybrid threat within a complex environment will require a broader community (including non-military) approach to collecting and sharing early warning indicators and other information to improve situational awareness.
- Recommendation 3. NATO could consider undertaking a continuous risk assessment as part of a ‘risk management’ vice a ‘crisis management’ approach.
- Recommendation 4. NATO needs to work with others to conduct continuous technology reviews of rapidly developing areas.

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

- *Recommendation 5. Without lessening its role in crisis response, NATO should look at how it can evolve and adapt its abilities to prevent future security challenges from developing.*
- *Recommendation 6. NATO should look to better define the nature of its relationships with key stakeholders, and create a sustained dialogue with a counter hybrid threats community of interest.*
- *Recommendation 7. NATO should encourage stakeholder efforts to create policy and legal structures for currently unregulated spaces where non-conventional threats thrive.*
- *Recommendation 8. The private sector has an increased role in the emerging security environment and NATO needs to develop mechanisms to improve engagement with this area of stakeholders.*
- *Recommendation 9. NATO should look to both its current strengths and capabilities to see how they could be adapted to proactively support other stakeholders in countering hybrid threats.*
- *Recommendation 10. NATO should assess where its principal vulnerabilities to hybrid threats lie in order to determine in which areas it must improve and address the key challenges identified.*

1. INTRODUCTION

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 the *Assessing Emerging Security Challenges in the Globalised Environment (Countering Hybrid Threats) Experiment*, at the Nordic Forum Hotel in Tallinn, Estonia from 09 – 13 May 2011.

The Experiment was designed by ACT and Allied Command Operations (ACO) with substantial input from the NATO International Staff (IS), International Military Staff (IMS), USJFCOM JIWC and NDU. It was also developed over several months with input from a broad NATO community of interest including the Joint Warfare Centre (JWC), Centres of Excellence (COEs) and a number of National Representatives.

*The BI-SC input to a new NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats (MCCHT)*¹ (hereafter referred to as the MCCHT Concept) provided the conceptual baseline for the event. Development of the Experiment background documents, scenario, aim, and objectives were also guided by the new NATO Strategic Concept and current work underway on the NATO Comprehensive Approach². The main event principally focussed on Framework Elements One and Two of the MCCHT Concept (Building Partnerships and Knowledge; Deterrence).

The principal motivation for the experiment was to demonstrate the key issues and challenges outlined in the draft concept in order to provide NATO civilian and military leadership with timely and actionable recommendations and identify follow-on activities

¹ Reference 8.4.

² Reference 8.2.

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

that could enable the Alliance to achieve greater unity of effort (within a comprehensive approach) to counter complex hybrid threats.

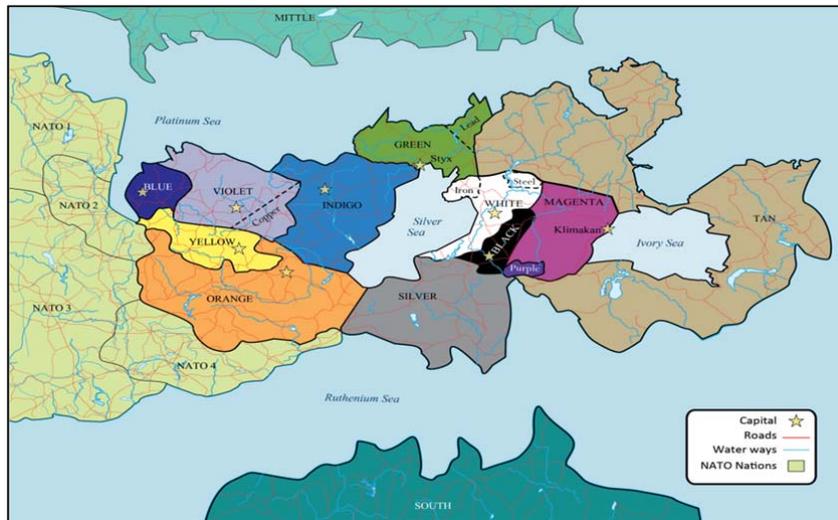
Detailed analysis of the results of the experiment is intended to be used to support transformational work based on the direction expected from 'MC 400/3: Military Committee Guidance for the Military Implementation of NATO's Strategic Concept' and to inform the current work on the NATO Defence and Deterrence Posture Review.

This First Impression Experiment Report (FIER) provides a brief overview of the conduct of the experiment, a general statement of what has been achieved, initial observations, assessments and evaluations related to the experiment planning and execution.

This FIER is submitted for initial situational awareness. The observations, assessments and evaluations are of preliminary status and do not represent the more thorough analysis within the Final Experiment Report (FER).

2. EXPERIMENT OVERVIEW

The aim of the MCCHT Experiment was to “investigate the utility and feasibility of the MCCHT concept and develop with both military and civilian actors an understanding of potential NATO approaches in addressing the identified key challenge areas”. A 2016 non-crisis scenario based within fictional Silver and Ivory Seas regions bordering NATO was used to reflect the range of current and emerging security challenges. The use of a fictional scenario in a so-called 'steady-state', non-crisis environment enabled participants to think about real-world security challenges in a future context without the potential constraints of political sensitivities.



Three panels, organized around the participants functional skill sets and organisational associations, were used to examine the security environment as well as the potential characteristics, capabilities, operating logics, and implications of hybrid threats. The panels were organised as follows:

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

- Cyber, technology and economic security.
- Stabilization, conflict prevention and partnership.
- Global commons and resource security.

All panels were provided with a similar set of research questions to examine through the contextual lens of their particular expertise. Each panel was asked to:

- Analyse and identify potential threats within the complex security environment.
- Identify key stakeholders, their common goals and objectives, and consider how various stakeholders may functionally interact to deal effectively with identified threats.
- Assess potential military contributions for countering hybrid threats.
- Examine the implications for NATO in terms of policies, relationships, partnerships and required abilities needed to effectively counter hybrid threats.

Participants for the experiment were chosen from a wide variety of government, military, and civilian (law enforcement, humanitarian assistance, business, academic, or technology) backgrounds. Approximately two-thirds of the participants consisted of non-military personnel.

A plenary session on Day 1 provided background information and briefings to familiarize participants on the scenario, objectives, and methodology for the experiment. Plenary sessions on Day 2 and 3 allowed panels the opportunity to update all participants on their initial observations. A final plenary on Day 5 summarized each panel's observations and insights for the week.

3. ACHIEVEMENT OF EXPERIMENT AIM

The Experiment Aim was determined as: *"To investigate the utility and feasibility of the MCCHT Concept and Develop with Both Military and Civilian Actors an Understanding of Potential NATO Approaches in Addressing the Identified Key Challenge Areas"*³.

A preliminary evaluation of the results indicates that the Experiment generated key information that both supports the utility of the MCCHT Concept, and demonstrates the key issues and challenges raised within it. It is noted that questions were raised about the feasibility of the concept, which will be investigated further in the final report. In addition, the data collected should identify areas that NATO should now develop with non NATO stakeholders to enable a better understanding of potential hybrid challenges and solutions.

4. ACHIEVEMENT OF EXPERIMENT OBJECTIVES

The IPT and Experimentation Team derived four primary objectives from the Experiment Aim⁴.

³ Reference 8.6.

⁴ Reference 8.7.

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

The achievement of primary **Objectives 1- 3** was deemed as instrumental to experiment success whereas **Objective 4** was identified as a desirable outcome.

The four Experiment objectives were:

- **Objective 1:** Assess the utility and feasibility of the Concept Framework Elements in enabling NATO to counter hybrid threats.
- **Objective 2:** Identify appropriate military contributions within a wider comprehensive approach to countering hybrid threats.
- **Objective 3:** Inform the NAC and the MC in support of NATO Defence and Deterrence Posture Review.
- **Objective 4:** Explore the MCCHT Concept amongst the community of interest.

A preliminary assessment of results indicates that sufficient analytical data was captured to achieve **Objectives 1 – 3**. In addition, the event attracted seventy-five panel members from a wide range of backgrounds⁵ (including Law Enforcement Agencies, International Organisations, Non-Governmental Organisations, Academic Institutions, Business and Industry) and twenty two working observers. Such a breadth of participation also allowed the event to achieve **Objective 4**.

5. ASSESSMENT OF EXPERIMENT EXECUTION

Overall, the execution of the experiment was a resounding success. While there were some minor logistical issues, all were quickly and efficiently resolved through the dedication and commitment of the organizing staff. If anything, time was the only limiting factor. The topic for discussion (hybrid threats in the complex security environment), was so diverse and encompassing that panel analysts were challenged to capture the many observations and insights of the participants. This section will highlight several key factors that were crucial to the experiment’s execution.

5.1. PARTICIPANT BREADTH AND EXPERTISE.

The organizing staff spent considerable time and effort to recruit participants to this event with the appropriate expertise. As the aim of the experiment was to bring together ‘both military and civilian actors’, the fact that two-thirds of the participants came from non-military backgrounds, indicates the success of the recruitment strategy. Participant feedback reflects recognition of the wide range of expertise present at the seminar, which enabled substantive discussions on the character of hybrid threats and a frank dialogue about NATO, civilian, and military functional interaction in dealing with these complex security challenges.

5.2. A LOGICAL, FOCUSED, ANALYTIC APPROACH.

The Experiment staff expended considerable energy developing, refining, and socializing the approach and methodology for this event. Hybrid threats come, by

⁵ Approximately 66% of all panelists at the main event were from a non NATO and non-military organizations.

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

definition, from actors that employ a combination of conventional and unconventional means adaptively to achieve their objectives. As such, they tend to remain ‘under the radar’ and are not easily detectable. By its design, the experiment was a broad effort to look across the spectrum to understand how these potential threats may affect the security of NATO and other stakeholders and identify areas for further examination. A few participants expressed concern that this structured analytical approach may have restricted creative thinking; however, brain-storming without understanding the overall context of the issues would not have produced meaningful results. It was a careful balance that the analytical team tried to take into consideration early in the event’s design.

5.3. CRITICAL IMPORTANCE OF A REHEARSAL.

The conduct of a one day panel rehearsal in late March (utilising JFCOM Foreign Liaison Officers) played a significant role in validating and improving the experiment design, methodology, scenario, research questions, and process for the event. In addition, having experiment leads, senior advisors, facilitators, and analysts conduct a final walk-through two days prior to the start of the experiment undoubtedly contributed to the overall success of the event.

5.4. CONDUCT OF A SITE SURVEY.

The site survey in early April enabled the Experiment staff to gain an appreciation for the infrastructure and support requirements necessary. Important details, such as the availability of computer networks, size and locations of plenary meeting rooms, projection systems, and hotel amenities were clarified and resolved through this site visit. An early site survey allowed for appropriate adjustments critical to smooth functioning of such events.

5.5. USE OF A FICTIONAL, NON-CRISIS SCENARIO SET IN THE FUTURE.

There was considerable debate in the organisational design of this event on whether to use a fictional or a real-world scenario. A real-world scenario may have raised political objections and potentially constrained creative thinking as participants defaulted to debate on what is do-able within today’s security realities. However, a fictional scenario required players to translate a series of hypothetical events and relate it to the complexities of the many organizations, actors, and their roles and stakes in a real-world environment. In this case, the staff created a scenario that provided participants a complex (but not complicated) situation to discuss the implications of potential adversaries and the likely impact on NATO and other stakeholders.

5.6. EMPLOYMENT OF A ‘DEVIL’S ADVOCATE’.

The use of a ‘devil’s advocate’ within the panels served to challenge potential conventional group thinking that may have arisen in discussions. It was a useful function that was planned from the outset of the experiment. In this case however, while the devil’s advocate contributed significantly to the dialogue, the excellent

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

quality of participants were such that there was already a constant challenge to ideas and a frank discussion of the merits and drawbacks of various proposals.

6. INITIAL OBSERVATIONS FROM THE EXPERIMENT

The observations, assessments and evaluations contained in this section are of preliminary status and do not represent a more thorough analysis that will be contained within the Final Experiment Report (FER). They come from observations and questions by participants themselves during the plenary sessions, as well as the observation of the analysis team. They are meant primarily as a summary of some of the key issues discussed. It is recognised that in some areas they may be incomplete.

6.1. WHAT ARE HYBRID THREATS?

At the beginning of the experiment the panels were given the description of hybrid threats from the MCCHT Concept:

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

In the first part of the experiment all 3 panels grappled with what a hybrid threat is based on this description and how the threats developed or linked to the various emerging security challenges in the scenario presented. It was clear that hybrid threats are not new in a general sense, all wars are of mixed character and military forces have always had to adapt to a changing environment and threat; however the experiment audience did outline some areas where new trends are presenting themselves.

In a steady state environment, such as that presented, it was found that many threats and are inter-related with challenging structural issues within the environment (e.g., growth of organized crime, fragile economies, weak political structures, widespread corruption, unresolved territorial disputes, risk of smuggling and cyber threats to critical infrastructure). This leads to questions of how to understand the various indicators of these threats and who is in a position to have the full breadth of information required to take action against them.

During the experiment it was suggested that NATO use the MCCHT Concept to focus attention on the less well understood, non-conventional aspect of the threat. While it is true that NATO understands and is better prepared for conventional threats, it is the dynamic and adaptive combination of conventional and non-conventional means and methods that must be holistically considered. Overall, the concept of hybrid threats was seen as a useful intellectual model, to draw our attention to what is unique about today’s threats.

6.2. WHAT ARE THE MOST DANGEROUS CHARACTERISTICS AND CHALLENGES POSED BY HYBRID THREATS?

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

Adversaries who generate hybrid threats are novel in their ability to exploit certain new and emerging aspects of the contemporary operating environment. For example, hybrid threats reflect the dynamic and complex nature of the steady-state operating environment that seems to defy disaggregation, understanding and centralized planning approaches. The three panels identified a number of characteristics or challenges that hybrid threats pose:

6.2.1. Operating below NATO’s radar complicates detection and response

Adversaries who can employ an ‘indirect’ approach, using a comprehensive combination of political, military, economic, social, informational and legal means, to make slow, steady, incremental progress toward their long-term strategic objectives. hybrid threats can therefore be understood as the employment of a ‘comprehensive approach’ by an adversary against NATO.

As such, hybrid threats could exist at a level and in a manner that is normally below the thresholds for detection or response. Firstly, many indicators of activity lie outside of the traditional military domain. Secondly, as an Alliance, NATO’s threshold for collective response leaves it vulnerable to many aspects of a hybrid threat approach. By operating below the threshold of response, an adversary could enable continuous, incremental progress without the risk of setbacks due to effective military response.

6.2.2 Difficult to Attribute threats and actions to adversaries

Through the use of proxies and the orchestration of a broad combination of actors within a complex operating environment, hybrid threats can be difficult to attribute. This will sometimes mean the hybrid threats are anonymous, or at least are so for the purposes of legitimate response.

If actions could be attributed, dealing with states would be easier (than non-states) as states have more tangible ways to receive consequences of their actions (e.g., sanctions). However, states are increasingly seeking ways to obscure their complicity in actions against other states. By using proxy organizations (e.g., non-state actors, criminal organizations), or by operating anonymously in the cyber domain, direct involvement can be denied.

Consequently, NATO will be tested in its attempts to detect, identify and attribute hybrid threats, and, thus, will be challenged to prevent or deter their actions. Categorizing threats will be necessary in order to identify appropriate responses.

6.2.3. Working in the grey areas inhibits assignment of responsibilities

Hybrid threats can also exist in the legal “grey space” between two areas of responsibility. For example, hybrid threats can blur the line between profit-motivated crimes requiring law enforcement action, and politically or ideologically motivated attacks requiring military action. This is particularly effective against

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

large governmental and bureaucratic organisations, the limits of whose responsibilities are legally defined.

Pre-emptive action to close these jurisdictional gaps in advance of their exploitation by adversaries would facilitate better Alliance response. Categorizing threats is necessary to identify appropriate responses. There must be a basis in law and jurisdictional definition in order to take legal action against actions by adversaries.

6.2.4. Adaptive use of new capabilities and technology that outpaces our ability to respond

New technologies are developing at an exponential rate. Adversaries who generate hybrid threats are capable of adapting dangerous new technologies for operational employment faster than legal regimes and security capabilities can be developed to deal with them. Some areas of particular concern identified were cyberspace technologies, nano-technology, robotics and biological and chemical sciences.

The development of policy structures and legal regimes to regulate the use of emerging technologies requires international and interagency cooperation, which is usually a time consuming process that allows the technology to exist within regulatory vacuums for some time.

Potential adversaries can take advantage of three technology related vulnerabilities: firstly the reliance of modern societies on technology; secondly the almost blind acceptance of the answers provided by technology; thirdly the speed of access to technology which makes it difficult to correct escalating problems.

6.2.5. Increased tempo of action challenges established responses

The globalised world is increasingly instrumented and monitored and most systems are now connected to a network. The developed world in particular, has benefitted greatly from connecting with trading partners, leveraging the internet within the business environment and reducing overall costs by controlling infrastructure through connected control mechanisms. With the availability of that information, information technology infrastructure and interconnectedness, an adversary is enabled to achieve high tempo and complexity in its operations. Global Positioning Systems, satellite phones and GOOGLE Earth for example have allowed actors (for example pirates in the Indian Ocean and Niger Delta, and the Mumbai terrorists) to undertake fairly complex operations.

6.3. IMPROVING UNDERSTANDING OF THE ENVIRONMENT AND THE THREAT

It is important to understand the motivations, relevance and potential sources of legitimacy of adversaries who employ hybrid threats hybrid actors in order to counter them. Deterrence of adversaries is only possible if there is a detailed understanding of the threat. Attaining and maintaining a high level of situational awareness

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

concerning potential hybrid threats is essential to deterring, planning for or conducting operations against such adversaries. Knowledge about their cultural characteristics and conditions, along with their objectives and methods is critical.

NATO has some inherent capabilities to achieve and maintain awareness of these security threats and limited capacities to assess their potential impact on security for the alliance. Because of the associated political, social, economic, and criminal dimensions, other organizations may be better able to understand threat trends and detect warning indicators related to these unique hybrid challenges. Non-military stakeholders in many cases will be the earliest and best source of information to provide the alliance better situational awareness of developing situations. Two key factors for improving situational awareness of potential hybrid threats will be broader information collection and sharing and a continuous assessment of the significance of that information (from which a shared appreciation of the problem can enable all players to act collectively).

6.3.1. Constructing information sharing relationships

There is a broad array of key stakeholders from different sectors who monitor key environmental factors that generate and sustain hybrid threats; particularly those characteristic to the root causes of the problems upon which hybrid threats exist. NATO often does not have direct access to much of this information nor does it have relationships established with key stakeholders monitoring the environment.

In order to receive information from a broader range of sources, NATO will need to reciprocate by sharing information and assessments with these same organizations. Since many aspects of hybrid threats are criminal in nature, the need for law enforcement information sharing was an issue raised in several panels (e.g. national data, INTERPOL data, and financial crimes data). However, it was recognised that there are caveats and firewalls preventing military intelligence in some nations having access to law enforcement data. The panels also discussed the importance of information sharing for cyber-security. There is a need to understand the adversary and risks plus collaborate on information gathering, management and dissemination.

There are, of course, many challenges to information sharing. Some that were identified were:

- Military classification protocols severely limit sharing.
- Proprietary information is usually a very sensitive issue for businesses and thus not always willingly shared.
- Some information sharing practices are considered unlawful (for example if interpreted as price fixing).
- Technical capabilities exist to enhance information sharing but policies and practices block most exchanges at the potential release points.
- Different levels of sharing are recognized and may be needed in different circumstances (i.e. Collaboration, Coordination, De-confliction, and Conflict).

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

- Information release authority varies considerably and exacerbates the issues of sharing and exchange (commander for military, owner for business, judges for police, etc.)

6.3.2. Undertaking continuous strategic risk assessment

All three panels discussed the importance of continuous assessment and re-evaluation of the situation. To this point, civilian stakeholders may often be the best source of information to feed situational awareness and a comprehensive assessment of the environment would also be of value to them as they conduct their normal activities.

There was agreement that NATO could benefit from early threat detection and risk assessments for hybrid threats in steady-state environments; however, one panel questioned whether NATO should adopt a ‘risk management’ approach vice ‘crisis management’. To identify the most pressing risks and threats from a wide range of indicators would require building risk assessments through timely, continuous partner engagement. The key thought was to be proactive and be able to ‘connect the dots’ and react quickly when necessary. Many risk assessment processes currently exist, i.e. from insurance companies, industry, NGOs, UN, and within NATO, however few of the evaluations from these are shared broadly amongst the community of interest.

Hybrid threat activities that occur below the threshold at which NATO would normally react must also be monitored in order to enable NATO to develop situational awareness and act or react appropriately to threat activity. Some participants thought NATO’s current processes do not seem to facilitate early understanding and therefore, do not enable actions to manage an emerging threat through deterrence or crisis prevention.

6.4. COUNTERING HYBRID THREATS.

6.4.1. Being proactive in preventing conflict

The MCCHT Concept suggests a framework approach to countering hybrid threats to provide a holistic solution for dealing with the associated issues. This framework includes building partnerships up-front and deterring emerging threats. In other words, the framework is focused on being proactive and attempting to deter or prevent threats from manifesting in the first place.

The panels concluded that this framework is a logical approach. By being proactive and preventing threats from manifesting in steady state, stakeholders can aim to save future expense in dealing with even more challenging crises. However, it was cautioned that prevention and deterrence may require a concerted effort across the economic, social, infrastructure, information and political domains of action with little investment in the military domain.

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

All panels agreed that this did not mean NATO should be inactive in trying to deter and counter hybrid threats. Areas where NATO could have a role include; improving resilience and reducing duplication of effort and redundancy, supporting efforts to be able to attribute threatening activities and supporting the wider preventative measures that others could take to deal with the root causes.

6.4.2. Creating an adaptive and flexible community of interest that is able to be comprehensive in its approach

Given the complex character of hybrid threats and their enabling environments, the panels identified that the key stakeholders can come from a wide variety of sectors, much broader than the traditional sectors with which NATO may have dealt with in the past.

These key stakeholders have a variety of interests and goals some of which diverge and others which may overlap with those of NATO. This is linked to jurisdictional and organisational mandates for various actors, and may also be situational dependant (especially where policy decisions are involved). Relationships will need to be forged and maintained in a manner that accounts for the dynamic nature of how situations change over time, allowing for the roles and contributions of any given actor to ebb and flow in a manner consistent with their interests. The overall goal may be best described as seeking to build relationships upon a *convergence of interest* rather than development of enduring and common interests.

Consequently in order for NATO to build an effective community of interest to counter hybrid threats, it needs to understand who the key stakeholders are, what their mandate and limitations are, what their interests and goals are and all relative to a situation in order to determine what types of relationship are feasible and desired. To define this the Alliance will need to enter into sustained dialogue with these other stakeholders; communicating and then demonstrating interest in forging such a community of interest will be a critical first step.

6.4.3. Legitimate authorities and legal regulation help enforcement and deterrence

Rapid advances have placed some technology ahead of the policy and legal regimes that are required to regulate its use – leaving unregulated spaces which adaptive adversaries can exploit. The lack of adequate legal and policy frameworks allows opponents to take advantage of the fissures that inevitably develop between international organisations, nations and agencies within nations. This is particularly evident in cyberspace, which by its nature crosses many borders and regulatory boundaries

The development of policy structures and legal regimes to regulate the use of emerging technologies may be an important element in deterring adversaries, but it requires substantial international and interagency cooperation. NATO

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

undoubtedly has a role in supporting the development of those political and legal frameworks.

As NATO looks to support deterrence and prevention of conflict, its actions must be credible, legitimate and proportionate in the eyes of its populations and others within the international community. Ensuring the correct legal framework exists for its activities in countering hybrid threats (and through partnering and working under wider mandates provided by the international community) will help NATO to do so.

6.4.4. Working with the private sector.

Hybrid threats, by their description (as those posed by adversaries that combine both conventional and non-conventional ways and means including potential action in the economic and social spheres), blur the division between conflict and competition, and therefore, the public and private sectors, drawing the latter more directly into the conflict space.

Furthermore, with 85% of the infrastructure that supports the internet being in private hands, use of technology by adversaries will drive the need for constructive dialogue with private enterprise and academia to develop robust, concerted and overarching approaches to defence in this environment.

NATO should subsequently look to improve its engagement with the private sector and industry. The desire to maintain stable economies and access to resources will provide incentives for the private sector and academia to enter into this dialogue.

Including the private sector within a comprehensive approach to countering hybrid threats will not be easy. There links between authorities, ownership, privacy and liabilities are unclear and this will increase the difficulty in identifying structures for collaboration that will be acceptable to all stakeholders.

6.4.5. Using current strengths and capabilities in adaptive ways

All three panels investigated what NATO could do to support deterrence and prevention of hybrid threats and concluded that the emphasis should not be about building new capabilities or expanding its charter but exploiting its existing capabilities to greater effect.

Some of the strengths and roles that were articulated by participants were:

- NATO can provide a strong international forum for bringing various experts from different backgrounds together to discuss emerging security challenges.
- NATO could provide leadership, mechanisms, and support (as appropriate) to help develop multi-lateral processes, standards and modus operandi to deal with a number of emerging threat areas.

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

- NATO and the military could support creating comprehensive mentoring, education and training opportunities where there are security challenges of common interest.
- NATO has strong partnership programs with other nations that can be used to facilitate stronger cooperative security.
- NATO could help shape robust mechanisms for the sharing of information within the broader community of interest, particularly in identifying pre-crisis warning indicators.

7. PRELIMINARY EXPERIMENT RECOMMENDATIONS

Further to the initial analysis of the data collected and in particular the panel's observations, the following are the preliminary recommendations:

7.1. Recommendation 1. The concept of hybrid threats is a useful intellectual model to draw attention to what is new and most challenging about today's threats and emerging security challenges. However, it needs further refinement to enable it to offer solutions to the challenges faced by both NATO and the broader range of non-NATO stakeholders.

7.2. Recommendation 2. Understanding all the elements of a hybrid threat within a complex environment will require a broader community approach from collecting and sharing early warning indicators and other information to improving situational awareness. From this community effort a shared appreciation of the problem can enable all players to act more effectively.

7.3. Recommendation 3. NATO could consider undertaking a continuous risk assessment as part of a 'risk management' vice a 'crisis management' approach in dealing with emerging security challenges.

7.4. Recommendation 4. NATO needs to work with others to conduct continuous technology reviews of rapidly developing areas.

7.5. Recommendation 5. Without lessening its role in crisis response, NATO should look at how it can adapt and evolve its current abilities to prevent future security challenges from developing.

7.6. Recommendation 6. NATO should look to better define the nature of its relationships with key stakeholders and create a sustained dialogue with a countering hybrid threats community of interest who might be engaged in addressing elements of the security environment or the emerging threats themselves. Within this dialogue NATO should be flexible in the nature of its relationships, which may vary according to actor interests, mandates and jurisdictions.

7.7. Recommendation 7. NATO should encourage efforts to create policy and legal structures for currently unregulated spaces where hybrid threats thrive. These in turn will help provide legitimacy for and effective response.

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

7.8. Recommendation 8. The private sector has an increased role and concern with some emerging security challenges. NATO needs to develop mechanisms to improve engagement with this sector above and beyond traditional procurement relationships.

7.9. Recommendation 9. NATO should look to its strengths and current capabilities and see how they could be adapted to proactively support countering hybrid threats. Possible first steps include: Continued external engagement on particular issues of common interest; conducting exercises with external participants on areas of common interest such as: stabilisation & reconstruction, cyber security, energy security.

7.10. Recommendation 10. NATO should assess where its principal vulnerabilities to hybrid threats lie in order to determine in which areas it must improve and address the key challenges identified.

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

8. REFERENCE DOCUMENTS

- 8.1. PO(2010)0169, The Alliances Strategic Concept, 19 Nov 2010.
- 8.2. PASP (2011) 0174 23 Feb: Updated list of tasks for the implementation of the comprehensive approach action plan and the Lisbon summit decisions on the Comprehensive Approach.
- 8.3. PO(2011)0019-REV 4 Terms of reference of the DDP.
- 8.4. IMSWM-0330-2010, Bi-SC input for a new Capstone Concept for the Military Contribution to Countering Hybrid Threats, dated 29 Sep 10.
- 8.5. IMSM 0292-2010 Hybrid Threats description and context, dated 31 May 10.
- 8.6. 5000 TSC FRF-0250/Ser: NU067716 Dec: After Action Report of the Countering Hybrid Threats (CHT) Experiment Main Planning Conference (MPC); Movenpick Hotel, Geneva, Switzerland (01 – 03 Dec 10).
- 8.7. 5000 TSC FXX-0100/Ser: NU0142: After Action Report (AAR) of the Countering Hybrid Threats (CHT) Experiment Final Planning Conference (FPC), Brussels, Belgium (09 - 11 March 11).

EXPERIMENT LEAD & FIER POC1:

Richard Hills
Lt Col (GBR) Royal Marines
Deployable Forces IPT
HQ SACT TSC PAX 0070
Phone: (001) 757-747-3268
IVSN: 555-3268
Fax: (001) 757-747-3863

ANALYSIS LEAD & FIER POC2:

Mr Alex Smethurst
GBR Civ A-2
Operational Analysis Branch
HQ SACT TSC FEA 0120
Phone: (001) 757-747-4271
IVSN: 555-4271
Fax: (001) 757-747-3863

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

DISTRIBUTION:

External –

Action:

IS/ASG ESC (Dr Jamie Shea, D. Ruiz Palmer, CV Heimferte, F. Perret)
IS/ASG PASP (L Meyer-Minnemann)
IS/Comprehensive Approach Task Force
IMS/P&P/A Branch (Col A. Budd, Col R. Lakin, Maj C. Romano)
NATO liaison to United Nations
SHAPE COS
SHAPE/ CPP
SHAPE/MCD
SHAPE/FOR
Joint Warfare Centre, Stavanger, Norway
Center for Analysis & Simulation for the Preparation of Air Operations (CASPOA)
COE, Taverny, France
Cooperative Cyber Defence (CCD) COE, Tallinn, Estonia
Combined Joint Operations from the Sea (CJOS) COE, Norfolk, USA
Command and Control (C2) COE, Ede, The Netherlands
Confined and Shallow Waters (CSW) COE, Kiel, Germany
Civil Military Cooperation (CIMIC) COE, Enschede The Netherlands
Defence Against Terrorism (DAT) COE, Ankara, Turkey
Human Intelligence (HUMINT) COE Oradea, Romania
Joint Air Power Competence Centre (JAPCC) COE, Kalkar, Germany
Joint Chemical, Biological, Radiation & Nuclear Defence (JCBRN) COE, Vyškov,
Czech Republic
Military Engineering (MILENG) COE, Engelstadt, Germany
COS, US JFCOM
USJFCOM JIWC
EUCOM
National Defence University (CCO, CTSS)
Senior Advisor (Ms Mary Beth Long)
Senior Advisor (Mr Sverre Diesen)
Senior Advisor (Mr Yves de Kermabon)
Senior Advisor (Sir Mike Aaronson)
Individual; all Experiment Participants

Internal –

Action:

POLAD
DCOS SPP (All Branch Heads)
ACOS CAP ENG
ACOS CAP REQ
DF IPT, CHT IPT
SACT NLRs/PNLRs
List III (HQ SACT DIR 35-1)

NATO CHT Experiment FIER	Version: Final
Co-Authors & POC: Experiment Lead: Analysis Lead TSC FEA 0120	Issue Date: 20 Jun 11