



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

Final Experiment Report (FER)

Final Experiment Report (FER) Authorship

This report prepared by:

Experiment Lead Analyst:

- Mr Alex SMETHURST, HQ SACT Operational Analysis Branch

In co-operation with:

Name	Organisation
Mr. John CALDWELL	IDA on behalf of US JIWC
Mr. David COCHRAN	US JIWC
Mr. Greg CONOVER	IDA on behalf of US JIWC
Mr. Han DE NIJS	HQ SACT
Ms. Caroline EARLE	IDA on behalf of US JIWC
CDR. Frank GROTHUSEN	COE CSW
LTC. Richard HILLS	HQ SACT
Mr. Leen NIJSSEN	HQ SACT
Mr. Kenny PERRY	US JIWC
Mr. Mark TOCHER	HQ SACT
Mr. Mark VINSON	IDA on behalf of US JIWC
Mr. Adrian WILLIAMSON	NATO JWC

EXECUTIVE SUMMARY

Background

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” in Tallinn, Estonia from 09–13 May 2011.

The principal motivation for this Experiment was to provide greater depth to the work already completed within the BI-SC Concept “The Military Contribution to Countering Hybrid Threats (MCCHT)” and to explore its impact amongst a broader community of stakeholders.

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. The development of the experiment background documents, scenario, aim and objectives was guided by the new NATO Strategic Concept and work underway on the NATO Comprehensive Approach.

The results of the Experiment will provide an opportunity to revise the current BI-SC Capstone Concept, which will subsequently inform the development of a NATO policy paper.

Experiment Execution

The aim of the experiment, which was achieved, 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”. The Experiment findings support the utility of the BI-SC Concept and its further development; they also support the need for an action plan to develop solutions to the issues and challenges raised within it.

A 2016 non-crisis scenario was developed for the event to reflect the range of current and emerging security challenges.

Participants in the experiment were chosen from a wide variety of government, military, and civilian backgrounds (two-thirds of the participants consisted of non-military and non-NATO personnel). A detailed overview of participating organisations can be found in Annex A to the FER.

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 panel groupings were:

Panel 1 – Cyber, Technology and Economic Threats.

Panel 2 – Conflict Prevention and Partnership.

Panel 3 – Global Commons and Resource Security.

Scope

The experiment concentrated on the strategic and operational level implications for NATO within a pre-crisis and steady state environment and, in particular, explored Framework Elements One and Two of the MCCHT Concept Paper: Building Partnerships and Knowledge; and Deterrence.

The event focussed on providing greater detail concerning the following four areas:

1. Understanding the emerging security environment and hybrid threats.
2. Dealing with the emerging security environment and hybrid threats.
3. Determining the implications for NATO alongside partner nations and organisations.
4. Assessing the utility and feasibility of the MCCHT Concept.

Analysis

The analytical findings from the experiment are based on a triangulation of three data sources: the work of the participants; the independent observations of the analysis team; a survey of relevant documentation. Findings and recommendations have been written thematically, or topically, within three subject areas related to the MCCHT and the

objectives of the experiment. The principal recommendations that follow have also been grouped under the three areas as follows:

1. Understanding hybrid threats and the emerging security challenges that they pose.
2. Being proactive: preventing or deterring hybrid threats.
3. Adopting a comprehensive approach to countering hybrid threats.

Principal Recommendations

A. Understanding Hybrid Threats and the Emerging Security Challenges that they Pose

What are Hybrid Threats?

- Continue to examine hybrid threats as a provocative and useful way to draw attention to what is new, complex and dangerous in the emerging security environment. Although components of hybrid threats are important, there is a need to examine them from the perspective of their multi-level inter-relationships.
- With hybrid threats potentially providing a very broad characterization of threat, NATO should try to prioritize the hybrid threats that it faces. It should primarily consider the probability of occurrence of the threats and their potential to have an impact on member nations.
- NATO should examine its own vulnerabilities with its current capabilities measured against different potential hybrid threats in order to understand better the risks that are posed.
- The description of hybrid threats should be further developed and socialised, both within NATO nations and externally with other relevant non-military and non-NATO stakeholders and partners.

Understanding the links between hybrid threats and other key challenges in the emerging security environment

- Seek to manage hybrid threats holistically, rather than in a purely military or security perspective. Devise better the indicators for hybrid threats that may not present

themselves initially in the military or security domains, but also during a steady state or pre-crisis situation.

- As security and rule of law are key contributors to a stable region in a steady state and pre-crisis situation, NATO should determine how it can expand further its assistance to relevant regional and local actors during these stages.
- Develop a mechanism for improving the categorization and prioritisation of hybrid threats. This might include risk-based assessments of the likelihood of occurrence and the potential impacts.

Adversaries operate below NATO's traditional thresholds of detection and response

- Develop and expand existing mechanisms for gathering and sharing threat warnings and indicators so as to include emerging security challenge areas.
- Further identify and then engage organisations (including non-military and from the business and private sectors) with which it can collaborate to attain early indication of hybrid threats.
- Consider the development of appropriate policies to identify response thresholds concerning the key areas that hybrid threats are likely to emanate from – particularly the cyber domain.

Adversaries operate in the peripheries of global environments and the grey areas of legal and enforcement responsibilities

- To provide legitimacy to act in a proactive manner to effectively counter cyber threats, NATO will need to:
 - Further develop policy and protocols for its own response to such threats.
 - Support international action to provide regulations, legislation and common enforcement of cyber space in order to combat illegal activities.
- Identify (and, when appropriate, advocate) the potential for closing gaps between military and law enforcement areas of responsibility. Explore opportunities to provide a better forum for sharing information with the law enforcement community on issues that cross security, military, financial, cyber and criminal boundaries.

- Explore opportunities to expand engagement with the financial sector in order to share information about, and develop appropriate responses to, criminal activities that have an impact on security and defence.

Adversaries adapt new capabilities and technologies for their use faster than NATO can respond

- Interact with other stakeholders (particularly the private sector) to monitor rapidly developing technologies with the potential of being used in innovative ways by adversaries.
- Advocate and promote the expansion of national and international regulations or 'arms control' type regimes to new technologies that it considers dangerous or a growing threat to its security.

B. Being Proactive – Preventing or Deterring Hybrid Threats

What is NATO's role in deterrence and prevention against hybrid threats?

- Develop improved mechanisms and processes for:
 - Intelligence and information sharing with the non-NATO and non-military community on emerging security challenges.
 - Collaboration with external partners on timely and relevant assessments against hybrid threats.
- Reach out and expand relationships with a larger community of stakeholders that can help to identify emerging trends that could affect the security of the Alliance.
 - Develop links with law enforcement and financial institutions to monitor emerging security trends.
 - Improve mechanisms for working with scientific and research communities to monitor and understand the potential impact of emerging technology developments, particularly cyber.

- NATO should augment its planning processes in a manner which allows for more efficient informal information sharing with those unable to participate directly.
- ACT should investigate further how hybrid threats can be built into NATO exercises and how a wider community of interested organisations can participate in NATO training and exercise opportunities.
- ACT should investigate how it can integrate the concept of hybrid threats into the NATO defence planning process to understand better what capability changes may be needed to counter the new challenges.

Indicators and Information Sharing for Situational Awareness and Early Warning

- Develop relationships with key civilian stakeholders (including those that may not initially be receptive to doing so) who are better placed to monitor key environmental factors linked to hybrid threats – this will enable development of necessary situational awareness.
- For early warning, as well as situational awareness, NATO should augment its intelligence fusion capability with data related to cyber security, law enforcement and financial intelligence.

Risk Assessment and Management of Hybrid Threats

- Review crisis management processes to determine whether they are suitable for non-crisis decision-making in a dynamic, steady state, security environment. This could include:
 - An examination of how the Alliance conducts 'risk and threat management' relative to 'crisis management'.
 - Examine crisis management terminology and processes to determine whether NATO should include or reflect risk and threat management standards and processes used by non-NATO organizations.
 - Review Chapter 2 of the NATO Crisis Response Manual to determine its adequacy and responsiveness for steady state (non-crisis) preventive actions.

- Explore development of a network for engagement, through a risk assessment and integration body, which could feed situational awareness for risk assessment and contingency planning. The NATO Shipping Centre could be evaluated as a model for this network.

Strategic Communications

- Determine whether a 'counter-messaging' approach is appropriate and feasible as part of the strategic communications required for countering hybrid threats.

C. Adopting a Comprehensive Approach to Countering Hybrid Threats

Role of Interests in Creation and Sustainment of a Community of Relevant Stakeholders

- Once NATO has determined who the key non-military/non NATO stakeholders are, it must understand their mandate, limitations, interests and goals (relative to the situation) in order to determine what type of relationship is feasible and desired. Key to gaining this understanding is:
 - Recognizing and differentiating between true, enduring, and near-term interests of stakeholders.
 - Recognising which are the most feasible areas of common purpose for NATO and the range of potential partnerships.
 - Developing methods for learning and understanding changing stakeholder interests over time (from the stakeholders' perspectives).

Relevant Stakeholders, Relationships, and Possible Partnerships in Countering Hybrid Threats

- Review current mechanisms for collaboration with industry, with a particular focus on key emerging security challenges.
- In line with the ambitions stated in NATO's 2010 Lisbon Summit declaration, NATO should commit to developing deeper relationships and cooperation with the UN, EU

and OSCE, which focus on the emerging security challenges in a pre-crisis and steady state environment.

Mechanisms for Developing Relationships

- Continue the efforts to include potential partners in the planning and execution of NATO training and exercises. Policy on training must reflect this.
- Review human resource processes to enable the hiring of staff with the understanding of a variety of approaches to emerging security challenges.

Leadership and Achieving Unity of Purpose within a Comprehensive Approach to Countering Hybrid Threats

- Develop a strategy for early engagement and relationship building with key communities of interest prior to emergence of crises, in order to establish a level of familiarity and trust required to work together in addressing hybrid threats.

Pre-conditions that would facilitate NATO's ability to move towards a Comprehensive Approach.

- Communicate to political leaders the nature of the hybrid threats facing the Alliance with recommendations for pursuing a comprehensive approach to counter these hybrid threats. Solicit the political support needed to execute the steps required to create a functional and effective community of interest to prevent, deter, and, if necessary, defeat hybrid threats.

Measuring Success of a Comprehensive Approach to Countering Hybrid Threats

- NATO should explore avenues to produce objective evaluations of progress within a comprehensive approach to countering hybrid threats; here, NATO should base measurements and metrics upon internationally agreed standards and consider the feasibility of utilizing independent evaluators to collect metrics data and provide independent evaluations of progress.

DISTRIBUTION

External –

Action:

IS/ASG ESC

IS/ASG PASP

IS/Comprehensive Approach Task Force

IMS/P&P/A Branch

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 –

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

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)

TABLE OF CONTENTS

ASSESSING EMERGING SECURITY CHALLENGES IN THE GLOBALISED ENVIRONMENT.....	1
EXECUTIVE SUMMARY	3
DISTRIBUTION	11
TABLE OF CONTENTS.....	13
1. INTRODUCTION.....	16
1.1 Aim of Report.....	16
1.2 Scope of Report.....	16
2. EXPERIMENT OVERVIEW.....	18
2.1 Experiment Aim	18
2.2 Experiment Objectives	18
2.3 Experiment Design & Architecture	18
2.4 Experiment Participation	19
2.5 Scenario	19
2.6 Experiment General Execution	20
3. ANALYSIS OVERVIEW	22
3.1 Data Collection and Analysis Method.....	22
3.2 Factors Affecting the Analysis.....	23
4. HYBRID THREATS & EMERGING SECURITY CHALLENGES.....	25
4.1 Overview: Key challenges.....	25
4.2 What are Hybrid Threats?.....	26

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

4.3 Understanding the links between hybrid threats and other key challenges in the emerging security environment.....28

4.4 Adversaries operate below NATO’s thresholds of detection and response32

4.5 Hybrid threats are difficult to attribute to an origin or sponsor34

4.6 Adversaries operate in the peripheries of global environments and the grey areas of legal and enforcement responsibilities.....36

4.7 Adversaries adapt new capabilities and technologies for their use faster than NATO can respond.....39

4.8 Adversaries increased tempo of action can challenge NATO’s established responses43

5. BEING PROACTIVE: PREVENTING OR DETERRING HYBRID THREATS.....45

5.1 Is it more appropriate for NATO to try to Deter or Prevent Hybrid Threats?45

5.2 What is NATO’s role in deterrence and prevention against hybrid threats?.....48

5.3 Indicators and Information Sharing for Situational Awareness and Early Warning54

5.4 Risk Assessment and Management of Hybrid Threats.....57

5.5 Strategic Communications60

6. TAKING A COMPREHENSIVE APPROACH TO COUNTERING HYBRID THREATS63

6.1 The Role of Interests in Creation and Sustainment of a Community of Relevant Stakeholders.....63

6.2 Relevant Stakeholders, Relationships, and Possible Partnerships in Countering Hybrid Threats67

6.3 Mechanisms for Developing Relationships.....76

6.4 Leadership and Achieving Unity of Purpose within a Comprehensive Approach to Countering Hybrid Threats79

6.5 Preconditions that would facilitate NATO’s ability to move towards a Comprehensive Approach.83

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

6.6 Measuring Success of a Comprehensive Approach to Countering Hybrid Threats:.....84

7. SUMMARY OF KEY RECOMMENDATIONS88

8. REFERENCE DOCUMENTS93

9. ACRONYMS95

10. POINTS OF CONTACT.....97

ANNEX 1: Experiment Participation98

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 principal motivation for this Experiment was to provide greater depth to the work already completed within the BI-SC Concept “*The Military Contribution to Countering Hybrid Threats (MCCHT)*” [Reference 8.1], and to explore its impact amongst a broader community of stakeholders.

The results of the Experiment will provide the opportunity to revise the current BI-SC Concept which will subsequently inform the development of a NATO level Concept and NATO policy paper.

This Final Experiment Report (FER) follows on from the First Impressions Experiment Report (FIER) [8.2] and contains a detailed account of the Experiment, findings and recommendations.

1.1 Aim of Report

The aim of this Final Experiment Report (FER) is to provide a full record of the Main Event including a comprehensive set of findings, conclusions and recommendations. The recommendations will help the Alliance to determine how it wishes to execute the countering hybrid threats programme of work and which of the key challenges in the emerging complex security environment it wishes to address (in terms of potential areas where current capabilities can be adjusted). It will also help to inform all related products and programmes of work.

1.2 Scope of Report

The Experiment concentrated on the strategic and higher operational level implications for NATO within a pre-crisis and steady state environment and in particular explored

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

Framework Elements One and Two of the MCCHT Concept Paper; Building Partnerships and Knowledge; Deterrence. The event focussed on providing greater detail concerning the following four areas:

- Understanding the emerging security environment and hybrid threats.
- Dealing with the emerging security environment and hybrid threats.
- Determining the implications for NATO alongside partner nations and organisations.
- Assessing the utility and feasibility of the MCCHT Concept.

This FER details the findings from the experiment. These are based on a triangulation of three data sources: the work of the participants; the independent observations of the analysis team; a survey of relevant documentation. Findings have been written thematically or topically within three broad areas related to the MCCHT and the objectives of the experiment:

- Understanding Hybrid threats and the key challenges that they pose.
- Being proactive in countering hybrid threats: Identifying, deterring and preventing them.
- Taking a comprehensive approach to countering hybrid threats.

2. EXPERIMENT OVERVIEW **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”[8.2].

2.2 Experiment Objectives

The Integrated Project Team derived four primary objectives from the Experiment Aim. [8.2]. These 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 North Atlantic Council (NAC) and the Military Committee in support of the NATO Defence and Deterrence Posture Review.
- **Objective 4:** Explore the MCCHT Concept amongst the community of interest.

2.3 Experiment Design & Architecture

The experiment was conducted as a stand-alone event at a conference venue in Tallinn, Estonia. It was designed to allow broad discussion and analysis of a high level and overarching concept by a largely civilian audience. The design needed to enable the team to capture discussion and analysis that would inform three key lines of development for ACT:

- Assessing the Draft BI-SC MCCHT Concept.
- Identify potential links to the Comprehensive Approach (CA) Action Plan.
- Inform the Defence and Deterrence Posture review.

Consequently, the event was designed to address four key sets of Top Level Research Questions which would provide the substantive discussion to address the three lines of development.

- Understand the security environment and hybrid threats.
- Dealing with the security environment.
- Determine the Implications for NATO alongside partner nations and organisations.
- Assess the utility and feasibility of the MCCHT Concept.

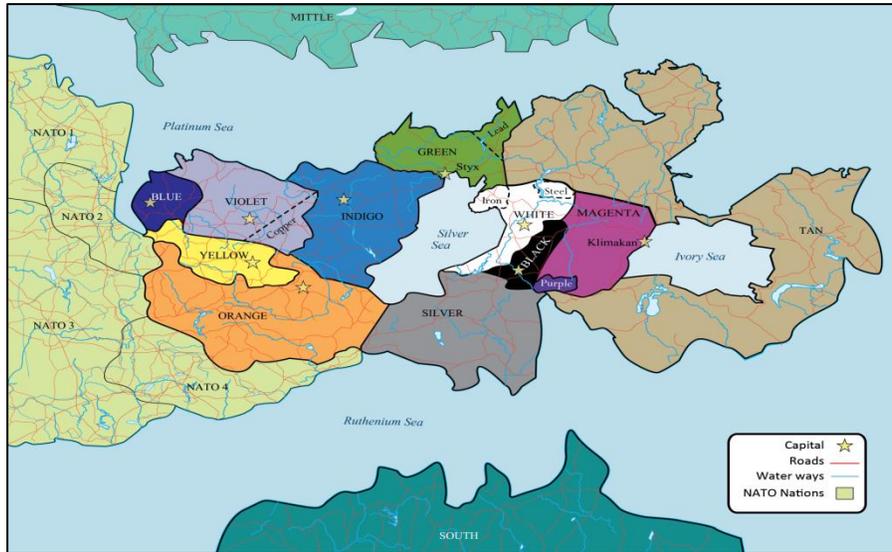
The Top Level Research questions were in turn broken down into a number of sub research questions to reach the required granularity of information and discussion amongst the participants

2.4 Experiment Participation

Experiment Participants were recruited from a broad range of backgrounds (military and non-military) and approximately 66% of the participants came from the public, private and industrial sectors. A more detailed list of the breakdown of participant background and experience can be found at Annex A.

2.5 Scenario

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. Further detail on the scenario can be found in reference 8.3.



2.6 Experiment General Execution

The experiment was executed in one working week. Participants were grouped into three distinct panels based on their background and subject matter expertise.

The panel groupings were:

- Panel 1 – Cyber, Technology and Economic Threats.
- Panel 2 – Conflict Prevention and Partnership.
- Panel 3 – Global Commons and Resource Security.

Each of the three panels were also populated so that they had a range of background and expertise including NATO/Non-NATO, Military/Civilian and Government/Non-Government.

All three panel groupings were given the same complex hybrid scenario and research questions to answer although the groupings of expertise enabled the three panels to consider the issues through a different “lens” of expertise

Each panel was briefed on the background scenario, strategic guidance and the main concept. They were then were facilitated through a set of research questions.

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

Panel members were asked to assess the issues from their own perspective and that of their organization. The panels were given time to conduct in-depth, focused analysis based on their functional expertise. Then within the panel they synthesized output to arrive at key issues and insights. Finally, findings and Q&A were presented in plenary to share awareness across all panels,

3. ANALYSIS OVERVIEW

3.1 Data Collection and Analysis Method

Through the design of the experiment, participants were asked to explore a scenario using a structured set of questions that led them to the following:

- Understand the security environment and hybrid threats within a scenario, and articulate how they would do so in reality.
- Form a plan or approach for countering the threats and dealing with the complex security environment.
- Determine the Implications of addressing hybrid threats for NATO alongside partner nations and organisations.
- Through undertaking the previous activities, assess the utility and feasibility of the MCCHT Concept.

As each panel followed the above line of reasoning and debated the answers, they were asked to record conclusions that they drew and present the key issues back in plenary at three points during the week.

In addition, a small team of observers and recorders sat with each panel. This analysis team made independent observations based on the discussion of the panel participants regarding the nature of hybrid threats and the potential implications for NATO. They were provided with a separate list of research questions to observe and comment against. All observers were selected both for their professional knowledge of particular subject areas and their analytic independence.

Finally, a relevant NATO and non-NATO documentation was collected prior to, during and post the experiment that could be used to 'baseline' the opinions and evidence against current policy, doctrine or written academic opinion.

The findings detailed in this report are based on a triangulation of these three data sources: the work of the participants themselves, the independent observations of the analysis team and a survey of relevant documentation. The analytical team has used all three sources to

write up findings thematically or topically within three broad areas related to the MCCHT and the objectives of the experiment:

- Understanding Hybrid threats and the key challenges that they pose.
- Being proactive in countering hybrid threats: Identifying, deterring and preventing them from action.
- Taking a comprehensive approach to countering hybrid threats.

Each topic has been written-up in the following format:

Observation: Overview/summary of the main point within the topic.

Discussion: Summary of the discussions that took place during the experiment and the observations from the analysis team that articulates the main issues within the topic.

Further Analysis (where needed): Details any further relevant analysis based on current NATO documentation or other references that were not available or used during discussions in Estonia.

Conclusions: Summary of main conclusions drawn about the topic.

Recommendations: Actionable recommendations for the way ahead.

The analysis team recognises that the topics identified across the three broad areas in the findings are interrelated and so readers may find themselves coming to the same or similar conclusions or recommendations from different parts of the report.

3.2 Factors Affecting the Analysis

There are a number of factors that affect the depth and rigour of analysis contained in this report:

- Classification: The classification of the experiment was 'Non-sensitive information releasable to the public' in order to allow for a free and easy discussion and debate amongst all participants. This report is intended to summarise findings at the same classification level. This prohibits analysis against relevant NATO policy, doctrine or systems that are classified. In cases where this would be beneficial it is

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

recommended that this analysis take place and be documented for NATO release only.

- Scope of the topic under discussion: The breadth and strategic level of the topics debated during the experiment means it has been impossible to analyse all areas with full depth of expertise and research. In some cases the report indicates areas that really require further research and study before actionable recommendations can be made. In the preparation of this report the time and resource has not been available to do so.
- Knowledge and background of participants: In an experiment of this form the findings are subjectively dependent on the knowledge and subject matter expertise of the participants. Where possible, skilled and relevant participants were brought to the experiment to provide the best judgement and maximum effort has been made to check assertions made during the experiment against documentary evidence.

4. HYBRID THREATS & EMERGING SECURITY CHALLENGES

4.1 Overview: Key challenges

NATO's new *Strategic Concept* identifies the need for "...NATO's evolution, so that it continues to be effective in a changing world, against new threats, with new capabilities and new partners." [8.4].

The BI-SC input to a new NATO Capstone Concept for the MCCHT identifies these "new threats" as *hybrid threats*, and describes them as: "*those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives.*" [8.5].

In order for NATO to identify hybrid threats, NATO must improve its understanding of these threats and their linkages to other key challenges in the emerging security environment. Furthermore NATO must be able to discriminate hybrid threats by their key characteristics, capabilities and operating logics.

Participants were asked to assess these challenges during the CHT experiment. Key points were captured under the following sub topics:

- What are hybrid threats?
- Understanding the links between hybrid threats and other key challenges in the emerging security environment.
- Adversaries operate below NATO's threshold of detection and response.
- Hybrid threats are difficult to attribute to an origin or sponsor.
- Adversaries that utilise hybrid threats operate in the peripheries of global environments and the grey areas of legal and enforcement responsibilities.
- Adversaries adapt new capabilities and technologies for their use faster than NATO can respond.
- Adversaries' increased tempo of action due to new technologies can challenge NATO's established responses.

4.2 What are Hybrid Threats?

Observation

The experiment participants endorsed the utility of describing the new aspects of contemporary conflict within a concept as hybrid threats, but they submitted that hybrid threats were not new, since most conflicts are of mixed character and consequently military forces have often had to adapt to a changing environment and array of threats.

Discussion

Based on the MCCHT concept's description [8.2] several panels summarized the idea of hybrid threats as similar to that of conflicts of mixed character. Further, they submitted that most conflicts were of mixed character and that military forces have usually had to adapt to a changing environment, threats, and new technologies. As a result, the panels concluded that, in a general sense, hybrid threats are not a new phenomenon. Most participants recognized that, whilst it is not a new phenomenon, the term 'hybrid threats' could be a useful intellectual model to draw attention to today's threats in order to allow NATO to consider how it should respond.

NATO's superiority in conventional and nuclear capabilities has forced its adversaries to adapt and seek new approaches to achieve their objectives. In looking at how NATO might profit from employing the terms hybrid threats, some participants suggested that it might use the concept to focus on non-conventional aspects of threats. NATO understands and is better prepared for conventional threats whilst hybrid threats imply a requirement for the dynamic and adaptive employment of conventional and non-conventional means and methods. Typically, hybrid threats are examined through a focused, military or law enforcement lens and not in a broad holistic and interconnected approach.

All three panels identified difficulties with understanding the nature of hybrid threats based on NATO's description, how the threats developed and how they were linked to the various emerging security challenges within the scenario. One panel posited that hybrid threats describe a complex operating environment that includes a multi-dimensional set of emerging security challenges that confront conventional approaches to conflict rather than an identifiable adversary. The idea that hybrid threats describe the complex operating environment encourages a broader approach. Conversely, the participants asserted that identification of an adversary was considered necessary if the concept of hybrid threats was to be developed in more depth. The conceptual articulation of hybrid threats may more

usefully describe an approach to conflict rather than a specific actor type in a contemporary operating environment.

Some participants interpreted hybrid threats as threats from non-state actors, whereas others suggested that they could be categorized as state, state-sponsored non-state (e.g., terrorist or insurgency organizations), and criminal actors. It was widely accepted that a key word in the hybrid threat description was adaptive. Hybrid threats may best be used to characterize an adversary employing an adaptive mix of means and methods.

Whilst simultaneous use of conventional and non-conventional means describe a threat that is hybrid, employed literally it excludes compound threats (uncoordinated and different forces, using conventional and non-conventional means, in the same space and within the same time). Identifying all adversaries that orchestrate a mix of means and methods is potentially more useful for NATO. An example of this mix is the cooperation of politically or ideologically motivated actors and opportunistic criminals. Such cooperation has blurred the line between military operations and law enforcement and therefore blurring of means and methods is a key distinguishing characteristic of hybrid threats

Hybrid threats can also be understood as the employment of a comprehensive approach by an adversary. In this interpretation, hybrid threats are not solely military threats, but they combine effectively political, economic, social, informational and military means and methods. Adversaries who pose a hybrid threat employ a comprehensive approach with the speed and agility normally associated with unity of command.

Conclusions

Hybrid threats are not adversaries, but describe adversaries who blend adaptively conventional and non-conventional means and methods (both military and non-military) to accomplish their strategic objectives.

Adversaries who pose a hybrid threat avoid NATO's strengths and focus on its weaknesses; consequently they are a real and current threat to Alliance member nations. They might be a cooperative consisting of state, non-state, terrorist and criminal actors; originating from a complex security environment; using a patient, incremental approach to achieve progress toward their strategic objectives.

The concept of hybrid threats has utility as an intellectual model or provocative label, to draw attention to what is most challenging about today's threats and emerging security

challenges. The term hybrid threat focuses NATO's discussion and thinking about what is new about contemporary threats and the operational environment.

Hybrid threat terminology is not understood fully nor agreed within the Alliance or externally with potential cooperative security partners and stakeholders. Consequently, additional efforts are required to both clarify and socialise the ideas of hybrid threats.

Recommendations

1. Continue to examine hybrid threats as a provocative and useful way to draw attention to what is new, complex and dangerous in the emerging security environment. Although components of hybrid threats are important, there is a need to examine them from the perspective of their multi-level inter-relationships.
2. With hybrid threats potentially providing a very broad characterization of threat, NATO should try to prioritize the hybrid threats that it faces. It should primarily consider the probability of occurrence of the threats and their potential to have an impact on member nations.
3. NATO should examine its own vulnerabilities with its current capabilities measured against different potential hybrid threats in order to understand better the risks that are posed.
4. The description of hybrid threats should be further developed and socialised, both within NATO nations and externally with other relevant non-military and non-NATO stakeholders and partners.

4.3 Understanding the links between hybrid threats and other key challenges in the emerging security environment

Observation

In a steady-state environment, such as that presented in the experiment scenario, it was found that many threats are inter-related with challenging structural issues within the broader environment. (i.e. the growth of organized crime, fragile economies, weak political structures, widespread corruption, unresolved territorial disputes, smuggling and cyber threats to critical infrastructure). This leads to questions of how to understand both the complex environment and the various indicators of these threats. There is also a need to

understand better the necessary balance of NATO's focus between the root causes of threats and the symptoms.

Discussion

Hybrid threat actors can operate from the problematic areas of the complex security environment such as: the safe havens of weak, failing or uncooperative states; the anonymity of the cyber domain; and the grey areas and that exist between, legal regimes or enforcement responsibilities. As such they reflect the dynamic and complex nature of the steady-state operating environment that seems to defy disaggregation, understanding and centralized planning approaches.

Participants identified a number of key security issues associated with hybrid threats including: weak or fragile economies with high unemployment; weak governance and poor public administration; widespread corruption; the growth of organized crime; smuggling; unresolved territorial disputes; insurgency; terrorism; cyber-crime and cyber-attacks affecting national security. Many of the issues are interrelated, for example; corruption leads to weakened government structures, supports organized crime and allows smuggling whilst cyber-crime or attacks may be symptoms of the higher-level problems of corruption and organized crime.

Some issues, such as ineffective governance and rule of law, and weak or fragile economies may be characterized as root-cause or structural problems causing instability and fostering the emergence and sustainment of hybrid threats. These issues tend to be deeper, and more fundamental; they will generally require long-term solutions to address them. Other issues associated with hybrid threats, may be characterized as symptoms stemming from the root-cause issues. These issues might be addressed temporarily with short-term solutions but until the root-cause issues are dealt with, the symptomatic issues are likely to return. Since hybrid threats are multi-dimensional, it may be necessary to address both the symptoms and the root causes with a holistic approach in order to effectively counter them.

Weak governance, fractured economies (including the existence of informal economies) and prolific crime are all closely linked, but the underlying issue is often weak governance. Without strong governance and effective political institutions (rule of law), formal economies cannot develop and crime will flourish. A weak economy is in itself potentially a root cause requiring a line of effort in any approach to addressing security issues. The existence of an informal economy provides opportunities for threats to stability and security. Enabling economic growth and development is a principal way to create, in the long term, an environment that would be inherently hostile to the growth and sustainment of hybrid

threats. Initiatives to enhance economic development however should be led by national or regional groups that have been invested with legitimacy by appropriate legal authorities.

Security is seen as an essential precondition for economic development and growth. In addition to security, NATO could also provide a range of other support capabilities (transportation, medical, communications, etc.) that would assist with economic development and growth. Activities in this arena would potentially bring NATO into relationships with a wide range of NGO's. Security of indigenous infrastructure was also seen as important to building the confidence necessary to encourage business investment in developing areas.

Criminal issues may also indicate a future security threat and could potentially be used as an early indicator of a hybrid threat. For example, piracy is an illegal activity that might transform into a hybrid threat if not dealt with effectively. The initial source of piracy is usually economic, often within the context of high unemployment within a failed state. Local police may be corrupt and ineffective in these areas, providing a secure sanctuary for the pirates. As the piracy profits grow, the "business" becomes more organized and attracts new partners. Should one of those partners be an international terrorist organization, the illegal criminal activity of piracy transforms into a hybrid threat, since it is now an extension of, and providing funding for, its terrorist partner. This highlights the need for information sharing with the law enforcement community on particular issues that cross security and criminal boundaries. Similarly insurgents could be identified as a symptom of a root cause that might relate to weak governance or economy.

It may however be difficult to attain long-term public and political support to address the root-cause issues and thus the focus for NATO may more feasibly be on shorter-term solutions to the immediate security issues at hand. Whether issues are root causes, symptoms or vulnerabilities, they are all linked to each other, and therefore, require action. Categorizing security issues as root-cause issues or symptoms, classifying them as either issues requiring either short- or long-term solutions, or binning them as either military or non-military issues may contribute to the development of an approach to dealing with them; however, all of these issues are linked and will require a holistic approach. For NATO to take action, participants suggested that issues be prioritized based on their likelihood and impact. .

The indicators and warnings of hybrid threats may appear as random and disconnected activities, such as: anonymous cyber-crime and attacks; sporadic, but deadly, terror attacks; threatening actions (from ambiguous origins), by proxy non-state organizations and organized crime syndicates; ominous attacks on vulnerable critical infrastructure (such as

power grids and financial institutions); profitable smuggling and piracy operations that challenge the economies and enforcement capabilities of weak and failing states; and nascent development of potentially catastrophic chemical and biological weapons. However, by the time these indicators of hybrid threats appear, root-cause issues in the complex security environment have already developed and evolved to support their existence. Consequently the early indicators that must be monitored in order to prevent hybrid threats from coming into being are the political, economic, and social indicators of a weak or failing state and a disenfranchised population.

The key deduction is therefore 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 about them. There was strong consensus from participants that in order to understand the root causes of issues in an area requires engagement with regional stakeholders and those directly affected by the problem.

Finally it was raised that it is important to understand the motivations, relevance and source of legitimacy of actors who utilise hybrid threats in order to plan the response to them. Deterrence is only possible if you are able to understand the threat.

Conclusions

Understanding the nature, cause and effect of security issues is a necessary step prior to developing an approach to dealing with hybrid threats. Hybrid threats are a part of a larger set of emerging security challenges and the result of root-cause issues in the environment. Therefore, Hybrid threats will require efforts to address multiple security and root-cause environmental issues simultaneously.

Employing short-term solutions without addressing root-causes issues will not lead to a successful result. It will be necessary to address both the symptoms and the root-causes in order to counter effectively hybrid threats. Given present fiscal constraints, NATO's ability to commit to long term efforts to address issues may be limited to focusing on priority security challenges and it will need to consider how best to support other stakeholders in a more comprehensive effort

Approaches to countering hybrid threats must include efforts by stakeholder organizations to improve the effectiveness of governance and rule of law, reduce corruption and organized crime, develop the economy and diminish, deter or prevent hybrid threat activities.

Categorizing a hybrid threat also includes identifying priority issues. Security issues associated with hybrid threats may be prioritized based on the potential impact and

likelihood of their occurrence. Categorizing threats with other stakeholders will aid in the development of relationships and expand communication.

Understanding all the elements of a hybrid threat within a complex environment will require a broader community approach to collecting and sharing early warning indicators and other information to improve situational awareness. From this community effort a shared appreciation of the problem can enable all players to act in their best interests.

Recommendations

5. Seek to manage hybrid threats holistically, rather than in a purely military or security perspective. Devise better the indicators for hybrid threats that may not present themselves initially in the military or security domains, but also during a steady state or pre-crisis situation.
6. As security and rule of law are key contributors to a stable region in a steady state and pre-crisis situation, NATO should determine how it can expand further its assistance to relevant regional and local actors during these stages.
7. Develop a mechanism for improving the categorization and prioritisation of hybrid threats. This might include risk-based assessments of the likelihood of occurrence and the potential impacts.

4.4 Adversaries operate below NATO's thresholds of detection and response

Observation

Adversaries can employ an 'indirect' approach, using a combination of political, military, economic, social, informational and legal means, to make slow, steady, incremental progress toward their long-term strategic objectives. As such they can operate at a level and in a manner that is normally below the threshold for detection or response by NATO.

Discussion

Hybrid threat actors may employ an 'indirect' approach, using a combination of political, military, economic, social, informational and legal means, to make slow, steady, incremental progress toward their long-term strategic objectives. As one panel suggested, hybrid threats could be understood as the employment of a 'comprehensive approach' by an adversary towards dislocating NATO or NATO nations.

As such, hybrid threat actors can operate at a level and in a manner that is normally below the thresholds for detection by the Alliance. Many indicators of activity will lie outside of the traditional military domain or will not manifest themselves as clear military threats. Indicators may also appear as random or disconnected events from across different domains, making the overall threat difficult to identify and characterise. For example, motivations may not be clear because they are financial, political or ideological, and actions may not be easily attributable because they are undertaken by criminal, non-state or state-proxy actors. Indicators and warnings may therefore need to be gathered and shared with other relevant organizations that already collect them. This will include both non-NATO and non-military organisations.

As an Alliance, NATO's threshold for collective military response is high enough that many aspects of a hybrid threat actor's approach will occur without triggering a traditional military response. Specifically, actors will operate below NATO's Article 5 threshold of an attack against NATO member states. By operating below NATO's threshold of response, an adversary can potentially enable continuous, incremental progress without the risk of large setbacks due to significant military action. They can also potentially undermine the legitimacy of a NATO response.

Although NATO's thresholds for military response are somewhat specified in order to provide a deterrent effect, their use is also sufficiently ambiguous due to the requirement for political consensus. While the utility is obvious, it can be argued that such thresholds are inherently contextual and thus essentially impossible to set. Further, while a Nation may be able to set a threshold, it is very difficult for an Alliance to set one as it depends on the individual Nations assessment of the threat to it - and, arguably more importantly, the public opinion of the threat. Ambiguous thresholds for action by the Alliance could also have advantages as adversaries do not know how far they dare go. Whilst NATO may currently have ambiguous thresholds due to a lack of political agreement inherent in the Alliance, such a situation it may have strengths in preventing the escalation of hybrid threats by potential adversaries. When considering some emerging security challenges such as cyber-attack, NATO will however have to consider how far it goes in specifying when and to what extent it will take action in order to provide a prevention and deterrence effect.

Conclusions

Actors posing a hybrid threat conduct operations and activities using a 'comprehensive approach', therefore attaining a holistic understanding requires a broad, rather than purely

military or security, perspective. In order to achieve cognizance of potential hybrid threats, NATO will need to share situational awareness with other stakeholders.

There is a requirement to develop mechanisms, relationships and abilities to address threats that deliberately operate below NATO's threshold for a military response.

Recommendations

8. Develop and expand existing mechanisms for gathering and sharing threat warnings and indicators so as to include emerging security challenge areas.
9. Further identify and then engage organisations (including non-military and from the business and private sectors) with which it can collaborate to attain early indication of hybrid threats.
10. Consider the development of appropriate policies to identify response thresholds concerning the key areas that hybrid threats are likely to emanate from – particularly the cyber domain.

4.5 Hybrid threats are difficult to attribute to an origin or sponsor

Observations

Through the use of proxies and the orchestration of a complex mix of actors within a complex operating environment, actions taken by hybrid threat actors can be difficult to attribute. This will sometimes mean the hybrid threat actors are anonymous, or, at least, cannot be held legally responsible for the purposes of a legitimate response.

Discussion

Hybrid threat activity is not only difficult to attribute to a proximate adversary or actor, but also to the identity of its originator or sponsor. Hybrid threats may be the result of ambiguous cooperation between sponsor states, terrorist and insurgent organizations, organized crime syndicates, corrupt governments, or individual actors, such as hackers or singular terrorists. Adversaries may attack their targets indirectly in order to cause a misidentification of the source or to hide their complicity.

Attributing and categorizing threats is necessary to be able to identify appropriate responses. If a threat is from a criminal actor or if a law is broken, then legal actions can be

taken. If a non-state or criminal organization is under the effective control of a state, then their actions can be legally attributed to the controlling state and appropriate action taken.

Responding to threats attributed to a state is often simpler than dealing with non-state organizations as there are more tangible and legitimate ways to impose consequences on states for their actions: for example with the use of economic sanctions. However, states may deliberately seek ways to obscure their complicity in actions against other states, by using proxy organizations such as non-state actors or criminal organizations, or by operating anonymously in the cyber domain. By doing so direct involvement in an offensive action can be denied. NATO will be challenged in trying to identify and attribute some aspects of hybrid threats, and therefore respond to their actions.

Attribution is a known issue in the case of cyber-attack and cyber-crime. The complex and relatively unregulated space of the internet makes tracing actors responsible for attacks or crime particularly difficult. As the internet is a global tool it is often impossible to trace or attribute attacks without international cooperation.

NATO primarily identifies itself by its nations and its national or geographic borders. By comparison individuals and groups now have greater opportunities to identify with non-state ideologies or movements that transcend state borders. Thus, there is a requirement to understand how people and groups identify themselves and be able to deal with them as groups that may not identify with a nation-state. Many current terrorist, ethnic religious or political movements transcend national borders but are linked by an overarching idea or vision and the use of the global web and media networks.

Conclusions

It will be challenging for NATO to attribute elements of hybrid threats or particular actions taken by adversaries if they are conducted by non-state actors and groups; this will limit its freedom of action. Where possible, attributing actions to a state will provide NATO more options for response but this is potentially a limited method of dealing with a complex threat environment. NATO will need to understand better how non state actors and groups identify themselves, their likely strategic intentions, their partnerships with state actors and likely methodologies.

In an increasingly interconnected world, it is difficult to identify particular adversaries in advance; categorizing threats by their trends, motivations, means and methods may be necessary in order to develop appropriate and legitimate measures to prevent or deter threat actor activity.

In some environments, in order to legitimately attribute threats and actions, NATO will need to work with a broad range of actors to understand the complexity and source of hybrid threats and their non-state perpetrators. This will particularly apply to the issue of cyber defence, networks and law enforcement.

4.6 Adversaries operate in the peripheries of global environments and the grey areas of legal and enforcement responsibilities

Observation

Adversaries operate increasingly in the unregulated and ill-defined environments between areas of fixed responsibility. For example, hybrid threat actors may operate with intentions ranging between profit-motivated crimes requiring law enforcement action, and politically or ideologically motivated attacks requiring military action, thus raising legal and jurisdictional questions that might prevent legitimate response. This may be particularly effective against large governmental and bureaucratic organisations, the limits of whose responsibilities are legally defined.

Discussion

Actors that pose hybrid threats often operate in the grey area between profit-motivated crimes, requiring law enforcement action, and politically or ideologically motivated attacks, requiring military action. These actors are more than military forces and may seek to operate with ambiguous intent and means. Conflict with them may be disguised as business competition, as both will be characterized by the adaptable employment of a mix of means and methods to gain advantage over a competitor.

As such, criminal activity may indicate a future security threat and should be a trend of interest to NATO. There must be a basis in law and jurisdictional definition in order to take legal action against adversaries using criminal means. Wherever possible, proactive work to close the legal and jurisdictional gaps in advance of their exploitation by adversaries would facilitate better Alliance deterrence and response. An example of this lies within piracy; pirates have had to be released from captivity due to a lack of a legitimate basis and means of prosecution. Intent to commit piracy is only illegal in a limited number of states.

The cyber domain is another good example where actors exploit legal seams or grey area that lack sufficient regimes and enforcement capabilities to enable their control. Cyber "crime" may not be done for profit, but for more pernicious reasons, such as to wreck

currencies or to destabilize a financial system. Therefore, the line between cyber-crime and cyber-attacks of financial institutions can be blurred, especially without a clear understanding of attribution and intent. Cyber-crime can be a major money maker for organized crime or other non-state actors or corrupt state actors. NATO nations are particularly lucrative targets, thus it is in NATO's interest to address cyber security issues at its source, no matter where it is.

As the cyber domain is global in its reach and not constrained by geographic borders, it requires a comprehensive, international approach in order to enable its effective control. The lack of international trust and cooperation required to legally control the cyber domain has resulted in it becoming an area that is particularly vulnerable to exploitation by hybrid threat actors, both for the disruptive effects of cyber-attacks and for the economic and financial effects of cyber-crime. Cyber-crime and cyber-attacks are global threats in that they can be conducted from sanctuaries against global targets. Sanctuaries for cyber-crime or cyber 'war' may include states with weak governance and law enforcement capabilities or uncooperative states that may use cyber-crime or cyber-attacks to their advantage against competitor states.

Further Analysis

NATO ACT has begun to study some of these grey areas with its study of the global commons [8.6]. A preliminary report by the Security and Defence Agenda drew some conclusions that strongly support insights gained from the CHT experiment. Namely that, *“Modern adversaries will avoid open military confrontation with NATO. Rather, they will focus on areas where the use of military power is not suitable and where the negative impact on western society is highest: maritime transit in support of economic growth and development; critical cyber infrastructure; and space-based communication networks. Concrete steps must now be taken to increase international cooperation to prevent and better manage crises that may threaten access to the Global Commons.”* [8.7]

The SDA report further highlighted the challenges in the cyber domain and stated that, *“Cyberspace, the wild west of the global commons, is a domain characterised by speed, automation, anonymity and a rapid pace of technological advancement, rendering it a very difficult environment for security actors. Vital international financial transactions and confidential alliance military data traverse the cyberspace domain. Yet the relatively low cost of a sophisticated attack makes it an asymmetric field. A major cyber-attack has the potential to destroy fundamental infrastructures on a massive scale. “There is thus dire*

need for urgency in improving NATO cyber defence as cyberspace has already proven to be an area of immense vulnerability.”

The SDA report underscored the need for a collaborative effort in dealing with threats in the cyber domain, stating that, “Intercepting cyber-threats will require NATO to rely upon the assistance of non-military security services, as well as the technical co-operation of industry experts. Cyber security effectiveness requires trans-national cooperation”.

Conclusions

The potential links, cooperation and blurring of objectives between adversaries who wish to utilise the financial and cyber domains but for different objectives (political and ideological versus the motivation of profit) means that there will be difficulties for the international community in apportioning responsibility to deal with various threats; the distinction between the response by law enforcement and military actors will be unclear.

The presence of organized crime and cyber-crime may be indicators of an emerging hybrid threat. The financial sector may be a willing partner in approaches to understand and counter hybrid threats, because it has a lot to lose to organized crime activities. The use of financial security regulations is an effective way to enforce cooperation with financial institutions.

The practicality of crime attribution and law enforcement of the cyber domain must be developed further to address this legal grey area, but this is long-term requirement that will require substantial international trust and cooperation. There is also no current evidence to suggest that legal structures will be able to solve this issue. To support this NATO and nations should advocate for international action to address cyber threats. In the near-term, improved information sharing relationships related to understanding, preventing, deterring or responding to cyber threats should be pursued.

Recommendations

11. To provide legitimacy to act in a proactive manner to effectively counter cyber threats, NATO will need to:
 - a) Further develop policy and protocols for its own response to such threats.
 - b) Support international action to provide regulations, legislation and common enforcement of cyber space in order to combat illegal activities.

12. Identify (and, when appropriate, advocate) the potential for closing gaps between military and law enforcement areas of responsibility. Explore opportunities to provide a better forum for sharing information with the law enforcement community on issues that cross security, military, financial, cyber and criminal boundaries.
13. Explore opportunities to expand engagement with the financial sector in order to share information about, and develop appropriate responses to, criminal activities that have an impact on security and defence.

4.7 Adversaries adapt new capabilities and technologies for their use faster than NATO can respond.

Observation

New technologies are developing at an exponential rate. Hybrid threat actors are capable of adapting dangerous new technologies for operational employment faster than legal regimes and security capabilities can be developed to counter or control them. Some areas of particular concern identified were cyberspace technologies, nano-technology, robotics and biological and chemical sciences.

Discussion

Current hybrid threat actors are both novel and dangerous in their ability to exploit certain new and emerging aspects of the contemporary operating environment. For example, hybrid threat actors have adapted commercially available, rapidly developing, high technology capabilities for creative employment in operations.

Potential NATO adversaries can take advantage of three technology-related vulnerabilities: (1) the reliance of modern societies on technology; (2) the almost complete acceptance of the answers provided by technology; and (3) the speed of access to technology which makes it difficult to correct escalating problems. For western nations, and to a growing extent in developing nations, most basic services are linked inextricably to technology. Banking, electrical and water services, and food distribution are fundamentally accomplished through technology and as such are susceptible to disruption. Populations have displayed a growing acceptance of what is seen and heard on the media which leaves them open to manipulation and persuasion through sophisticated means. As the human interface is gradually removed technology systems are increasingly connected to other systems providing ways for nefarious manipulation of key networks. This also increases

the speed with which disruptions in technology can cascade throughout the initial and associated networks compounding the consequences of the initial disturbance.

New technologies are developing at an exponentially fast rate as illustrated by Moore's Law¹. Technology developments may pose a significant security threat and require constant monitoring to maintain awareness of the opportunities and potential threats they may present. For example, cyber technologies are rapidly developing and are already being used effectively against nations yet until recently NATO had not updated its policy and planning regarding cyber security.

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 extended periods

Availability to adversaries of radiological and nuclear technology is a critical issue, but, since they are fairly stable technologies (and with non-proliferation policies and enforcement regimes are already in place), they pose perhaps lower future risk than chemical and biological materiel. Chemical and biological technologies are evolving rapidly and present critical challenges. The potential related issues are substantial; for example, unregulated genome technology development and bio-hacking, organ theft, DNA use and bio havens (states with little or no laws and enforcement for bio research).

Actors that pose hybrid threats have also exploited global communications technology and the media to influence the public and political will of their opponents. NATO's adversaries can exploit the internet and social media through malicious and false propaganda. They can also be used to increase the transparency of government and military actions in conflict; for example, a picture posted on the internet or social media can be used to undermine a government's version of events.

¹ Moore's Law, initially postulated by Gordon E. Moore the co-founder of Intel, describes the long-term trend that shows that the number of transistors that can be placed inexpensively on an integrated circuit doubles approximately every 18 months resulting in a doubling of computing speed. This trend has continued for more than half a century and is expected to continue until for some time to come.

As such, actors that pose hybrid threats can use global communications and social media to move NATO's centre of gravity to its public and political support and drive a more immediate and persistent need for accountability.

The rapid development of technologies that may represent a significant threat if misused i.e. chemical, advanced biological, artificial agents, nano-technology, smart grids; Twitter (now being used as a 1st responder tool)) is already a significant challenge for the international community. Nefarious manipulation of such capabilities to connect to devices (i.e. disrupting pacemakers, turning off or overloading power grids) is well within the capacity of smaller non state actors. The business sector remains the primary element in the technology development field and currently NATO is not being engaged sufficiently by business. This should and must change but will require overtures from NATO. There are potential ways of dealing with these growing concerns and an ombudsman approach can be used to monitor technology threats and their development whilst the social media should be developed as a tool to build trust. Arms control regimes must also be kept at the forefront of new technology weapons development. NATO could and should be involved across this spectrum. The Internet was developed without security controls as their need was not anticipated but it may already be too late to resolve this issue; by comparison. Biotechnology is just reaching a point where it is a prime candidate for the development of control measure.

Further Analysis

Within NATO, the efforts to predict emerging and disruptive technologies have been disjointed. Recent work within the RTO Systems Analysis and Studies (SAS) Panel to develop a methodology for predicting disruptive technologies has been positive, but the full and persistent application of the methodology has suffered from a lack of resources. Within the NATO Defence Planning Process (NDPP), it is well understood that technological improvement over the coming decades will be one of the most important drivers in determining long term requirements. This has resulted in actions to develop a persistent technology horizon scanning activity to keep current with emerged and emerging technologies that could be disruptive or present a threat or opportunity for NATO. In previous decades much of the technological innovation started within defence industry for military applications and then extended into the commercial domain. More recently, it has been seen that innovation brought about by research and technology within industry and academia has been the principal driver within the commercial domain which then leads to the discovery of military applications. This makes the private sector a key player in any exploration of future technology and its application. The key for NATO will be to develop a

persistent methodology for technology horizon scanning that incorporated and provides value for all key stakeholders and players across the commercial and military domains.

Conclusions

Technology is developing at a rapid rate and must be constantly monitored and assessed for opportunities, risks and potential threats. Where technologies are anticipated to be potentially dangerous, NATO should advocate that they be targeted for the proactive development of regulations, legal or political restrictions and enforcement mechanisms.

As well as the speed of development of technology, potential adversaries to NATO can take advantage of the reliance of our nation's societies on network systems and the increasing acceptance of the answers provided by technology. NATO must prepare contingencies to operate without many aspects of modern technology and network systems should the need arise.

The private sector (including business, industry and academia) is a primary player in the technology development field. They must be engaged by NATO as a stakeholder when monitoring and predicting future technology development and to assist in the understanding of potential new solutions and uses for safety and security.

NATO requires a legitimate basis for its actions and transparency with its home public in order to enable long-term public and political support for its contributions to countering a hybrid threat.

Recommendations

14. Interact with other stakeholders (particularly the private sector) to monitor rapidly developing technologies with the potential of being used in innovative ways by adversaries.
15. Advocate and promote the expansion of national and international regulations or 'arms control' type regimes to new technologies that it considers dangerous or a growing threat to its security.

4.8 Adversaries increased tempo of action can challenge NATO's established responses

Observation

The world is increasingly instrumented, monitored and connected to a network. With such a breadth of available information, information technology infrastructure and interconnectedness, hybrid threat actors are enabled to achieve high tempo and complexity in their operations, particularly at the tactical level. As an Alliance, NATO may not be able to achieve or circumvent such tempo, limiting its ability to seize the initiative.

Discussion

The globalised environment is increasingly instrumented and monitored with most systems now connected to a network. Nations (particularly in the developed world), have 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, a hybrid threat is enabled to achieve high tempo and complexity. For example, Global Positioning Systems, satellite phones and GOOGLE Earth have allowed actors such as pirates in the Indian Ocean and Niger Delta, and the terrorists that conducted the Mumbai attacks to undertake increasingly adaptive and intricate operations.

Gaining and maintaining the initiative is a key factor in determining the outcome of conflicts. Actors that pose hybrid threats can operate in flat, distributed networks using decentralized command and control approaches to empower rapid decision making at the execution level of the organization. Often this means that NATO's adversaries would tend to have the "first move" and with it the initiative.

By contrast, NATO is an Alliance of Nations. This entails a level of bureaucracy where important decisions are taken by a consensus approach. On initial inspection these are limitations to a timely and effective approach for dealing with adaptive, dynamic hybrid threat actors and a complex security environment. In turn this may inhibit NATO's ability to seize the initiative and reduce its agility for responding to hybrid threats.

It should also be noted that by using a blend of non-conventional methods, actors who hybrid threats may be able to operate on a long-term timeframe, with conflicts falling somewhere between conflict and stability and not triggering a full military response. What seem like major events may be separated by years. Adversaries may seek to maintain the initiative by avoiding a robust military response that might cause a significant setback. What may be welcomed by NATO as an acceptable, steady state peace may in fact be a period of slow, steady progress for an adversary that utilises hybrid threats to achieve their strategic aims.

Conclusions

Actors that pose hybrid threats are able to gain and maintain the initiative through their effective and innovative use of new technologies to enable a high tempo of operations and adaptation. As such, NATO needs to consider when and how it might be appropriate to adapt its organization and decision making processes to enable a higher tempo of action.

Hybrid threat actors manage their operations and activities over a long-term campaign in order to make slow, steady progress toward their strategic objectives while carefully avoiding provocation of a response that might result in a significant setback.

5. BEING PROACTIVE: PREVENTING OR DETERRING HYBRID THREATS

5.1 Is it more appropriate for NATO to try to Deter or Prevent Hybrid Threats?

Observation

NATO's strategic concept [8.4] states that the best way to manage conflicts is to prevent them from happening. By being proactive and keeping threats manageable within a steady state environment, NATO seeks to potentially save costly expenses associated with dealing with challenging problems when the situation develops into a crisis requiring military intervention. The MCCHT identifies deterrence of hybrid threats as part of its framework solution, but deterrence may be a limiting concept and deterring hybrid threats may not be possible.

Discussion

Panels identified three types of possible deterrence that could be relevant for hybrid threats:

- Conventional deterrence by threat of retaliation (e.g. - Mutual Assured Destruction)
- Deterrence by denial of success - demonstrating the ability to mitigate an attack or prevent it from being successful.
- Deterrence by entanglement; by promulgating international norms and codes of conduct; by cultural entanglement; or by economic entanglement

However, deterrence of adversaries is only possible if there is a detailed understanding of the threat they pose. It is critical therefore to understand the motivations, relevance and potential sources of legitimacy of adversaries in order to counter them. Attaining and maintaining a high level of situational awareness concerning potential hybrid threats is essential to deterring, planning for, or conducting operations against them.

Webster's dictionary defines deterrence in the military sense as 'the maintenance of military power for the purpose of discouraging attack'. Participants identified that deterrence connotes a retaliatory aspect - the preclusion from action by an aggressor for fear of the consequences. It is a state of mind brought about by the existence of a credible threat of unacceptable counteraction. NATO's Strategic Concept views deterrence as a core element of its overall strategy based on an appropriate mix of nuclear and conventional capabilities.

Participants pointed out, however, that it may be quite difficult to identify, much less *deter*, an agile, multi-faceted hybrid threat seeking to operate under the threshold of detection. Non-state actors or marginal groups using non-conventional means may be difficult to identify, anticipate or even attribute threats to. This raises the question of what deterrence might mean with respect to adversaries applying hybrid means. In some participants' view, conducting activities to prevent adversaries from being successful is more appropriate, thus making prevention a more appropriate goal for dealing with hybrid threats. Prevention as defined by NATO, can include a range of activities from diplomatic initiatives, fact-finding missions, consultations, warnings, inspections and monitoring and preventive deployment of forces. [8.8]

While the first two types of deterrence in military terms approaches, the third also talks to prevention of conflict through economic, cultural or regulatory entanglement. Through this entanglement one could also be perceived to have deterrent value. For example, a nation would not want to go to war because it may wreak havoc on their economy - as economic interdependencies increase, deterrence increases by default. As with the other types of deterrence, economic initiatives might not necessarily work well in deterring non-state actors or irrational individuals.

This distinction between deterrence and prevention may also be an important one from a partnership perspective. When NATO works alongside non-NATO and non-military organisations the use of the word deterrence may bring up fears of use of military force, particularly in retaliation. A broader synonym like prevention may be preferred and more appropriate.

Finally, participants discussed a number of ways that NATO could enhance its contribution to preventing hybrid threats such as improved information sharing, common assessment, and expanded partnerships. However, they also articulated the reality that there will always be uncertainty over whether the political will to intervene in a given situation will be

sufficient until a crisis undeniably exists. Every intervention in which NATO has been involved could subsequently be perceived as a result of a failure of prevention.

Further Analysis

AAP-6 NATO Glossary of Terms [8.9] defines deterrence as *'the convincing of a potential aggressor that the consequences of coercion or armed conflict would outweigh the potential gains. This requires the maintenance of a credible military capability and strategy with the clear political will to act.'* Participants did not question or contradict this view of traditional deterrence or dispute the need for the maintenance of sufficient military capability within NATO to deter state actors who may employ hybrid threats.

Nevertheless, the basis of deterrence in the past has primarily rested upon the concept that if one acts in a particular manner, then effective retaliation will follow. The threat of retaliation forces the potential aggressor to conduct a cost-benefit analysis to decide whether the potential act is worth the resulting pain. When the cost outweighs the benefit, deterrence will be effective.

Effective retaliation against a stateless actor's hybrid threat is more difficult due to its adaptive character. This suggests that some broadening of scope or alteration to the basis of deterrence will be necessary to make it effective against most hybrid threats.

Detailed environmental understanding will also be a necessary precondition for effective deterrence against a hybrid threat. Such understanding will allow NATO to identify and evaluate the overall situation and those factors which will most effectively influence adversarial actions.

Conclusions

The MCCHT in its framework solution identifies the need to deter hybrid threats; however it may be difficult to clearly identify agile, multi-faceted hybrid threats seeking to operate under NATO's thresholds of detection. Consequently, prevention may be a more appropriate goal for dealing with them.

It is important to understand the motivations and sources of legitimacy of actors that use hybrid threats in order to deter or counter them. Attaining and maintaining a high level of situational awareness concerning potential hybrid threats is essential to prevent or deter adversaries using hybrid means.

NATO should maintain its existing focus on capabilities for deterrence against identified threats. Deterrence is essential, although it forms only part of a broader goal of prevention. NATO may wish to investigate how it can use its capabilities for supporting preventive actions to alleviate factors that lead to the rise of hybrid threats. The ability for NATO to take appropriate, timely and proactive actions to preclude the deterioration of a situation is necessary to prevent potential crises.

5.2 What is NATO's role in deterrence and prevention against hybrid threats?

Observation

If NATO wishes to prevent hybrid threats from occurring it must identify how it can best do so. As hybrid threats pose problems across a number of domains, NATO may find itself taking a supporting role in aiding others to take preventative action. However there are clear opportunities available for NATO to do more in preventing hybrid threats from occurring.

Discussion

The idea of "prevention" rather than "reaction" shouldn't be controversial. When countering hybrid threats, almost all participants agreed that to wait for something to happen and then react would leave the Alliance vulnerable to innovative and adaptive adversarial. However, undertaking preventative activities as an Alliance rather than as individual nations was a topic of great debate. The participants believed that in some cases there would likely be pushback against NATO involvement from some in the international community, and from within the Alliance itself.

NATO member states collectively possess the capability to track, monitor and engage hybrid threats in the military, information, geographic and economic realms. NATO can work with and through its member states, as it was seen that member states would often have greater and more credible roles in prevention activities. Participants viewed NATO as an organization that would contribute the requisite military support, and in some cases diplomacy, dialogue, consultation or coordination.

NATO can act as an integrator for Nations. Countries are currently re-evaluating their military doctrines to consider prevention actions before a crisis occurs as well as post-conflict end-state.

NATO can support in this development. Similarly within the current economic situation, bringing together Nations capabilities, be they used in a crisis prevention or crisis management, has the potential to save money whilst achieving common aims. Lastly, if a comprehensive approach is deemed necessary to counter hybrid threats, then in some cases NATO may be in a ready-made position to provide the necessary links.

Participants were asked to identify tasks and roles which NATO could perform in countering hybrid threats. A number were identified including:

- Partnerships to support long term defence sector reform.
- Defence sector anti-corruption programs.
- Defence diplomacy with national militaries in fragile/conflicted states.
- Disarmament, Demobilisation, Reintegration (DDR) support.
- Logistics support for civilian stakeholders.
- Interdiction of pirates at sea.
- Airspace security and interdiction.
- Security and stability in reconstruction environments
- Incentives for good behaviour such as NATO membership
- Intelligence gathering
- Reinforcing internal security in certain cases (if given mandate)
- Support to protecting critical infrastructure
- Enabling economic growth and development by providing security as well as a range of other support capabilities such as transportation, medical, communications, etc.

As NATO's contributions to preventative measures were explored, a number of core areas where NATO has expertise were identified. Most participants articulated that NATO should try and provide support within its key and core competencies, using existing capabilities in better ways. Areas identified included:

a) Training and Exercises

As part of steady state preparation it would be a great advantage to have established the necessary collaborative bodies in advance of conflict. This primarily concerns the human factors aspects of collaboration (establishing relationships), but also shared processes. Development and availability of training and exercises was identified as a perceived strength of the military and NATO that could be utilised to support that preparation, improving relationships and common procedures.

NATO could facilitate training, exercising and engagement with a broad range of actors as appropriate. In emerging security challenge areas such as cyber security or energy security, jointly exercising alongside other interested stakeholders could help identify common interests. One area specified was how NGOs and NATO could assist each other with monitoring and reporting on environmental conditions. Some NGO's have an interest in this area and would likely welcome a common exercise.

b) Standards and procedures

Development of common standards was also perceived as a NATO strength. The panel looking at cyber security suggested that this could be utilised when considering emerging security challenges such as cyber security. Although it may not be appropriate for NATO to lead or implement standards in this area distinct from those used in the commercial world, it was felt it could play a role in bringing nations together. One example expressed was that NATO could provide advice, standards and inspection teams of Supervisory Control and Data Acquisition (SCADA) and physical infrastructure in the energy sector to develop actions plans and education advice for nations.

c) Planning

The NATO planning processes when appropriate might be used to facilitate collaborative planning alongside partners. Collaborative Planning Mechanisms are required to enable a fully comprehensive approach. When not in the lead NATO will need to fit its operational planning process into a larger framework.

Not all organizations can participate in NATO planning, consequently a heterogeneous model with tighter levels of coordination and information sharing for planning for some actors and looser information sharing with other actors (to improve understanding of their contribution, but without integrated planning) is potentially a more feasible approach.

A lesser threshold for common action may be when a community of interest can share information, and thus each draw up more informed and synergistic plans. Participants noted that NATO will likely end up with an asymmetric planning process - parts of planning process will be more rationalized, others will be less planned.

d) Intelligence & assessments

It is essential that NATO maintain the necessary situational awareness to identify potential security threats, so as to address them with appropriate actors before they materialize into something more serious. NATO already provides a forum for Nations to share intelligence and assessments on threats to North-Atlantic security. When considering hybrid threats however it may need to develop further as a forum for sharing wider assessments between nations including appropriate aspects of cyber security, law enforcement and financial intelligence. Further to this it may be appropriate to share information and assessments with appropriate international organisations and bodies.

e) Advocating Countering Hybrid Threats

Panellists recognised what could be termed as 'the convening power of NATO.' By this they meant that NATO is recognised as a key actor in international security and crisis response and thus has the credibility required to convene those that need to build collective preparedness. This view was even advocated by those NGOs who make clear that their willingness to partner NATO is circumscribed.

As such, NATO has an important part to play in advocating for international action in areas that could support preventing hybrid threats. Examples may include, advocating the addressing of grey areas, such as the space between cyber-crime and cyber war, or bringing together nations to monitor technology development for threats and opportunities. NATO should also realise that its policies in dealing with emerging security challenges send clear messages to the rest of the interested community about the way forward. An example could be the USA clearly identifying that cyber-attack could be considered an act of war.

The perception of NATO and its ability to swiftly and efficiently counter hybrid threats is important. If NATO is perceived as such, then this serves as an important deterrence capability.

Further Analysis

NATO has a definite role in preventing Hybrid Threats from developing. In terms of crisis prevention, Chapter 2 of the Crisis Response Manual outlines a number of diplomatic, economic and military preventive options to influence the behaviour of potential risk-generating country (or countries). It further specifies that risk generating countries could include 'those states which harbour terrorists groups that are considered by the NAC to constitute a threat to NATO'. NATO's 2010 Strategic Concept stated that NATO has a unique and robust set of political and military capabilities to address the full spectrum of crises – before, during and after conflicts. NATO will 'actively employ an appropriate mix of those political and military tools to help manage developing crises that have the potential to affect Alliance security, before they escalate into conflicts'.

In the current financial climate the ability to use NATO's core capabilities in a more productive manner is important. In focussing on improved preventative initiatives NATO has the potential to save money by avoiding crises and the need to deploy large military force. To better identify the capability changes required to counter hybrid threats they should be examined alongside other requirements as part of the NATO Defence Planning Process (NDPP). Two areas where hybrid threats could be better integrated are in an extension of the scope of ambition of the NDPP to look at capabilities needed for "steady-state" preventative activities, as well as the consideration of the characteristics of hybrid threats within the planning situations.

Conclusions

NATO should play a proactive role in prevention and deterrence of hybrid threats. Although Alliance members may deal primarily with the some of the root causes of hybrid threats, NATO can play a supporting role in prevention activities helping to link together a broad range of political, economic and military actions intended to deal with the emerging security challenges.

Country-specific threats may not always be relevant in today's global security environment when threats may be more hybrid in character. NATO will have to consider carefully its role in integrating Alliance efforts in countering these types of non-traditional threats. NATO should continue to focus on its core strengths to support prevention activities.

This includes expertise in:

- Planning.

- Training and exercises.
- Standards.
- Intelligence and assessment.
- Being an international advocate

NATO's strength has always been its ability to provide security, stability, as well as communications, and logistics capabilities and support as necessary.

NATO members recognize the need for the Alliance to be able to respond to developing threats, but are reluctant to commit additional resources in today's fiscal environment. NATO should examine ways to use its existing capabilities innovatively, efficiently and effectively.

Recommendations

16. Develop improved mechanisms and processes for:
 - a) Intelligence and information sharing with the non-NATO and non-military community on emerging security challenges;
 - b) Collaboration with external partners on timely and relevant assessments against hybrid threats.
17. Reach out and expand relationships with a larger community of stakeholders that can help to identify emerging trends that could affect the security of the Alliance:
 - a) Develop links with law enforcement and financial institutions to monitor emerging security trends;
 - b) Improve mechanisms for working with scientific and research communities to monitor and understand the potential impact of emerging technology developments, particularly cyber;
 - c) NATO should augment its planning processes in a manner which allows for more efficient informal information sharing with those unable to participate directly.

18. ACT should investigate further how hybrid threats can be built into NATO exercises and how a wider community of interested organisations can participate in NATO training and exercise opportunities.
19. ACT should investigate how it can integrate the concept of hybrid threats into the NATO defence planning process to understand better what capability changes may be needed to counter the new challenges.

5.3 Indicators and Information Sharing for Situational Awareness and Early Warning

Observation

There is a broad array of key stakeholders from different sectors who monitor key environmental factors linked to hybrid threats (characteristic to the root causes or symptoms of the problem). Many of these environmental factors are outside NATO's traditional focus and are not regularly monitored by the Alliance. NATO does not have direct access to much of this information thus the importance of establishing arrangements for information sharing with the key stakeholders who monitor these factors.

Discussion

Attaining and maintaining a high level of situational awareness about potential hybrid threats is seen as essential to both planning for and conducting operations against such adversaries. Knowledge about their cultural characteristics and conditions, along with a deep understanding of their objectives and methods are critical.

There are significant differences in what information is required to establish situational awareness and understanding between those elements operating within the security sector and those who routinely operate outside of it. For a comprehensive approach to be effective, a much wider range of information and intelligence must be collected to develop effective situational awareness for all of the relevant partners. Civilian stakeholders will often be the best source of information to feed situational awareness. A resulting common assessment of the environment will likely be of value back to them as they conduct their normal activities. As such, NATO will need to develop relationships and partnerships with these stakeholders to enable identification of indicators and the development of the necessary situational awareness.

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

Indicators will need to be shared when considering some of the emerging security challenges that cross civil military boundaries. A good example is cyber-security where stakeholders could include governments, law enforcement and the for-profit private sector. Since many aspects of hybrid threats may be criminal in nature, the need for law enforcement information sharing was an issue raised in several panels (national data, INTERPOL data, and financial crimes data). There were caveats in the form of firewalls between military intelligence and law enforcement data. That said, it was noted that law enforcement expertise present in an intelligence fusion centre would allay that concern.

This is indicative of the varied challenges to Information Sharing. Participants discussed how information sharing is essential for an effective comprehensive approach, yet it is a challenge for both the military and civilian sides of the equation. Challenges include, but may not be limited to:

- Military classification protocols severely limit sharing;
- Proprietary information is very sensitive for businesses and some information sharing activities are considered unlawful if interpreted as price fixing. Business may see firewalls as essential for managing risk and return on investment;
- Technical capabilities exist to enhance information sharing but policies and practices block information exchange at the potential release points;
- Different levels of sharing are recognized based upon the nature of interactions: Collaboration, Coordination, De-confliction, or Conflicted²; [8.10] and
- Information release authority varies (e.g. commander for military, owner for business, judges for police).

One of the challenges noted is that information sharing opens a vulnerability-trust issue. As a result, governments often don't share and are sometimes viewed as a dead end for information sharing. In return this policy reduces incentive for the private sector to share information with national governments or NATO. Also, due to a lack of trust or lack of mechanism to enable it, the private sector may not share information on threats (such as

²Levels of C2 Maturity.

with cyber-security). Participants noted that National governments and NATO are losing an opportunity if they are not working with the for-profit private sector on cyber threats.

Coordination with other key civilian stakeholders such as NGOs and humanitarian actors would need to take place at their headquarters offices rather than in the field to ensure continued safety and access for those actors to do their work in the field. It was noted that the ICRC and similar bodies would not share any private information. They would share anything already in the public domain - and this could be useful. Participants suggested that it was also preferable for NATO and others to utilize published reports from the ICRC and humanitarian NGOs to reinforce the neutrality of those actors.

A strong discussion theme was the need for a 'fusion organisation' to draw together all of the necessary types of information for early warning and situational awareness to inform NATO in dealing with hybrid threats. Three areas in particular stood out from the discussion: cyber, law enforcement, and financial intelligence. These topics were consistent with discussions across the panels.

Conclusions

NATO would benefit from broadening information sharing with a wider array of key stakeholders, specifically from sectors that may be monitoring key environmental factors linked to hybrid threats. These stakeholders may also provide data that might improve our situational awareness of the environment and threat. There may be one-way or reciprocal information sharing relationships depending upon the stakeholder and the situation. Information may be shared at different echelons (strategic, operational, tactical) depending upon the comfort level, culture, and capacity of the stakeholder organizations.

NATO will need to confront the challenges and limitations inherent to information sharing within a comprehensive approach to include: limitations due to military classification protocols, business community sensitivity to sharing proprietary information, policies and practices that block information exchange, varied levels of sharing based upon the level of organizational interaction, and varied information release authorities.

A high level of situational awareness about potential hybrid threats is essential to preventing, deterring and countering them. Civilian stakeholders will often be the best source of information to feed situational awareness and shared situational awareness will often be in their best interest to inform their normal activities.

Key types or topics of information required to improve NATO's understanding and situational awareness to counter hybrid threats include: cyber-security, law enforcement/criminal statistics data and financial intelligence data.

Recommendations

20. Develop relationships with key civilian stakeholders (including those that may not initially be receptive to doing so) who are better placed to monitor key environmental factors linked to hybrid threats – this will enable development of necessary situational awareness.
21. For early warning, as well as situational awareness, NATO should augment its intelligence fusion capability with data related to cyber security, law enforcement and financial intelligence.

5.4 Risk Assessment and Management of Hybrid Threats

Observation

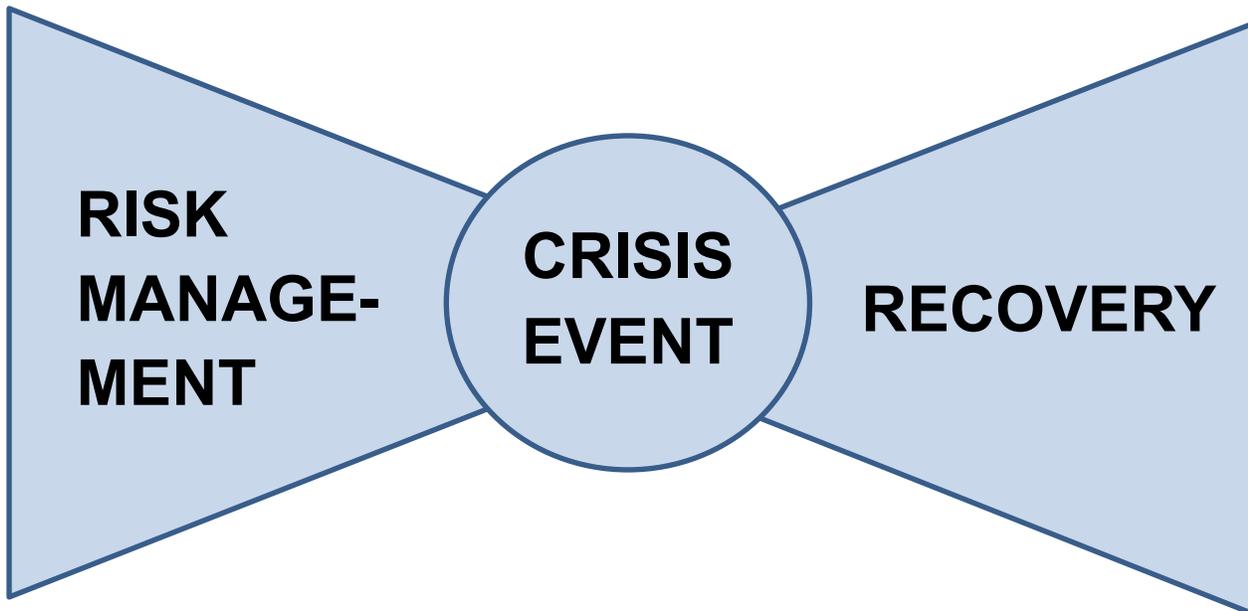
When considering hybrid threats in a steady-state environment, when a crisis has yet to occur, it may be difficult to define specific threats or have the resources and take action to prevent all threats from occurring. One way to identify those threats NATO wishes to expend most effort on would be through conducting risk assessment and then managing those risks through a coherent effort of preventative actions.

Discussion

Risk is widely assessed in the private sector. Civilian businesses are concerned about risk in areas ranging from damage to the environment, image, safety of employees and the public, protection of assets, and often most importantly to economic gain or profit generation. Basic risk assessment often uses a model designed to assess the impact of consequences and the probability of an incident.

While NATO has existing capabilities for monitoring and assessing potential threats, particularly from states and terrorist organisations, it may need to consider risks to Nations from a wider and more holistic viewpoint. Emerging security challenges such as cyber security, energy security, maintaining access to the global commons and the movement of men and materials related to CBRN, on their own or in combination may create significant risk directly to NATO or NATO member nations.

Once high risk threats and emerging security challenges are identified, NATO would wish to prevent them from developing into a crisis. This requires barriers to be erected or preventative action to be taken, not only through the military but in the economic, social, legal or infrastructural domains as well. One panel presented the consequence management 'bowtie' as a simple model for how one should consider both risk management as well as crisis action and recovery.



The Crisis Response Manual is the procedural document that NATO uses for crisis management. The manual includes preventative measures as well as response measures. However the fact that the crisis has occurred in order for there to be response does not make it easy to undertake these preventative measures. Terms such as 'pre-crisis' do not help to determine when a 'pre-crisis' began or when it is possible to take preventive measures.

NATO may have to adapt its pre-crisis language to match that in the commercial world, where attempts to prevent a crisis are undertaken by risk management. Risks are identified, mitigated, avoided or taken as a calculated risk. Thus, NATO may have to conduct 'threat management' by implementing preventative measures to minimize the impact of potential crisis situations. Countering hybrid threats should be wider than actions to only engage within a crisis. NATO can undertake risk management without having identified a direct and pressing threat to its own security.

There are many non-NATO risk assessment bodies existing including in insurance companies, industry, NGOs, and the UN that may assess risk from similar threats or adversaries as NATO. As NATO does not have access to all the sources of information needed for a complete picture of hybrid threats it may be useful to share common assessments of interest with these bodies, however NATO would need to address the challenge of bringing these entities together. These risk assessment bodies in other organisations may also have valuable methods and lessons that they could share with NATO in this area.

There was a general sense among participants that NATO must create the ability to access a network that allows continuous partner engagement through a risk assessment and integration body. The function of a body would be to enable the maintenance of high fidelity situational awareness on the hybrid threat, from which risk assessment and contingency planning can be effectively conducted. Such a capability would be critical to enable civilian-military connectivity or a comprehensive approach at the operational and strategic levels. The NATO Shipping Centre³ may provide a useful prototype example for this function. As well as processes for sharing, common standards for reporting on vulnerabilities should be developed. For example the EU has developed procedures and standards for the protection of critical infrastructure⁴. These EU standards could be a model for NATO as well as others.

Conclusions

The NATO Crisis Response System Manual [8.8] provides mechanisms to respond to pre-crisis situations. However it appears to be primarily focused toward crisis response, not crisis prevention. Further, the manual is oriented toward nation states (risk generating countries). A review of the Crisis Response Manual to determine whether it is sufficient for enabling pre-crisis prevention processes and actions is warranted.

³ www.shipping.nato.int

⁴ The European Programme for Critical Infrastructure Protection' (EPCIP) – this refers to the doctrine or specific programs created as a result of the European Commission's directive EU COM(2006) 786 which designates European critical infrastructure that, in case of fault, incident or attack, could impact both the country where it is hosted and at least one other European Member State.

Countering hybrid threats requires a proactive effort to understand the character and capabilities of the potential adversary. NATO needs to develop or improve its ability to monitor and produce continuous and timely assessments of the risks of potential hybrid threats in steady-state (pre-crisis) environments, with in some cases appropriate partners.

NATO would benefit from a network allowing continuous partner engagement through a risk assessment and integration body to enable maintenance of high fidelity situational awareness to inform risk assessment and contingency planning. The NATO Shipping Centre may provide a useful prototype example for this function.

Recommendations

22. Review crisis management processes to determine whether they are suitable for non-crisis decision-making in a dynamic, steady state, security environment. This could include:
 - a) An examination of how the Alliance conducts 'risk and threat management' relative to 'crisis management'.
 - b) Examine crisis management terminology and processes to determine whether NATO should include or reflect risk and threat management standards and processes used by non-NATO organizations.
 - c) Review Chapter 2 of the NATO Crisis Response Manual to determine its adequacy and responsiveness for steady state (non-crisis) preventive actions.
23. Explore development of a network for engagement, through a risk assessment and integration body, which could feed situational awareness for risk assessment and contingency planning. The NATO Shipping Centre could be evaluated as a model for this network.

5.5 Strategic Communications

Observation

Effective strategic communications is an important aspect of countering hybrid threats in terms of maintaining the support of the public and key stakeholders engaged in countering hybrid threats, maintaining the understanding and support of the affected local/indigenous

populations within the region, and as a tool aimed directly at the hybrid threat adversary to deter action, undermine their initiative, and weaken resolve.

Discussion

Strategic communications should be a key piece of a comprehensive strategy to countering hybrid threats, given its importance for the success of such a campaign. It's important to clearly articulate to the public a credible picture of the adversary and what their long term objectives are to justify intervention or action against them. It is also important to communicate to the public the time commitment required for a comprehensive campaign to defeat the threat (reflecting on the case of the Afghanistan conflict). Political leadership can create false expectation by underestimating the duration or cost of an undertaking, as the negative effect of an expectations mismatch could be loss of public support for any action or mission.

Participants discussed the relationship between strategic communications and measures of effectiveness, with discussions in one panel suggesting that effective strategic communications recognizes that the strategic message, measures of effectiveness and actions are all interconnected. The strategic message must be carefully tailored to the target audience. Actions, message, and assessment must all co-evolve and change as the mission progresses. This aspect is important to maintain the trust, confidence and support of the broader stakeholder community (to include where applicable, affected local communities).

While participants discussed the need to tailor strategic messaging regarding countering hybrid threats to specific target audiences, in the age of global communications and a media rapidly accessible to a broad variety of audiences, tailoring may not work. Instead a broad based message which is carefully tuned to address concerns of a variety of audiences may be preferable and more feasible option.

If actions to counter hybrid threats require engagement abroad, any strategic message will need to carefully articulate objectives to assuage sensitivities and some pre-conditioned suspicions of western interventions for ulterior motives such as access to resources at the expense of local populations. There was caution raised regarding NATO relationships with industry, and how that is conveyed in strategic communications as that may pass the wrong perception or strategic message.

Participants also discussed the role of new media and social networks as a vehicle for communications allowing the adversary to influence public perceptions; it can also be used

as well as a venue for NATO and other key stakeholders to pass their own message and counter adversary messaging. In the recent past industry has employed counter-messaging campaigns on social media as a part of its strategic communications strategy. A good example of this was in the case of the Gulf of Mexico oil spill. As described by an oil industry representative, in this example the oil industry wanted to provide accurate information to counter incorrect rumors promulgated on Twitter and other social media outlets.

Conclusions

NATO needs to include strategic communications as an important element of any comprehensive campaign to counter hybrid threats, conveying clearly and credibly the nature of the hybrid threat as well as the international community's long term objectives and abilities to counter those actions. NATO needs to employ pro-active messaging to seize the initiative from hybrid threat adversaries, capitalizing upon social media as part of its strategic communications strategy.

It is important for NATO to understand the nature and motivations of several important audiences to develop an effective strategic communications strategy as part of a campaign to counter hybrid threats. These audiences include: i) key stakeholders within or sought to be included within a community of interest utilizing a comprehensive approach to countering hybrid threats; ii) the general public within the international community; and iii) the indigenous communities of local actors (where that is applicable) within the hybrid threat adversary's operating environment.

Any messaging about NATO relationships with business or industry needs to be carefully calibrated to prevent mistrust by the public regarding potential improper engagement.

Recommendations

24. Determine whether a 'counter-messaging' approach is appropriate and feasible as part of the strategic communications required for countering hybrid threats.

6. TAKING A COMPREHENSIVE APPROACH TO COUNTERING HYBRID THREATS

In conventional warfare and during crisis management, stabilisation and reconstruction operations, the roles of the public sector and private sector⁵ are defined, with the purpose of the military, as the main conflict resolution element of the public sector, focused upon reducing the means and will of the opposing force. The hybrid threat, by its nature from a non-state adversary or adversary that combines both conventional and non-conventional ways and means, can both effect and work within the seams of responsibility of both the public and private sectors, drawing the latter more directly into the effort to counter hybrid threats.

The challenges of hybrid threats create a necessity for the military to combine efforts with the other elements of the public and private sectors to take a more comprehensive approach for preventing, deterring, and, if necessary, defeating hybrid threats. Conceptually, this approach would work by common purpose across the public and private sectors where each could contribute assistance in understanding and countering threats based upon their individual goals, interests and capabilities within an overarching community of interest.

6.1 The Role of Interests in Creation and Sustainment of a Community of Relevant Stakeholders

Observation

Although NATO may identify common goals with some national and international bodies or other organisations, outside of the public sector relative interests may form the basis for engagement and cooperation.

⁵ *'The part of the national economy not under direct control of the government.'* Oxford English Dictionary

Discussion

Interests and goals:

Stakeholders will have a variety of interests and goals, some which diverge and others which may overlap with those of NATO. This is linked to jurisdictional and mandate issues for different actors, and may also be situational dependant (especially where policy decisions are involved). When addressing complex hybrid threats involving different actors, panels concluded it would be difficult to identify shared interests because of the multiple stakeholders with different perspectives and interests involved.

The Experiment explored how deconstructing the hybrid threat into its constituent parts might enable agreement on shared goals/ interests on some individual elements of the problem. It was noted that jurisdiction causes divergences; different entities would deal with different parts of the threat according to their organizational mandates e.g. law enforcement organisations dealing with criminal activity whilst the IAEA would deal with nuclear trafficking issues. It was suggested that the way the threat is defined would be key to how goals are framed and would influence the ability to come to a common understanding of shared strategic goals with a disparate group of stakeholders.

It is also necessary to understand and differentiate between a group or organisation's near-term and enduring interests. If enduring interests are similar then they will present an improved opportunity to work together and achieve better unity of effort. Examples where this can be used include; achieving a comprehensive solution toward stability and effective governance, establishment of internationally accepted legal frameworks, addressing the root causes that underpin territorial conflict, terrorism and insurgency, and developing the economic environment throughout a region with the goal of raising security levels and conditions, living standards and gaining economic partners. More near-term interests such as securing a particular supply of energy, reducing vulnerabilities in essential sectors relative to strategic interests, addressing organized crime when it has a negative regional impact, controlling arms flow, controlling migration, or advancing human rights in a region tend to be subject to shifting importance, priorities, and levels of commitment. There is also an inherent risk in selecting partners within a comprehensive approach based solely upon an alignment of immediate or near-term interests. There may be stakeholders whose short term interests may align and whose contributions could provide value but whose long term character and objectives may not be desirable. This tension between short-term advantage and long-term disadvantage is a key consideration when building a community approach. It was also recognized that apparent interest may not actually reflect true interests.

Within a comprehensive approach to a particular situation, when there are no obvious shared interests, there may still be a need to share information in order to de-conflict actions with other stakeholders in the operating environment. The broad range of stakeholders needs to be understood along with their interests in order to determine what kind and level of relationship might be desired and feasible.

Potential stakeholders with common interests:

There are likely to be bands of potential stakeholders in any particular situation based upon the nature of their interests. These will range from those that are very likely to share common interests and be supportive of NATO and international interests community goals, e.g. NATO Member States, United Nations (UN), European Union (EU), Organization for Security and Cooperation in Europe (OSCE), Organization for Economic Co-operation and Development (OECD), International Monetary Fund (IMF), World Bank, to those whose support will be more closely tied to the specifics of a given situation e.g. International Businesses dealing with energy, shipping, pipelines, high technology, regional governments, immigrant groups, Non-Governmental Organizations (NGOs), Private Security Companies (PSC) and Media. There will also be those who are likely to oppose any NATO or multinational intervention into the existing status quo if it has the potential to threaten their interests.

The overlapping interests between NATO, NATO Nations and private sector businesses came under scrutiny during the experiment. The relative nature and utility of a prospective NATO business partner can be subject to a number of considerations. NATO will be concerned about compatibility in terms of political objectives, trustworthiness and capability. Potential partners from the business sector may care less about those factors, and instead place great weight upon things such as the ability to deliver and sustain security and stability or the degree of investment risk. Working with NATO will need to be of benefit to a private sector company, as there will need to be the ability to offset the cost. Business will not develop capabilities to help NATO unless the benefit of doing so is worth it to them. This benefit can take many forms and cannot be limited to just security. Businesses may be concerned about risk in terms of damage to environment, safety of their employees and the public, protection of assets, and profit generation.

NATO might work with other non-military organizations with common interests in cyber security, from international organisations such as INTERPOL to private organisations such as Google. There could be different common interests such as investigating a cyber-attack (NATO-INTERPOL) or mitigating the effects of an attack (NATO and Google.) Experiment

Participants indicated that they were not aware of existing mechanisms to work with NATO in this area, but felt that it could be usefully pursued. The role of the financial sector and its interests in relation to cyber-crime and organized crime activities employed by hybrid threat actors was also investigated. Destabilization of currency markets, financial systems and financial institutions are often the targets of cyber-crime activity, thus the line between “for-profit” cyber-crime and attacks on financial institutions can be blurred with regard to attribution and intent. Financial institutions can be reluctant to release information on cyber-crimes since it might hurt the public or their customer’s perceptions of the security of their money. However, the financial sector has a lot to lose and may be a willing partner in a comprehensive approach to tackling hybrid threats.

Working directly with private sector partners does have limitations within an Alliance context. The concern raised was that each member nation would have to evaluate such partnerships to determine if national interests supported the risk of sharing national information. If a member nation shared information with NATO, it would need careful understanding and assurances about how the information concerned was shared with businesses.

Conclusions

Strategic partnerships for countering hybrid threats in a steady state or pre-crisis environment will be different based on the situation and will have to be crafted based upon a clear understanding of each potential partner’s individual interests. To enable these partnerships, relationships will have 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 goal may be seeking to build relationships upon a convergence of (potential) interest rather than long term development of enduring and common interests.

Even where there are not obvious shared interests for common action, there is often a need to share information in order to de-conflict actions with other stakeholders in the operating environment. It is important to understand the different levels of necessary and feasible relationships.

Private sector businesses may have some overlapping interests with NATO and the international community in countering hybrid threats but won’t develop relationships and mechanisms to work with NATO unless mutual benefits are clear. Information-sharing relationships between private sector companies and NATO raise issues regarding maintaining control of national proprietary information.

Recommendations

25. Once NATO has determined who the key non-military/non NATO stakeholders are, it must understand their mandate, limitations, interests and goals (relative to the situation) in order to determine what type of relationship is feasible and desired. Key to gaining this understanding is:
- a) Recognizing and differentiating between true, enduring, and near-term interests of stakeholders.
 - b) Recognising which are the most feasible areas of common purpose for NATO and the range of potential partnerships.
 - c) Developing methods for learning and understanding changing stakeholder interests over time (from the stakeholders' perspectives).

6.2 Relevant Stakeholders, Relationships, and Possible Partnerships in Countering Hybrid Threats

Observation

Experiment discussions in all three panels recognized the importance of relevant stakeholder nations and organizations and attempted to identify the characteristics and identities of those with whom NATO should seek to build partnerships and knowledge to enhance their collective ability to counter hybrid threats. Key factors in identifying stakeholders rest upon who is most directly negatively impacted by the hybrid threat or potential NATO operations, who can provide information on the presence or nature of the hybrid threat, and who can exert influence to advance or reduce the effectiveness of potential actions to counter the hybrid threat.

Discussion

Given the complex character of hybrid threats and their enabling environments, the key stakeholders in a comprehensive approach to dealing with hybrid threats can come from a wide variety of sectors, broader than the traditional sectors which NATO has dealt with in the past. This includes contributions from both the public and private sectors. In summary these sectors and actors may include: Security, National Intelligence, Economic, Financial (including international banking), Social, Development, Governance, Humanitarian, Civil Society, Rule of Law, Legal, Multinational Law Enforcement bodies, Justice Sector,

Information Technology, Communication and Cyber domain, Nano-Technology, Robotics, Bio-science, Critical Infrastructure (for Energy, Transportation and Essential Services), Maritime organisations and Commercial users of Space. The types of actors in these sectors include: Government, Non-government (NGOs, Think Tanks, and Academia), Business and Industry, Media (Traditional, Social Media), Local Actors (indigenous community groups, religious leaders), International Organizations and Multinational Bodies. Depending upon the nature of the threat and the environment or domain of this threat, a different set of sectors and actors may apply. Over time, the set of interested actors may change as circumstances develop and change. If NATO wishes to comprehensively address hybrid threats it would need to partner or develop relationships with these actors.

When trying to understand and prevent hybrid threats from developing during a pre-crisis or steady state situation, those potential partners' best placed to detect hybrid threat indicators will be of particular interest. These may include: International, regional and national criminal intelligence agencies that can detect crime statistic indicators; international bodies which can track monetary flows; Stock markets; Banks which have to provide information to national governments; UN agencies for countermeasures; IMF; World Bank; UN agencies monitoring international reporting standards for money laundering and bodies who monitor cyber-crime within the international private sector. Some participants also noted that community based organizations (e.g. municipalities in towns/cities) often are more informed about indicators for elements of hybrid threats and are often the ones best placed to identify home-grown terrorism.

Indigenous Populations

Understanding and engaging with actors in the regional and local (indigenous) population is also important to understand and therefore effectively address hybrid threats and their enabling environments. When engaging local populations, it's important to understand that they are not homogenous and that they are made up of various civil society groupings with different interests and constituencies. The context and dynamics between these groups will also affect ways in which hybrid threats can be addressed.

The indigenous population of a region may well be the primary "stakeholder" and will "own" the underlying problems generating a hybrid threat. Others (to include NATO), who may be trying to counter the threats are really "outside participants". Any indigenous population will be made up of different factions with different interests, meaning that some are more likely than others to be supportive of outside efforts affecting their home territory. The strong differences in perspective and cultural nature between potential NATO partners, either as

factions within the indigenous population, independent actors, or members within regional organizations, will need to be understood and managed in order to conduct effective CHT activities. These elements will include:

- **National Actors.** National stakeholders will include more groups than the national governments; the population is also a stakeholder.
- **Groups.** It would be insufficient to identify the general public as the target audience – there remains a need to specify groups within a society (e.g. IDPs, ethnic, social, religious groups). It is necessary to understand who the relevant population groups are as well as any sensitivities and/or tensions between groups in order to be able to effectively engage and leverage them as part of counterinsurgency approach to deal with the threat.
- **Elites.** Elites in the region will potentially be stakeholders as they do not wish to lose power and often have influence. This can be extended to other groups content with the current security situation (e.g. organized criminal gangs).
- **Disenfranchised.** Disenfranchised local populations could be enablers of hybrid threats, in particular local populations threatened by negative distributional changes such as the loss of political or economic power.
- **Diasporas.** Diasporas are potentially important stakeholders with influence on the security environment. They can represent their home nation interests to their host countries where they are living abroad and also provide financial flows back to their home nations. Tensions may exist between these “natives abroad” and the local leadership that has remained in place, tensions that could actually be leveraged by potential hybrid threats.

Law Enforcement and the Legal Community

Hybrid threat activities usually occur below the thresholds of conventional warfare, frequently within the realm of criminal activity and often exploiting the seams between the jurisdictions/responsibilities of different actors and the unregulated legal grey areas where law has lagged behind the adversaries’ ability to innovate. Given the nature of hybrid threats, participants across all panels discussed the important role of law enforcement and legal instruments in a comprehensive approach to countering hybrid threats.

Weak Rule of Law, Lack of Governance and State Fragility were some of the root or structural problems outlined that could cause instability fostering the emergence and

sustainment of hybrid threats. Data on criminal activity could serve therefore as an indicator of environments conducive to hybrid threats (root cause indicator) as well as a low-level indicator of actual hybrid threat activity (symptom indicator).

National criminal intelligence agencies were identified as good sources to monitor indicators for hybrid threats. Other specific organizations such as INTERPOL and within Europe, EUROPOL and FRONTEX were also discussed. INTERPOL, the International Police Organization, has an international mandate and is an intergovernmental organization, made up of member states which share criminal data via various online networks. INTERPOL has an online reporting system which can be used to support countering piracy and is a good source of crime statistics. EUROPOL is the European Law Enforcement Agency which aims at improving the effectiveness and co-operation of the competent authorities in the Member States in preventing and combating terrorism, unlawful drug trafficking and other serious forms of organised crime.⁶ FRONTEX is the EU's body to coordinate the operational cooperation between Member States, Schengen Associated Countries and other partners in the field of border security. Formed in 2005 to enhance external border security, FRONTEX actively promotes cooperation among border related law enforcement bodies responsible for the internal security at EU level.⁷

As highlighted earlier establishing a relationship with INTERPOL could enhance NATO's ability to effectively counter piracy activities. INTERPOL has an internet based reporting system, access to which would benefit NATO commands within the Horn of Africa. This would suggest the need for an enduring relationship with INTERPOL in this area.

Participants also identified the role that legal frameworks and regulatory regimes (to include UN conventions, financial sanctions, embargoes) could provide in helping to counter hybrid threats, making it more difficult for them to act and/or providing legitimacy for taking specific action against the adversary. There is currently an inability of legal frameworks and regulatory regimes to adapt to the rapid growth rate of technology and social media tools which hybrid threat actors have capitalized upon. There is the need to develop longer term

⁶ EUROPOL website: <http://www.europol.europa.eu/>

⁷ FRONTEX website: " More about Frontex," http://www.frontex.europa.eu/more_about_frontex/; "Origins." http://www.frontex.europa.eu/origin_and_tasks/origin/

enduring relationships with communities of interest and to collaboratively work with technical and legal experts to close loopholes in legal and regulatory regimes to counter hybrid threat activity.

Intelligence Community

NATO's intelligence capacity may be insufficient to persistently monitor and assess all the indicators of potential hybrid threat activity. Participants across the panels discussed the importance of intelligence to inform NATO early warning and situational awareness to counter hybrid threats. Participants also discussed the need to broaden the scope of intelligence and information gathered (to include use of open sources) to better understand the environment and the threat. Participants highlighted the need to access criminal and financial intelligence and information. The types of information required are perceived to be resident in member state intelligence organizations as well as certain international organizations which collect specific intelligence such as INTERPOL for criminal data and the Financial Action Task Force (FATF) for financial data.

Financial Sector

There is an important economic/financial aspect to hybrid threat activity and thus data resident in the financial sector could contribute early warning indicators and provide situational awareness of hybrid threat activity. Some financial community stakeholders also have the ability to take effective action to undermine and counter hybrid threat activity. Much illicit money is not located in conflict zones; the FATF for example has issued a mandate to monitor funds used by NGOs that may support terrorist organisations. Financial intelligence can also be used to improve and inform planning, especially in post conflict settings plus financial countermeasures can be useful in deterring countries who want to get off financial blacklists. Specific financial information which could provide useful indicators of potential hybrid threats includes money laundering statistics and financial flows and transactions between nations or groups.

The World Bank and the International Monetary Fund (IMF) are bodies which monitor financial transfers. Others include the FATF and the regional financial task forces who track monetary flows for the EU, Africa and Asia. The umbrella organization for these regional groupings is FATF, the inter-governmental body whose purpose is the development and

promotion of national and international policies to combat money laundering and terrorist financing. It has 36 members from around the globe, with 34 countries and two regional organizations (European Commission and the Gulf Coordination Council); and includes several regional associate member groups.⁸ FATF resolutions and standards on countering terrorist financing are supported by UN Security Council and General Assembly Resolutions.⁹ The FATF represents a world-wide network of financial intelligence, and the legal frameworks for these related institutions are the same; they can share information based on legal requirements.

Additional sources of hybrid threat indicators could include UN agencies monitoring international reporting standards for money laundering (mandatory for G20 states) and the IMF and World Bank. NATO should consider how it might develop or improve relationships with these institutions related to hybrid threats.

Private Sector Business and Industry

NATO could benefit from relationships with business and industry for information sharing, early warning and situational awareness. It was clear that there is an interest within business and industry to participate in a comprehensive approach to counter hybrid threats; It was also indicated in discussion that NATO's current mechanisms for business and industry engagement, such as Industry Day are not necessarily optimally used for this purpose.

There are limitations to where and what extent business and industry will be able to partner with NATO. The need to maintain and protect their relationships with host nations in order to conduct business and protect their investments may cause such stakeholders to operate at cross purposes with NATO. This will mean that business and industry may need to distance themselves from NATO or its activities and the civilian-military relationship will need to be sufficiently flexible to accommodate these situations.

⁸ "About the FATF", www.fatf-gafi.org/aboutfatf; "FATF membership" www.fatf-gafi.org/membership

⁹ United Nations Office on Drugs and Crime, "UN Instruments and Other Relevant International Standards on Money-Laundering and Terrorist Financing" <http://www.unodc.org/unodc/en/money-laundering/Instruments-Standards.html>

Private sector participants identified that NATO could have a role in advancing consultation and engagement about particular threats of common interest. A commonly used example was cyber security. They also highlighted NATO's current expertise in developing military-military and civil-military interaction via partnership programs and security dialogue programs. Ideas to improve and shape NATO's relationship with the private sector included the use of a Business Advisory Board or the identification of a business ombudsman. In this context, an ombudsman would be a person or organization that acts as a trusted intermediary between NATO and the external business and industry communities.

Another area identified where NATO could partner with the business and industry sector was in sharing (or in some cases even integrating) risk assessment data. In the private sector many risk assessment bodies exist, such as those from insurance companies, the energy industry and NGOs. These risk assessments could in some cases complement those undertaken by NATO and other military in identifying and allowing mitigating action of hybrid threats.

The role of the private sector in understanding and monitoring the rapid development of technology which adversaries could exploit is also important. NATO must develop or improve ways to monitor and understand rapid development of technologies that may represent a significant threat if misused. Examples given included; chemical, advanced bio-tech, artificial intelligence, artificial agents, nano-technology, smart grids and social media. The private sector is a primary element in the development and use of this technology; participants identified the need for NATO to engage with industry as a partner in this area. It was articulated that from a private sector perspective they would require increased indication of NATO's interest to provoke increased engagement.

Intergovernmental Organizations

An Intergovernmental Organisation (IGO) is an "association of States established by and based upon a treaty, which pursues common aims and which has its own special organs to fulfil particular functions within the organization."¹⁰ A unique characteristic of an IGO is that it can enter into agreements (to include treaties) with other IGOs or nation states. IGOs are

¹⁰ Encyclopedia of Public International Law, p.1289.

distinct from Non-Governmental Organizations (NGOs) which do not have the same legal personality and cannot enter into such agreements.

Besides INTERPOL, EUROPOL, and FRONTEX, other examples of IGOs with potential roles in countering hybrid threats include the UN family of organizations, the Organization of Security and Cooperation in Europe (OSCE), the World Bank, IMF, and the EU.

Participants agreed that the UN is a key actor with regard to countering hybrid threats within a comprehensive approach. The UN can provide the legal mandate for action and has the broadest set of member states and affiliated organizations and mechanisms to address various aspects of the hybrid threat root causes and symptoms.

Participants also discussed the importance of NATO continuing to develop its relationship with the EU, especially given its role as a regional European IGO with a broader mandate than NATO, which allows it to address civilian aspects such as rule of law, justice, governance, humanitarian and development issues which are outside NATO's purview. The EU has developed procedures and standards for the protection of critical infrastructure which could be a model for other areas of the world. These standards of how and what to report are embodied in the European Program for Critical Infrastructure Protection (EPCIP), established under EU Council Directive

The UN, EU and OSCE were referenced by participants as IGOs which might support institution-building and infrastructure support activities, getting at the root causes of hybrid threats, as well as Security Sector Reform activities that could help to counter them. The UN, World Bank, Organization for Economic Cooperation and Development (OECD) and INTERPOL were mentioned as key institutions for anti-corruption activities. The World Bank and IMF were noted as key partners for economic development activities.

Non-Governmental Organisations

A wide range of NGOs operate with relative freedom in the same areas affected by hybrid threats. This potentially makes them a useful partner in the effort to counter hybrid threats, but it is a relationship that comes with unique limitations and weaknesses. Participants raised the point multiple times that NGOs cannot allow themselves to be closely linked to the military. NATO should understand that NGOs won't be able to be plugged into a comprehensive approach to countering hybrid threats in the same way or to the same extent as other stakeholders.

Most Humanitarian Assistance NGOs have policies consistent with the NGO/International Federation of the Red Cross (IFRC) Code of Conduct, which states three guiding principles: (1) the humanitarian imperative, (2) independence, and (3) impartiality in situations of conflict. As noted in the U.S. Institute for Peace "Guide for Participants in Peace, Stability and Relief Operations [8.11], *"their purpose is to relieve human suffering regardless of political, ethnic, religious or other affiliation."* Thus they maintain a principal of impartiality and neutrality, and cannot be seen as directly affiliated with the military or NATO, as this may compromise their security and freedom of action in the field. These organisations require the flexibility to 'engage interact with both sides' if it supports the ability to deliver aid.

While the military could certainly monitor and utilize published information from NGOs to identify early warning indicators of hybrid threats, or the environmental conditions where such threats would likely thrive, NGOs would likely not share other data not already publically available. This is despite the recognized need for a certain level of security in order to maintain a humanitarian space. While NATO may seek to work more effectively with other stakeholders through exchange activities and cross postings, NGO representatives at the experiment cautioned that closer collaboration with the military might create perceptions that could harm humanitarian organizations' work.

NGOs can often serve as a good information source, but they are unlikely to be able to cooperate with, let alone "integrate" into any formal government or military program or organization. It was emphasized that interaction with NGOs or other humanitarian actors would preferably be done at the headquarters level rather than in the field to maintain their security and freedom of action. Strategic Partnership is often possible, when operational and tactical cooperation may be more difficult. In the field it will likely be a situational judgment whether partnership with NATO brings more benefits than problems.

Conclusions

There are many actors engaged in the environment that are either directly or indirectly addressing some of the problems associated with Hybrid Threats. There are opportunities for NATO to improve the way it works with and alongside these actors and organisations.

There is a significant amount of expertise and knowledge held within the for-profit business and industry sectors. This could be better capitalised upon to improve dialogue, understand common risks and threats and explore the use of emerging technology. NATO should review its established mechanisms for collaboration with industry, particularly with a focus on key emerging security challenges such as cyber security.

NATO would benefit from enduring relationships with key law enforcement community stakeholders to include INTERPOL, EUROPOL, FRONTEX and other criminal intelligence organizations from member states or partner nations. Similarly, NATO should explore enduring relationships (via appropriate interlocutors) with key financial sector actors such as: the Financial Action Task Force and its members; UN agencies which monitor money laundering standards; IMF and the World Bank.

In keeping with NATO's 2010 Lisbon Summit declaration regarding its commitment to fostering deeper relationships and cooperation with the UN, EU and the OSCE, NATO should develop dialogue with each of these organizations specific to the emerging security challenges posed by hybrid threats.

Recommendations

26. Review current mechanisms for collaboration with industry, with a particular focus on key emerging security challenges.
27. In line with the ambitions stated in NATO's 2010 Lisbon Summit declaration, NATO should commit to developing deeper relationships and cooperation with the UN, EU and OSCE, which focus on the emerging security challenges in a pre-crisis and steady state environment.

6.3 Mechanisms for Developing Relationships

Observation

Given the unpredictability of future hybrid threats, where they might emanate from, and where NATO might choose to engage, it is impossible to know exactly who you would need to form partnerships with to counter future hybrid threats. In order to deal with unanticipated threats, NATO needs to focus on relationship building to enable situational dependant agile partnerships with relevant stakeholders. There are a number of mechanisms that can be used to support this.

Discussion

The approach will require flexibility, agility, and a degree of tolerance for ambiguity. Lessons from operational level coalitions of the willing (such as that employed in Afghanistan) that take into account flexibility of relationship could be reviewed and appropriately applied at the strategic level.

Once a stakeholder is identified, NATO must decide whether having a relationship with them will enhance its ability to recognise and subsequently counter hybrid threats. Each stakeholder will have different characteristics and interests and NATO might need different types of relationships with different stakeholders. It may not be desirable or possible for NATO to develop formal relationships with all the key stakeholders involved with addressing hybrid threats or the enabling environment.

NATO will need to develop relationships tailored to each partner and the degree and nature of engagement will change over time as events evolve. In each case, the relationship between NATO and partners would reflect their particular interests and the degree and nature of engagement would ebb and flow to the degree that those interests were advanced or threatened. In absence this degree of sophistication and flexibility, a comprehensive approach will not be cohesive and effective.

Experiment discussions also emphasized the need for cooperative partnerships with other stakeholders as opposed to directive relationships. In some cases NATO's relationships will be confined to informal information sharing and de-confliction of actions with others. The attributes of these partnerships will need to be: access, transparency, information sharing, and commonality of interests.

In order to develop partnerships organisations need to have a better mutual understanding. Potential mechanisms for NATO were outlined for building relationships with partners to deal with a threat:

- NATO can emphasise and communicate its interest in developing a CA to perspective stakeholders. This would need to articulate its aims in terms of countering common threats and also identify the nature of NATO's contributing role. Developing open and early communication channels helps to build familiarity and trust;
- Develop relationships with stakeholders by inviting them to participate in common risk assessment and planning. It is recognised that this would not be appropriate to all organisations. Where possible, early engagement in these processes would be preferable;
- Exchange of personnel is a good way of improving understanding of different organisations. This may be less feasible and desirable when considering exchanges with some NGOs if it harms the neutrality or credibility of NGOs. Another option in

this case could be to hire former IO or NGO staff that could bring that perspective into NATO;

- Inherent to the need to develop flexible and agile partnerships is the requirement to evolve the way we train and educate within a new community of interest in order to produce adaptive leaders and organizations. NATO needs to seek out and support opportunities to cross-train with stakeholders. This could include hosting exercises with a range of non-NATO stakeholder organizations focused on likely and dangerous challenges presented by hybrid threats;
- Informal coordination and information sharing forums as used at the operational level. Potential field interaction with the various stakeholders; coordination meetings, for de-confliction and debate, but not to coordinate the actions of the others.

Throughout the experiment it was recognized that NATO was not starting from a zero position in developing partnerships and the comprehensive approach. The latest NATO operations planning process includes a specific methodology for interaction with and inclusion of other agencies. In planning for the Libya conflict, NATO was able to contact and de-conflict with a number of non-military organizations, enabling planners to mitigate where NATO may cause them problems. At the strategic level NATO has developed relations with many non-NATO countries and also with several international organizations such as the UN, with regular workshops and meetings. NATO has also been developing civil-military links in relation to piracy off of the Horn of Africa.

Conclusions

NATO must develop longer term relationships with others, building trust and familiarity, whilst working on flexible frameworks that allow partnering in a situational dependent manner, based on where we understand it likely for interests to be common.

NATO can emphasise and communicate its interest in developing a CA to perspective stakeholders. It can then further develop relationships by inviting them to participate in common activities, including workshops, training opportunities or risk assessments. Exchange of personnel is a good way of improving understanding of different organisations. NATO could also recruit former IO or NGO staff that could bring a broader perspective from the international and humanitarian sectors.

NATO needs to seek out and support opportunities to cross-train with stakeholders. This could include hosting exercises with a range of non-NATO stakeholder organizations focused on likely and dangerous challenges presented by hybrid threats.

Recommendations

28. Continue the efforts to include potential partners in the planning and execution of NATO training and exercises. Policy on training must reflect this.
29. Review human resource processes to enable the hiring of staff with the understanding of a variety of approaches to emerging security challenges.

6.4 Leadership and Achieving Unity of Purpose within a Comprehensive Approach to Countering Hybrid Threats

Observation

When dealing with and crafting a comprehensive approach, two of the fundamental questions are who should own the problem and who should be placed in the role of leading the effort. Not all stakeholders will be able to closely align themselves enough for complete unity of effort, command and purpose across all actors; in particular Humanitarian Assistance actors and NGOs will seek to retain autonomy, neutrality and separation from the military.

Discussion

All panels agreed that NATO would normally be a contributing or supporting member of a broader comprehensive approach effort to countering hybrid threats, suggesting the focus of NATO's activities would be oriented upon the areas of security, defence, and logistical requirements or support. When considering conflict prevention it was concluded that NATO should not take the lead but rather consider complementing efforts of others based on its core competencies.

This leads to the question of who should provide leadership. When discussing who should lead a comprehensive approach to countering hybrid threats, participants in two panels outlined legality and legitimacy as key requirements for the leadership role. The two panels also recognized the UN as an established body which can bestow legitimacy and legality upon an effort by enacting its charter and mission.

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

While agreeing to the UN as a legitimizing authority, some participants had a mixed reaction as to whether the UN was capable of acting as a “hub” to coordinate a comprehensive approach effort, with some members expressing strong scepticism. Furthermore participants recognized that exercise of the veto power within the UN could create a situation where you have legitimacy without legal authority whilst in other cases such as recent events in Libya; it is possible to have legal authority granted by the UN but still be perceived as conducting activities that are not legitimate in some quarters.

Conceptually there needs to be an entity with authority for coordinating any comprehensive approach. A suggested template was a multi-organizational collaborative group with international membership and rotating leadership among the key organizations. In order to facilitate something of this nature it is necessary to pre-define the frameworks for partnership, NATO and other actors in the collaborative group would need to determine whether and which actors would come together as part of a single entity or core group and which would remain independent. All panels generally agreed that NATO would not function effectively as a coordinating authority.

Panels also discussed the challenges of unity of purpose due to the different interests, mandates, authority, jurisdiction and modes of operation of various stakeholders. As some actors will need to maintain their autonomy and independence (such as industry, businesses, etc.; for NGOs and humanitarian actors such as ICRC the aspect of neutrality is an additional factor), they will not be prepared to engage in the Joint Planning required for true unity of purpose and action. It is more realistic that NATO will need to work within a community of interest based on limited coincidence of purpose.

Two models of cooperation were discussed; one where there is an agreed single overarching objective with different actors’ contributions to achieving that objective, potentially the “idealized effort” to be attained. The other and typical of the hybrid threat problem, is where a diverse range of objectives but similar actions from different actors contributing towards the end state. The latter model was identified as more realistic but limiting in the ability to achieve unity of purpose, effort, and command. If unity of command is not achievable, the collective approach may still succeed, but in total may take more time and require more resources.

If NATO believes it cannot be the solution alone to addressing Hybrid Threats then the political-military effort it makes must recognize the independence and different purposes of other relevant actors and invite these actors to determine where their activities are complementary to countering hybrid threat activity.

Further Analysis

Recent analysis on comprehensive approaches defines two models of potential cooperation: an integrated approach and a coordinated approach. According to a report by the Norwegian Institute of International Affairs (NUPI), '*Comprehensive Approach: Challenges and opportunities in complex crisis management*,' [8.12] within an integrated approach: *"the aim is to develop systems, processes and structures that will ensure that all the different dimensions are integrated into one holistic effort"* while the coordinated approach is less formal and *"favours utilizing diversity of actors as a way to manage the complexity, while pursuing coherence through bringing the various dimensions together at the country level."*

The conclusion drawn from this discussion in the NUPI report is that a comprehensive approach doesn't require all actors to be engaged at the same levels of cooperation. Friis and Jarmyr discuss how the most effective approach may be a combination of both models where there is an integrated approach among a core group of like-minded actors willing and able to work together closely with integrated systems for assessment, planning, mission management and monitoring and evaluation, together with a coordinated approach for and with actors that are more loosely interlinked with the core. This ensures a more flexible process and allows for coordination methods that respect the culture, mandates, structures and situational factors of the various actors.

To facilitate this, the NUPI study argues for the need for each actor and their higher headquarters elements within a comprehensive approach to understand its independent as well as interdependent realities to better work within a highly dynamic and complex environment. They argue that while integration of all actors into a formal structure is not required, some degree of strategic coherence is a precondition to a coordinated comprehensive approach.

Similarly, from the C2 domain, David Alberts contends that the traditional concepts of command and control are outdated and no longer useful for modern requirements to meet uncertain and dynamic twenty-first century security challenges. [8.13] Alberts posits that *"focus and convergence"* should replace command and control: *"focus as a replacement for command speaks directly to what command is meant to accomplish while being agnostic with respect to the existence of someone in charge or particular lines of authority...convergence speaks directly to what control (the verb) is meant to achieve without asserting that control as a verb is possible or desirable"*.

Alberts further notes that focus includes ideas related to bringing organizations together in the pursuit or achievement of something, it encompasses concepts such as intent, awareness, understanding, and represents a synthesis of how the situation is perceived and understood. The metrics he posits for focus are: establishing shared intent and understanding intent in context. Convergence as articulated by Alberts connotes a journey toward a definable outcome; it implies coordinated movement and some relationships and interactions between and among participants. There is potential for independent entities to converge in the ways they operate and for peer-dominated coalitions to converge. There is a possibility that a collective can behave as a single entity if it is convergent, as such independent actors can achieve operational coherence which has traditionally associated with centrally managed operations.

Conclusions

NATO may not be the most appropriate organization to lead a comprehensive approach to countering hybrid threats, but should support such an effort. Whoever is to lead and coordinate such an effort will need the legitimacy and authority to do so. One example of this would for it to be bestowed via a UN mandate for action.

Not all actors need to be formally involved in a highly structured comprehensive approach to countering hybrid threats. The diversity of actors engaged in the environment may preclude much more than relationships built on convergence of interests. The most effective approach may be a combination approach with a core group of like-minded actors which employ a more coherent integrated approach to assessment, planning, task management and monitoring and evaluation together with a coordinated approach for and with actors that are more loosely interlinked with the core. This ensures a more flexible process and allows for coordination methods that respect the culture, mandates, structures and situational factors of the various actors.

Key to working effectively with different actors will be early engagement and relationship building of various communities of interest prior to problem occurring, in order to establish a level of familiarity and trust required to work together in addressing hybrid threats.

Any political-military effort to counter Hybrid Threats must recognize the independence and different purposes of actors relevant to addressing Hybrid Threats (international business, humanitarian organizations) and the involved actors must be able to determine where their activities are complementary to counter the hybrid threat activity.

Recommendations

30. Develop a strategy for early engagement and relationship building with key communities of interest prior to emergence of crises, in order to establish a level of familiarity and trust required to work together in addressing hybrid threats.

6.5 Preconditions that would facilitate NATO's ability to move towards a Comprehensive Approach.

Observation

The potential for success by a Comprehensive Approach to counter hybrid threats can be greatly enhanced if a number of preconditions can be established prior to the onset of activities.

Discussion

It was recognised that enabling economic growth and development was a principal way to create an environment that would be inherently less favourable for the growth and sustainment of hybrid threats. Initiatives to enhance economic development should be led by national or regional groups that have been invested with legitimacy by appropriate legal authorities.

Security is seen as an essential precondition for economic development and growth. NATO's contribution as a Trans-Atlantic Alliance in this area would be of a supportive, yet critically important, nature. In addition to security, NATO could also provide a range of other support capabilities such as transportation, medical support and communications that would assist those working towards economic development and growth (both governmental and nongovernmental). Security of indigenous infrastructure was seen as particularly important to building the confidence necessary to encourage business investment in developing areas.

Within NATO nations a Comprehensive Approach must bring together different functions of government. However different dynamics drive how political, diplomatic, and military functions are performed, these differences must be recognized and accommodated. The importance of an interlocutor to bring in non-military organizations to the dialogue was emphasized; U.S. experience with engaging State Department representatives to bring interagency actors to DOD-sponsored activities was given as an example.

For the CA and MCCHT concepts to work there must be political sanction or direction to the civilian stakeholders to direct or encourage their engagement with the military to enable NATO to actually operate in accordance with the MCCHT concept.

Conclusions

Movement towards a Comprehensive Approach that will be effective in countering hybrid threats would be greatly assisted if steps can be taken outside of NATO to shape the environment for adopting such an approach. Addressing the root causes that encourage the rise of hybrid threats would be wise, with progress in achieving economic growth and development as perhaps the most important single objective.

If a fundamental part of a Comprehensive Approach is a partnership between the public and private sectors, authoritative political sanction and support is needed to initiate and sustain the building of relationships and protocols between NATO and the other public and private participants in the effort.

Finally, the sophisticated and continuous nature of the challenge raised by hybrid threats demands a proportionate change in the character of political leadership to set and sustain the conditions that will enable the coalition to both deter and defeat hybrid threats.

Recommendations

31. Communicate to political leaders the nature of the hybrid threats facing the Alliance with recommendations for pursuing a comprehensive approach to counter these hybrid threats. Solicit the political support needed to execute the steps required to create a functional and effective community of interest to prevent, deter, and, if necessary, defeat hybrid threats.

6.6 Measuring Success of a Comprehensive Approach to Countering Hybrid Threats:

Observation

How do you measure the on-going success or failure of a comprehensive approach? In order to determine whether a Comprehensive Approach is effectively countering hybrid threats, there need to be metrics and indicators designed to measure progress towards and achievement of common objectives and goals. Clear goals and objectives are a prerequisite, yet the myriad of actors within a comprehensive approach may not share the same vision of success.

Discussion

Trying to identify whether actions are being successful as part of a comprehensive approach, poses a number of challenges. Firstly the problems of finding commonly agreed effect or value across the broad civil-military community of stakeholders will make it difficult to agree to cost-effectiveness metrics. This will mean it will be challenging for the organizations involved to manage and measure their contribution. Secondly there is the issue of accurately measuring effectiveness with regard to countering hybrid threats anyway. The complex and aggregate nature of the conditions to be gauged may defy measurement by a quantifiable and commonly agreed metric, furthermore there will be difficulty in establishing causal linkages between actions and effects with any degree of certainty.

The complex environment and adaptive nature of hybrid threats leads to questions such as; what are the indicators, what to measure, and how will that be recorded? There needs to be a balance between quantitative and qualitative measures. Quantitative measurements of success may often be confused with measures of performance, focusing on input variables (such as money spent, manpower expended etc.) which may lead to false conclusions about the situation. Qualitative assessments by those best qualified to provide such an evaluation often provide valuable context but are subjective and may not be agreed across partners.

There are lessons to be learned from the characteristics of successful evaluation approaches from the reconstruction and stabilization experiences in Iraq and Afghanistan, namely the need to combine as many pieces of qualitative and quantitative information possible (such as gallop polls, interviews, and quantitative data regarding market place perceptions) and triangulate to understand if MOE are working. USAID has launched a new evaluation policy focused upon impact analysis which emphasizes the facets of upfront measurement design during the program planning process as well as evaluation of progress and impact conducted by an independent body. [8.14]

If NATO is interested in commonly understanding alongside partners whether efforts are effective, there may be the need for a common or independent body to provide analysis, metrics and measures of effectiveness. This will mean that measures of effect are not perceived to be tainted by organizational bias. An independent body can be candid about monitoring and perceived success and failure, allowing better debate amongst partners about the changes that need to be made.

Recognising that NATO will likely continue its own assessment of the situation, independent assessment can provide a second opinion. If there are sensitivities the independent body could provide feedback in a confidential manner to leadership, for example reporting to a NATO or common committee. There is precedence for this approach, with the US using independent monitors tasked with providing evaluation and feedback to refine measures of effectiveness and plans in Iraq and Afghanistan. An independent body would need to be professionally and academically recognised in order to provide legitimacy to their work.

Another tool used for assessment and evaluation across multiple organizations is to agree a common assessment framework. If, as identified before, NATO is a supporting entity within a Comprehensive Approach then it may be difficult for it to develop such a framework. NATO could develop and introduce a concept for an assessment framework but would likely need to develop and vet this with the broader community of stakeholders, to gain appropriate buy in. An assessment framework based upon internationally agreed standards would have greatest chance of acceptance by the wider stakeholder community and a number have been developed by nations.

When considering the breadth of hybrid threats and the ability of NATO to deter or prevent them it was suggested that it may be impossible to know if measures taken have been effective. NATO should potentially seek a more realistic objective, such as becoming a better learning organization. By adopting a cyclic "plan, act, monitor, reassess, modify actions" template NATO can iteratively learn about and shape the steady state environment. As part of this there is the need for conducting an upfront assessment to frame the problem and understand the environment, before identifying stakeholders that can best contribute by distinct lines of operation; establishing objectives for each line of operation; building a supervising/coordinating organization; and then establishing a role for NATO.

Conclusions

Given the complexity of hybrid threats and the environments in which they operate, NATO should develop an understanding of the problem context before launching a comprehensive effort to ensure it has planned the appropriate actions and that it has chosen the appropriate metrics and indicators to measure success

When developing measures of effectiveness for countering hybrid threats within a comprehensive approach, NATO should seek to utilize a mixture of impact-focused qualitative and quantitative data, measuring performance as well as progress. NATO

should avoid relying exclusively upon quantitative measures of performance, as use of such input/output data in isolation without the proper context can lead to false conclusions about relative success.

NATO is unlikely to be able to develop a commonly agreed set of metrics for measuring effectiveness in countering hybrid threats across all stakeholders within a comprehensive approach. The best chance of gaining acceptance of an assessment framework by the stakeholder community would be to:

- engage the broader community early to develop a common understanding of the problem
- base measurements and metrics upon internationally agreed standards
- consider the feasibility of using independent evaluators

Recommendations

32. NATO should explore avenues to produce objective evaluations of progress within a comprehensive approach to countering hybrid threats; here, NATO should base measurements and metrics upon internationally agreed standards and consider the feasibility of utilizing independent evaluators to collect metrics data and provide independent evaluations of progress.

7. SUMMARY OF KEY RECOMMENDATIONS

1.	Continue to examine hybrid threats as a provocative and useful way to draw attention to what is new, complex and dangerous in the emerging security environment. Although components of hybrid threats are important, there is a need to examine them from the perspective of their multi-level inter-relationships.	28
2.	With hybrid threats potentially providing a very broad characterization of threat, NATO should try to prioritize the hybrid threats that it faces. It should primarily consider the probability of occurrence of the threats and their potential to have an impact on member nations.	28
3.	NATO should examine its own vulnerabilities with its current capabilities measured against different potential hybrid threats in order to understand better the risks that are posed.	28
4.	The description of hybrid threats should be further developed and socialised, both within NATO nations and externally with other relevant non-military and non-NATO stakeholders and partners.	28
5.	Seek to manage hybrid threats holistically, rather than in a purely military or security perspective. Devise better the indicators for hybrid threats that may not present themselves initially in the military or security domains, but also during a steady state or pre-crisis situation.	32
6.	As security and rule of law are key contributors to a stable region in a steady state and pre-crisis situation, NATO should determine how it can expand further its assistance to relevant regional and local actors during these stages.	32
7.	Develop a mechanism for improving the categorization and prioritisation of hybrid threats. This might include risk-based assessments of the likelihood of occurrence and the potential impacts.	32
8.	Develop and expand existing mechanisms for gathering and sharing threat warnings and indicators so as to include emerging security challenge areas.	34

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

9.	Further identify and then engage organisations (including non-military and from the business and private sectors) with which it can collaborate to attain early indication of hybrid threats.	34
10.	Consider the development of appropriate policies to identify response thresholds concerning the key areas that hybrid threats are likely to emanate from – particularly the cyber domain.	34
11.	To provide legitimacy to act in a proactive manner to effectively counter cyber threats, NATO will need to: <ul style="list-style-type: none"> • Further develop policy and protocols for its own response to such threats; • Support international action to provide regulations, legislation and common enforcement of cyber space in order to combat illegal activities. 	38
12.	Identify (and, when appropriate, advocate) the potential for closing gaps between military and law enforcement areas of responsibility. Explore opportunities to provide a better forum for sharing information with the law enforcement community on issues that cross security, military, financial, cyber and criminal boundaries.	39
13.	Explore opportunities to expand engagement with the financial sector in order to share information about, and develop appropriate responses to, criminal activities that have an impact on security and defence.	39
14.	Interact with other stakeholders (particularly the private sector) to monitor rapidly developing technologies with the potential of being used in innovative ways by adversaries.	43
15.	Advocate and promote the expansion of national and international regulations or 'arms control' type regimes to new technologies that it considers dangerous or a growing threat to its security.	43
16.	Develop improved mechanisms and processes for: <ul style="list-style-type: none"> • Intelligence and information sharing with the non-NATO and non-military community on emerging security challenges; • Collaboration with external partners on timely and relevant assessments 	53

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

	against hybrid threats.	
17.	<p>Reach out and expand relationships with a larger community of stakeholders that can help to identify emerging trends that could affect the security of the Alliance:</p> <ul style="list-style-type: none"> • Develop links with law enforcement and financial institutions to monitor emerging security trends; • Improve mechanisms for working with scientific and research communities to monitor and understand the potential impact of emerging technology developments, particularly cyber; • NATO should augment its planning processes in a manner which allows for more efficient informal information sharing with those unable to participate directly. 	53
18.	ACT should investigate further how hybrid threats can be built into NATO exercises and how a wider community of interested organisations can participate in NATO training and exercise opportunities.	54
19.	ACT should investigate how it can integrate the concept of hybrid threats into the NATO defence planning process to understand better what capability changes may be needed to counter the new challenges.	54
20.	Develop relationships with key civilian stakeholders (including those that may not initially be receptive to doing so) who are better placed to monitor key environmental factors linked to hybrid threats – this will enable development of necessary situational awareness.	57
21.	For early warning, as well as situational awareness, NATO should augment its intelligence fusion capability with data related to cyber security, law enforcement and financial intelligence.	57
22.	<p>Review crisis management processes to determine whether they are suitable for non-crisis decision-making in a dynamic, steady state, security environment. This could include:</p> <ul style="list-style-type: none"> • An examination of how the Alliance conducts ‘risk and threat management’ relative to ‘crisis management’. 	60

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

	<ul style="list-style-type: none"> • Examine crisis management terminology and processes to determine whether NATO should include or reflect risk and threat management standards and processes used by non-NATO organizations. • Review Chapter 2 of the NATO Crisis Response Manual to determine its adequacy and responsiveness for steady state (non-crisis) preventive actions. 	
23.	Explore development of a network for engagement, through a risk assessment and integration body, which could feed situational awareness for risk assessment and contingency planning. The NATO Shipping Centre could be evaluated as a model for this network.	60
24.	Determine whether a 'counter-messaging' approach is appropriate and feasible as part of the strategic communications required for countering hybrid threats.	62
25.	<p>Once NATO has determined who the key non-military/non NATO stakeholders are, it must understand their mandate, limitations, interests and goals (relative to the situation) in order to determine what type of relationship is feasible and desired. Key to gaining this understanding is:</p> <ul style="list-style-type: none"> • Recognizing and differentiating between true, enduring, and near-term interests of stakeholders; • Recognising which are the most feasible areas of common purpose for NATO and the range of potential partnerships; • Developing methods for learning and understanding changing stakeholder interests over time (from the stakeholders' perspectives). 	67
26.	Review current mechanisms for collaboration with industry, with a particular focus on key emerging security challenges.	76
27.	In line with the ambitions stated in NATO's 2010 Lisbon Summit declaration, NATO should commit to developing deeper relationships and cooperation with the UN, EU and OSCE, which focus on the emerging security challenges in a pre-crisis and steady state environment.	76
28.	Continue the efforts to include potential partners in the planning and execution of NATO training and exercises. Policy on training must reflect this.	79

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

29.	Review human resource processes to enable the hiring of staff with the understanding of a variety of approaches to emerging security challenges.	79
30.	Develop a strategy for early engagement and relationship building with key communities of interest prior to emergence of crises, in order to establish a level of familiarity and trust required to work together in addressing hybrid threats.	83
31.	Communicate to political leaders the nature of the hybrid threats facing the Alliance with recommendations for pursuing a comprehensive approach to counter these hybrid threats. Solicit the political support needed to execute the steps required to create a functional and effective community of interest to prevent, deter, and, if necessary, defeat hybrid threats.	84
32.	NATO should explore avenues to produce objective evaluations of progress within a comprehensive approach to countering hybrid threats; here, NATO should base measurements and metrics upon internationally agreed standards and consider the feasibility of utilizing independent evaluators to collect metrics data and provide independent evaluations of progress.	87

8. REFERENCE DOCUMENTS

1. 1500/CPPCAM/FCR/10-270038 AND 5000 FXX/0100/TT-0651/SER: NU0040 Dated 25 August 2010: *BI-SC Input for a new Capstone Concept for The Military Contribution to Countering Hybrid Threats*.
2. Enclosure 2 to 5000 FXX 0100/TT-7361/Ser:NU0367 dated 20 June 11; *Assessing Emerging Security Challenges In the Globalised Environment – The Countering Hybrid Threats Experiment First Impressions Report*.
3. HQ SACT Experiment “*Assessing Emerging security Challenges in a Globalised Environment – Countering Hybrid Threats*” Scenario dated 09 May 11. Environmental Conditions, International Context, NAC Initiating Directive, Silver and Ivory Sea Association.
4. PO(2010)169, The Alliance Strategic Concept, 19 November 10.
5. Hybrid Threats Description 1500/CPPCAM/FCR/10-270038 AND 5000 FXX/0100/TT-0651/SER: NU0040 Dated 25 August 2010: *BI-SC Input for a new Capstone Concept for The Military Contribution to Countering Hybrid Threats* dated (Paragraph 7).
6. ACT Publication - *Assured Access to the Global Commons – Maritime Air, Space and Cyber*; dated 03 April 11.
7. Security and Defence Agenda. *Protecting the Global Commons*, Dolce La Hulpe, Brussels, September 16, 2010.
8. NATO Crisis Response System Manual, Chapter 2 – Preventative Options, 2009 (NU)
9. NATO Glossary of Terms and Definitions, AAP-6(2010)
10. David Alberts & Richard Hayes. *Planning: Complex Endeavors*. USDOD CCRP, April 2007
11. U.S. Institute for Peace “*Guide for Participants in Peace, Stability and Relief Operations*” (2007), Robert Perito (ed)
12. Norwegian Institute of International Affairs (NUPI), “*Comprehensive Approach: Challenges and opportunities in complex crisis management*.” Karsten Friis and Pia Jarmyr (eds), 2008

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

13. David S. Alberts, *“Agility Focus and Convergence: The Future of Command and Control,”* The International C2 Journal, Vol 1, No.1, 2006.
14. United States Agency for International Development (USAID) Evaluation Policy, Bureau for Policy Planning and Learning, January 2011

9. ACRONYMS

ACO	Allied Command Operations
ACT	Allied Command Transformation
BI-SC	Bi-Strategic Command
CA	Comprehensive Approach
CBRN	Chemical, Biological, radiation and Nuclear.
CHT	Countering Hybrid Threats
CRM	Crisis Response Manual
DDR	Disarmament, Demobilization and Re-integration
EPCIP	European Program for Critical Infrastructure Protection
EU	European Union
FATF	the Financial Action Task Force
FER	Final Experiment Report
FIER	First Impressions Experiment report
FRONTEX	Frontières Extérieures - European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
ICRC	International Committee of the Red Cross
IDP	Internally Displaced Person
IFRC	International Federation of the Red Cross
IGO	Inter-Governmental Organisation
IMF	International Monetary Fund
INTERPOL	International Criminal Police Organisation
MCCHT	Military Contribution to Countering Hybrid Threats
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organisation
NDPP	NATO Defence Planning process
NDU	National Defence University
NGO	Non-Governmental Organisation
NNEC	NATO Network Enabled Capability
NUPI	Norwegian Institute of International Affairs
OECD	Organization for Economic Co-operation and Development
OSCE	Organization for Security and Cooperation in Europe
PSC	Private Security Company
SACT	Supreme Allied Commander Transformation
SAS	Systems Analysis Studies
SCADA	Supervisory Control and Data Acquisition
SDA	Security and Defence Agenda
SHAPE	Supreme Headquarters Allied Powers Europe
UN	United Nations

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

USAID
USJFCOM JIWC

United States Agency For International Development
United States Joint Forces Command – Joint Irregular
Warfare Centre

10. POINTS OF CONTACT

ANALYSIS LEAD & FER POC1:

Alex Smethurst
GBR Civ A-2
Operational Analyst
HQ SACT TSC FEA 0120

Phone: (001) 757-747-4271
IVSN: 555-4271
Fax: (001) 757-747-3863

POC2:

Rich Hills
Lt Col RM (GBR)
SO1 Deployable Forces IPT
HQ SACT PAX 0070

Phone: (001) 757- 747-3268
IVSN: 555-3268
Fax: (001) 757-747-3863

ANNEX 1: EXPERIMENT PARTICIPATION

PANEL 1 - CYBER TECHNOLOGY AND ECONOMIC SECURITY

	Function/Role	Command/Organisation
1	Coop Cyber Defence CoE SME	Cyber Defence CoE
2	Defence Against Terrorism CoE SME	DAT CoE
3	Counter Threat Finance SME	US EUCOM
4	Coop Cyber Defence CoE SME	Cyber Defence CoE
5	NATO Rule of Law (Cyber) SME	Portsmouth Business School, University of Portsmouth, UK
6	National Law Enforcement and Organized Crime	Retired Advisor for Romanian Ministry of Administration and Interior
7	International Police SME (National Rep)	SHAPE
8	NATO Operations Planning and C2 SME	SHAPE
9	Cyber Critical Infrastructure SME	Cyber Crime Research Institute
10	International Business (Information Communications Technology IT)	IBM/EU
11	Communication Industry (Google, Facebook, IT Co) SME	CASSIDIAN METAPOLE Systems/FRANCE
12	Cyber Defence Academic SME	Institute Français de Relations Internationales (IFRI)

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

13	World Bank SME/ International Financial Institution SME	World Bank
14	Devil's Advocate / Adversary SME	General Dynamics UK
15	Hybrid Threat SME	Bundeswehr Transformation Centre Germany
16	Cyber Information Warfare SME	Carnegie Endowment for International Peace Washington/US
17	Cyber Security SME	US State Department
18	National Security SME	Royal United Services Institute for Defence and Security Studies
19	Information Management SME	HALTIK (ICT Agency)
20	Identification Management SME	Technology Morpho UK, Limited
21	JAP National Rep (Civilian Protection)	Defence Policy Bureau Ministry of Defence/JAPAN
22	DEU National Rep	German MoD
23	SWE National Rep	Associate Professor War studies, Swedish National Defence College, Stockholm Information Systems Security Association (ISSA)
24	Network Centric and Information Operations SME	US JFCOM

PANEL 2 - STABILISATION, CONFLICT PREVENTION AND PARTNERSHIP

	Function/Role	Command/Organisation
1	NATO Stability Operations/CIMIC SME (SHAPE)	SHAPE
2	Military Cooperation SME (SHAPE)	SHAPE
3	International Committee of the Red Cross (ICRC) SME	ICRC
4	Rule of Law/Jud. / EULEX	Office for the protection of classified information (NSA)At the Ministry of Interior of Slovenia
5	International Police SME (Training) EUROPOL INTERPOL	NLD Task Force Counter IED/NLD
6	EU Stabilisation and Reconstruction (Security and Sector Reform) SME	Institute for European Studies, Belgium
7	PIRACY PREVENTION CENTRE	Norwegian Defence University
8	UN Development Program - UNDP SME	National Defence University/Institute for Strategic Studies
9	UNHCR / World Bank SME	McGill University, Montreal, Canada
10	Humanitarian SME	Canadian Government
11	CCoE SME	CIMIC CoE
12	Defence Against Terrorism CoE SME	DAT CoE

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

13	CBRN SME	JCBRN Defence COE
14	Trade and Finance SME	US EUCOM
15	Operations in Confined and Shallow Waters CoE SME	COE for Operations in Confined and Shallow Waters
16	Regional SME (Academic social science)	Royal United Services Institute, UK
17	International Finance /Counter Threat Finance SME (Banking)	MONEYVAL Committee /Council of Europe, FRANCE
18	Critical Infrastructure SME (National Rep)	University of Rome "Tor Vergata", ITALY
19	Military Environmental SME	French CD&E Centre
20	NGO (Medical)	HQ SACT
21	Devil's Advocate/Adversary SME (info about area)	Special Inspector General for Iraq Reconstruction
22	Partnership Development SME	ICCT
23	Strategic Communications SME	SEGARRATERES INTERNATIONAL
24	Democratic Control of Armed Forces SME	The Security Companies Professional Association Geneva Centre for the Democratic Control of Armed Forces (DCAF),Switzerland
25	JAPCC CoE SME	JAPCC CoE
26	National Representative (Italy)	MOD Italy

27 **Humanitarian/Refugee SME** IRC-UK

PANEL 3 - GLOBAL COMMONS AND RESOURCE SECURITY

	Function/Role	Command/Organisation
1	NATO policy SME	SHAPE
2	Political Advisor	STRIKFORNATO
3	Rule Of Law/Judicial SME	Center of Excellence for Stability Police Units, Vicenza, Italy
4	GLOBAL COMMONS/SPACE SME	Naval Postgraduate School
5	Cyber Security SME	BOEING
6	International Police Org (National Rep)	Landelijk Coordinator CBRN-Explosieven Veiligheid Politie
7	Defence Against Terrorism CoE SME	DAT CoE
8	CBRN CoE SME	JCBRN Defence COE
9	CBRN SME	Norwegian Defence Research Establishment
10	Operations in Confined and Shallow Waters CoE SME	COE for Operations in Confined and Shallow Waters
11	Natural Resource Extraction SME	The Peace Research Institute Oslo
12	Air transportation civilian companies	Schenker Deutschland AG
13	Land transportation civilian companies	KUEHNE NAGEL
14	International Financial SME (Banking)	The Hague Centre for Strategic Studies
15	Critical Infrastructure SME	Centre for European Security Strategies (CESS)

NON SENSITIVE INFORMATION RELEASABLE TO THE PUBLIC

16	UNHCR SME	UNHCR
17	Anti-Piracy, maritime security SME	Maritime Command Northwood (MCNW)
18	Sea Shipping and Insurance Industry SME	Den Norske Krigsforsikring for Skib (DNK)
19	Maritime Industry and Maritime Security SME	Norwegian Ship owners Association
20	Devil's Advocate/Adversary SME	KBR
21	Oil SME	SHELL
22	Strategic Communications (Media) SME civilian	SEGARRATERES INTERNATIONAL
23	NGO (Environmental)	Bundeswehr Transformation Centre
24	International Atomic Energy Commission	World Association of Nuclear Operator WANO
25	FRA National Rep	French MOD