Military Implications Workshop

Read-Ahead

12-13 November 2014
Royal Military Academy
Brussels, Belgium

<u>Organized by</u>
Allied Command Transformation, Norfolk
Strategic Plans and Policy Directorate

Contents

Général d'armée aérienne Jean- Paul Paloméros
Supreme Allied Commander Transformation keynote speech
MC Conference Vilnius, Lithuania
20 September 2014

"Thank you Knud,

The very stimulating presentations and comments this morning have emphasized the increasing volatility of our security environment due to ambition competing interests between some major powers (in Asia), disaggregation of states as Libya, use of ambiguity and hybrid threat by state actors and organized barbarity of religious fundamentalists empowered by strategic communication. ***Anticipate how our military forces could be employed in this uncertain future is the aim of the Framework for Future Alliance Operations that we are currently developing with your staffs. It is an ambitious endeavour, but indispensable to share the conclusions of your national studies so that we are able to define and prepare the capabilities that we will need together tomorrow. It is all the more important as we are about to start a new cycle of NDPP in 2015, for which our military advice should be clearly stated.***

(....)

To counter this increasing level of ***instability situations***, our Bi-SC approach points out once again the need for an improved, credible and ***shared Strategic awareness***. To seize opportunities and respond correctly to emerging crisis, political and military leaders will request not only a full set of JISR assets to detect, understand, visualize and adapt to the premises of a crisis but as well creative and critical thinking to describe the possible options and above all a ***functional security networking*** with regional Partners and different organizations to communicate, share assessment in a timely and coordinated manner.

Our ***operational agility***, on the model of our current efforts on the RAP will provide our decision makers more options by making military forces more flexible and responsive. In practice, units should be able to operate with scalable troop organization and command and control structures that are able to aggregate and disaggregate quickly and to adapt easily to the circumstances. Interoperability will remain at the centrepiece of operational success.

While improving our responsiveness, we will have to ensure our Alliance the ability to conduct sustained operations in spite of surprise or strategic shock, to quickly recover from setbacks and to face the likely simultaneity and diversity of crisis, in summary, to develop our shared resilience. This implies sustained Defence budget efforts as well strengthening our ties with partners and organizations. Therefore, in the scope of what I will call our ***Global resilience***, I will strongly advocate first to refocus on comprehensive approach and secondly to maximize our collaboration with strategic partners and in particular the European Union by breaking the invisible "barriers" between our two organizations and proposing a clear roadmap in this regard.

Looking ahead, our next step will start this month with the development of the military implications of this future security environment. They should deliver a series of potential tasks or targeted effects to fuel our capability development process and the NDPP.

To conclude, **FFAO will capitalize on those observations to propose orientations for the future. I'm convinced that we need this shared framework to develop a relevant Defence Planning Process. It must place a premium on being agile enough to adapt, fostering innovation in operational planning and maintaining a clear margin of error in both sizing and structuring the force. I therefore propose that we carry on this process in close coordination with your staffs and may other stakeholders. <u>The next milestone is a key workshop in 12-13 November in Brussels which conclusions will be presented to the MC</u> and to you during our next session if you agree. It is never too early to prepare the future even and because it is "difficult".**
Thank you for your attention".

Agenda

Wednesday, 12 November 2014

0900-0945 Check-in/Registration and Coffee

0945-1030 Plenary Session: Welcome and Introductory Remarks

1030-1100 Coffee Break

1100-1130 Syndicate Session #1

Intro by the 5 syndicates: Maritime, Land, Air/Space, Human & Cyber.

1130-1230 Lunch (Self-paid)

1230-1415 Syndicate Session #2

Sub-syndicates analyse SMP in **State to State** to derive MI

1415-1445 Coffee Break

1445 -1630 Syndicate Session #3

Sub-syndicates analyse SMP in **Urban/Mass Population** to derive MI

1630 -1730 Syndicate Session #4

Syndicates consolidate sub-syndicate work

1730 -1800 Plenary Session: Wash up day one

1830 -2000 Reception in the Atrium

Thursday, 13 November 2014

0830-1015 Syndicate Session #5

Sub-syndicates analyse SMP in **Non-State Actors** to derive MI

1015-1045 Coffee Break

1045-1130 Syndicate Session #6

Sub-syndicates analyse SMP in **Global Commons** to derive MI

1130-1230 Lunch (Self-paid)

1230-1330 Syndicate Session #7

Continuation of Session #6

1330-1430 Syndicate Session #8

Syndicates consolidate sub-syndicate work

1430-1530 Plenary Session: Syndicate Work Debrief, Closing Remarks

The findings of each syndicate will be debriefed in plenary session. The way ahead will be presented.

Workshop Overview

- **Aim:**
  - o **Maximise collaboration with NATO experts from the futures community of interest**

- **Objective:**
  - o **Conduct a strategic level analysis of the Instability Situations, Strategic Military Perspectives assessed within domains, using the Capability Hierarchy Framework (CHF)**

- **Expected Outcome:**
  - o **Derive CHF-structured ideas to inform post-workshop generation of Military Implications (MI)**

Groups of Instability Situations

(1)	**Global Commons**
	• **Access and Use of Global Commons Challenged**
	• **High-Impact Cyber Threat**
	• **Space Capability Disruption**
(2)	**Urban/Mass Population**
	• **Disruptive Impact of Migration**
	• **Large-Scale Disaster**
	• **Megacity Turmoil**
(3)	**Non-State Actors**
	• **Conflict in Euro-Atlantic Region**
	• **Non-State Actors Rival State**
	• **Weapons of Mass Destruction/Effect (WMD/E) Use or Threat**
(4)	**State to State Conflict**

NORTH ATLANTIC TREATY ORGANIZATION

Supreme Allied Commander, Europe
B-7010 SHAPE
Belgium

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

DRAFT
version 11

Framework for Future Alliance Operations

Strategic Military Perspectives

CHAPTER 1 - INTRODUCTION

1-1.   The future security environment of 2030 will present NATO Nations with a wide range of conventional and unconventional threats. NATO's strong conventional and nuclear capabilities remain the bedrock upon which the security of the Euro-Atlantic region rests. Because of the Alliance's strong conventional forces, adversaries increasingly will choose unconventional methods to challenge the Alliance, such as hybrid[1] warfare and cyber-attacks. In order to retain its ability to deter aggression and prevail in conflict, the Alliance must continue to invest in modern, conventional forces as well as enhance, adapt or develop the capabilities needed to counter adversaries operating in unconventional ways and in non-traditional domains.

1-2.   Strategic Military Perspectives (SMPs) provide six areas of focus for enhancing Alliance forces to address the full range of conventional, hybrid and unconventional threats of the future. These perspectives are military advice from Supreme Allied Commander Transformation and Supreme Allied Commander Europe that provide guiding principles to inform long-term military transformation through NATO defence planning. These principles support longer term processes including the development of guidance for the NATO Defence Planning Process, concept development, education training and exercises so as to support adaptable and flexible future forces.

1) **Adaptive Shaping:** Proactively influencing the future security environment to enhance Alliance forces' freedom of action.

2) **Military Operational Guidance:** Establishing predetermined, military specific authorisations, boundaries and guidance that Alliance forces may require to engage future challenges and exploit opportunities successfully

3) **Operational Agility:** Providing decision makers more options by making military forces more flexible and responsive.

4) **Security Networking:** Enhancing Alliance capacity and options through an expanded network of partners.

5) **Shared Resilience:** Ensuring the Alliance retains the ability to quickly recover from setbacks and conduct sustained operations in spite of surprise or strategic shock.

---

[1] Hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives. IMSM-0292-2010 "*Hybrid Threat Description and Context*."

6) **Strategic Awareness:** Increasing decision-space for senior leaders by providing information on potential sources of instability sooner and in greater detail.

1-3.   While SMPs represent high-level, broad guidance, the next step of the Framework for Future Alliance Operations, Military Implications, will contain concrete, military-specific deductions that may drive change in how the military prepares for and executes operations. Appendices to this document provide source data for development of SMPs. Appendix A gives background on ACT's Long-Term Military Transformation effort. Appendix B contains a summary of the 15 trends identified in the SFA 2013. Appendix C lists the 10 Instability Situations derived from the SFA. Appendix D lists Common Challenges associated with the SFA and the Instability Situations.

CHAPTER 2 - THE FUTURE SECURITY ENVIRONMENT OF 2030

2-1.   The future security environment is shaped by the intersection of three significant questions:

(a) **What types of challenges might NATO face?** NATO will face adversaries consisting of both traditional state and non-state actors, who work independently or in concert to challenge the Alliance in ways that complicate consensus response. Adversarial states will be able to use non-state proxies to deny responsibility for their actions. Non-state actors will be more difficult to identify and to deter, as they may not possess resources or assets that can be credibly threatened by military force.

(b) **Where will NATO have to operate?** In addition to traditional territorial domains, military operations in the future will likely occur in un-governed or under-governed regions, in large urban areas with complex terrain, and in the global commons, to include space and cyberspace. Operations in these areas and domains may not have traditional boundaries; therefore, adversaries may test NATO resolve in mission areas that fall outside of NATO's traditional Euro-Atlantic territorial focus and where the Alliance may not have clear, pre-existing policies or legal jurisdictions.

(c) **How will NATO's future adversaries operate?** The underlying theme in the instability situations is that future threats will occur both within and outside of NATO's traditional conventional, territorial, state-centred focus. Future threats will seek to operate in the "grey areas" or "seams" of the Alliance, evading attribution through calculated ambiguity, complicating consensus through non-territorial, unconventional attacks, and avoiding conventional confrontation through hybrid warfare.

2-2.   While NATO is strong in conventional capabilities and prepared for traditional territorial conflict, the Alliance must also prepare for states employing non-state proxies and using hybrid means to achieve their objectives. In addition to conventional warfare, future threats are likely to combine special operations and irregular forces (including mercenaries and criminal organisations) as well as offensive cyber and space actions. Dedicated adversary psychological operations will exploit social and traditional media to win the battle of the narrative in specific locales. Future adversaries will have access to an increasing range of new capabilities and technologies that will give them qualitative parity or advantage in some domains and will, therefore, pose a greater threat to NATO.

2-3.   Adversaries will attack Alliance cohesiveness. Actors in the future will seek to engage NATO in innovative ways that magnify possible divisions within the Alliance and operate at a level that makes consensus-based response more difficult. Furthermore, the speed and pervasive nature of the flows of people, data, disease, money, drugs and weapons through the global commons and elsewhere allows these actors to move easily from one area to another converging for operations and then dispersing rapidly to evade detection and engagement.

CHAPTER 3 - ADAPTIVE SHAPING

3-1.   Adaptive shaping is the ability to influence the security environment in order to set the conditions for Alliance success, thereby preserving the flexibility, agility and freedom of action for friendly forces, while denying a favourable environment to potential adversaries. Future adversaries can take advantage of conditions such as natural and man-made disasters, increasing youth populations, inadequate energy and industrial infrastructure and insufficient security to create instability. Adaptive shaping can help to strengthen stability and prevent or reduce the creation of under-governed areas or power vacuums where adversaries can thrive.

3-2.   Adaptive Shaping is proactive, deliberate and continuous. Adaptive Shaping merges, coordinates and builds upon the Alliance's current shaping activities to anticipate and counter a more diversified range of potential threats from a larger number of state and non-state actors. Adaptive shaping will require the Alliance to maximise its network of partners to achieve its objectives and will require planners at all levels to envision innovative approaches to rapidly evolving challenges.

3-3.   Adaptive Shaping actions are aimed at building capacity in our member Nations and partners, through such activities as defence capacity building, security force assistance, security cooperation, foreign military sales, training, exercises and maintaining an open door to those who share our values.

Adaptive Shaping also attempts to mould the global environment through arms control, disarmament and non-proliferation efforts. It includes actions in emerging domains such as space and cyberspace to maintain the Alliance's access to these domains and to leverage technology and innovation in ways that are beneficial to the Alliance.

3-4.   Some of the greatest opportunities for Adaptive Shaping occur in the information environment. Communicating NATO's narrative via traditional and social media for reassurance, support-building and deterrence purposes can have a powerful, positive impact on stability. NATO should continue to develop and implement a strategic narrative that clarifies Alliance positions and policies by establishing communication and engagement goals, identifying and understanding of relevant audiences, and providing straightforward content.

3-5.   **Conclusion**: Adaptive Shaping will help NATO influence its security environment by expanding both its network of partners and its set of activities to counter a broader range of potential threats in the future. It will coordinate and merge efforts such as defence capacity building, security force assistance, education, training and exercises to form a coherent and consistent shaping effort. Strategic communications efforts between political, strategic, and operational/tactical levels should be increasingly aligned and synchronised through a central coordinating agency. Training in strategic communications will help to better incorporate these efforts into operational plans.

CHAPTER 4 - MILITARY OPERATIONAL GUIDANCE

4-1.   Military Operational Guidance is the establishment of predetermined, military specific authorisations, boundaries and guidance that Alliance forces may require to engage future challenges and exploit opportunities successfully. These policies cover the range of domains (such as cyber) and types of operations (such as hybrid warfare) that NATO may face in the future. Military Operational Guidance aims at removing potential obstacles and filling in gaps in policy before they impede NATO's ability to operate in a proactive, resilient and agile manner and before they might be exploited by potential adversaries. Military Operational Guidance is a prerequisite for rapid military decision-making within the Alliance.

4-2.   National strategic governmental direction will remain paramount in the future. In the uncertain future security environment, NATO's Military Operational Guidance process needs to anticipate, adapt and evolve to keep pace with rapidly changing events. Within the borders of political guidance, NATO Military Operational Guidance provides a range of military specific guidelines which clarify the framework and operational boundaries for Alliance planning and actions. This will support military decision-making and concept development in emerging areas such as the military aspects of crisis

management, hybrid threats, global commons, partnerships, and rules of engagement.

4-3.　　Conventional threats combined with intensified use of hybrid warfare enhanced through technological advancement will challenge existing NATO military policies in new ways.　Operations across the global commons, including the non-traditional domains of cyber and space, and the use of new technologies increase the likelihood of actions falling within gaps of existing policy framework.　These new challenges will likely reduce decision time and limit options available to senior leaders.

(a) **Crisis Management:** Refining crisis response policies and disaster relief action plans will increase NATO readiness to respond more efficiently and effectively.

(b) **Hybrid Threats:** Preparing Alliance forces for the increasing adversary use of hybrid or asymmetric warfare will enable NATO to anticipate, detect and respond more effectively to hybrid threats.

(c) **Global Commons:** Most activities in the global commons are covered by international treaties. Some actors, however, will have an increased capacity to disrupt flows of people, resources and assets, thereby degrading the lines of communication through the global commons. Establishing a framework of military policies adapted to address the limits of military actions within the global commons is necessary to support possible operations in reaction to such disruptions.

(d) **Partnerships:** New types of partnerships could enhance specific areas of cooperation with a whole range of actors, from states and corporations to international organisations and non-governmental organisations. These partnerships would significantly enhance Alliance capabilities by filling capability shortfalls and taking advantage of areas of mutual interest between NATO and outside organisations, particularly within new domains like cyber and space.

(e) **Rules of Engagement:** Asymmetric and hybrid warfare, operations among civilian populations in complex terrain, working with private military security companies and operations in the information and cyber environments will inevitably cause differences between Nations on what they deem acceptable in the application of force. Nations will continue to evaluate and approve rules of engagement as it deems appropriate. Therefore, establishing military policy for ROE development, coordination and implementation will help to limit the adverse impacts of the ambiguous, complex and rapidly-changing future security environment.

4-4.　　**Conclusion**: Military Policy Development will help the Alliance to prepare for emerging threats, reduce vulnerabilities and policy gaps, and

facilitate accelerated decision-making at all levels. Potential refinements to the ROE development process, including long-term guidance that reflects the new threats of cyber, space, and hybrid warfare will be paramount to this effort.

CHAPTER 5 - OPERATIONAL AGILITY

5-1.　　Operational Agility is the ability to respond effectively to dynamic, complex and uncertain operational challenges with appropriate, flexible, and timely actions. Future operations will be characterised by highly adaptive adversaries, equipped with a mix of low-tech and advanced military technology and utilising new and ever-changing methods to achieve their aims. Operational Agility provides an opportunity to preserve decision space and leads to multiple creative and scalable options for decision makers.

5-2.　　Adjusting complex operations effectively demands military leaders who demonstrate creativity while developing solutions to unusual or wicked problems. A thorough understanding of the context of any particular situation will be necessary in order to act boldly and decisively in a measured way to achieve both tactical and operational advantages that maximise strategic options. Operational Agility also requires timely decision-making by operational and tactical leaders. This decision-making can be aided by efficient information management, as well as a mission-command type leadership philosophy that allows decentralised, flexible decision-making within the overall commander's intent.

5-3.　　In addition to innovative and creative leaders, the Alliance will need flexible, tailorable and robust forces. Interoperability, facilitated by the evolution of NATO joint doctrine and standardisation, will be crucial for Alliance forces in the future. Alliance forces will need to be specifically prepared to conduct rapid, distributed operations, often with little prior notification. Providing rapidly-deployable response capacity and pre-packaging of capabilities will enhance responsiveness. Alliance forces should increase their ability to operate in complex terrain, including networked large urban areas or megacities. Alliance forces could also increase their responsiveness by quickly exploiting new technologies such as autonomous systems, merging new technologies with existing high and low-technology capabilities.

5-4.　　To maximise the ability of the NATO to apply appropriate combinations of Alliance Power, it should emphasise the ability to assemble and train diverse multinational units to address challenges that have seized our common attention. Recognising that the shape of challenges will shift and change over time, the Alliance should have the capability to bring new alliance units, force and capabilities on line when necessary, and redeploy units and forces as the complete their missions.

5-5.   **Conclusion**: Operational Agility places significant importance on the development of leaders with creativity, initiative, and the ability to make timely, effective decisions that support their unit's mission. It reinforces the requirement to organise and operate based on assigned tasks, with scalable troop organisations and command and control structures that are able to aggregate and disaggregate quickly and to adapt easily to the circumstances encountered across all domains and the full spectrum of military operations. Operational Agility focuses on developing flexible units and creative leaders comfortable in situations that are characterised by ambiguity, complexity and rapid change.

CHAPTER 6 - SECURITY NETWORKING

6-1.   Security Networking presents an opportunity for NATO to act in concert with a variety of state and non-state actors to address future security threats in a holistic way. Security Networking means cooperative, persuasive and proactive engagement with organisations and actors, both inside and outside of NATO, to develop a wider range of capabilities. NATO might strive to work with others to address security in a more comprehensive manner while retaining the sole responsibility for Alliance security and the capabilities to achieve its objectives. These partnerships can be temporary or enduring in nature and could include international and national security, law enforcement, intelligence and other organisations.

6-2.   The scale, complexity and nature of future challenges will require the Alliance to act in cooperation with others, including both states and non-state actors. Thus, future operations will be characterised by an increasing number of actors coexisting and working with or beside NATO in all domains, including domains such as cyber and space which are growing in importance. These actors may provide a range of services such as police and medical training, electrical power production, supply of fresh water or governing capacities; however, they would best act in a complementary way to avoid duplication and maximise efficiency, effectiveness and affordability. NATO may play a new role as an enabler or facilitator in any operation by using its assets to coordinate and assist all participating actors. Such cooperation may also include, on a case by case basis, an exchange of sensitive information relevant to specific operational needs of the cooperating actors. This coordination and cooperation should be integrated at all levels from tactical through strategic to facilitate a shared view of the situation.

6-3.   Such a view of security as a network would build upon existing agreements and develop new relationships of varying scope. This new expanded understanding of partnerships would include prearranged collaboration with a large variety of actors through education, training and

exercises and would help NATO to improve its ability to respond to crisis or conflict.

6-4. **Conclusion**: Security Networking is a continuation of current NATO policies, expanded and modified for a wider range of actors and activities in different domains in the future. These new, expanded associations should be variable in length and depth of commitment, allowing NATO to benefit from numerous temporary partnerships for specific aims without over-committing the Alliance.

CHAPTER 7 - SHARED RESILIENCE

7-1 Shared Resilience is the characteristic of having sufficient capacity across the defence and security community to provide a shared ability to endure adversity over time and to recover quickly from strategic shocks or operational setbacks. Chaotic and complex operational environments, where adversaries may employ sophisticated anti-access and area denial capabilities, will demand increased resilience from Alliance forces in the future. Shared Resilience encompasses structures and systems necessary to provide NATO with a constant capability to analyse and process information throughout a crisis despite potential interruption.

7-2 In the increasingly complex environment of the future, threats will be less foreseeable. NATO planning should be conducted in such a manner that the effects of complexity, surprise or strategic shock do not prevent NATO from accomplishing its Core Tasks. This level of resilience will require the Alliance to connect with a range of different actors across the military and civil security spectrum. Under this construct, all organisations that play a role in security, stability and safety will have to work together in a more unified and coordinated manner. A certain degree of trust, facilitated by a common understanding and vision among Alliance members and their partners, will be important to achieving this coordinated effort.

7-3 Sustainment is another key aspect of Shared Resilience. Alliance forces must possess the capabilities to sustain both themselves and, if necessary, coordinate sustainment for segments of the local population as the introduction of large military forces may tip delicate local resource balances. Pre-aligned coordination and cooperation among civilian and military authorities will be essential in this case. The Alliance will also need to have the capability to provide decentralised sustainment to all echelons of its dispersed military forces by expanding sustainment support networks.

7-4 **Conclusion**: To achieve Shared Resilience, the Alliance must seek redundancy in its systems wherever possible. However, Shared Resilience is more than redundancy, it's about learning to operate despite the loss of critical systems and developing a system wide capability to overcome and adapt to

changing circumstances. In order to quickly recover from strategic shocks or operational setbacks, the loss of critical systems should be a regular part of the Alliance education, training and exercise program for units and leaders. Shared Resilience will require a mix of high and low technology to be incorporated in Alliance and National military systems.

CHAPTER 8 - STRATEGIC AWARENESS

8-1 Strategic Awareness represents an opportunity to increase Alliance cohesion through a shared assessment of current and future strategic level challenges and opportunities, and to allow timely synchronisation and alignment of military planning and organisation with political intent. Institutions and states face a rapidly growing range of security challenges and opportunities including those presented by trans-national and non-state actors. State-sponsored proxies using hybrid warfare methods require the Alliance to gain a broad knowledge and understanding of a wide range of criteria that might fuel a potential crisis or conflict. By identifying the first signals of an impending threat, the Alliance prevents strategic surprises, and supports timely decision-making. By promoting a shared understanding of future challenges and opportunities, the Alliance can influence developing Instability Situations at an early stage, particularly through Strategic Communications.

8-2 Continuous monitoring of the sources of instability will result in the collection of large amounts of data, particularly in areas such as economics and finance, space and cyberspace, energy and water. Gaining an understanding of the physical and virtual flows in these domains allows the Alliance to recognise anomalies at an early stage of development. Increased amounts of information and intelligence will become available to the Alliance through expanded partnerships.

8-3 Due to the increased ability of highly empowered individuals and small groups to threaten security, there will be a continuing focus on intelligence, especially enhanced human intelligence. Information fusion, management and dissemination will be vital, since they are on the critical path of allowing the Alliance to start its decision-making process to exploit possibilities and address threats at an early stage. Sharing this achieved Strategic Awareness within the Alliance and with appropriate partners is a prerequisite for timely decision-making. A comprehensive and long-term understanding of the environment and associated cultures in the Alliance areas of interest should enable NATO to make more informed decisions about appropriate mitigation activities, either in the pre-crisis or subsequent phases of crisis or conflict.

8-4 **Conclusion**: Strategic Awareness leverages new and emerging technologies to collect, process and analyse a vast amount of data. A shared assessment can be gained by fusing this analysis with traditional intelligence in a combined NATO Intelligence Fusion Centre. This shared assessment can

increase cohesion throughout NATO and can be used to create a strategic advantage that will allow improved anticipation of crises and conflicts and expand decision space for senior leaders.

CHAPTER 9 - CONCLUSION

9-1   Strategic Military Perspectives (SMPs) provide six areas of focus for enhancing Alliance forces to address the full range of conventional, hybrid and unconventional threats of the future. The Strategic Foresight Analysis 2013 report described the future as increasingly complex and uncertain, presenting threats and opportunities fuelled by an accelerating rate of social, economic, scientific, technological and environmental change. In preparing to adapt for this future, there are no simple solutions to ensure success for the Alliance. The Strategic Military Perspectives outlined in this document represent broad, guiding principles that can be used throughout the Alliance for future planning. Some of these perspectives may be more evolutionary than revolutionary; indeed, many represent a continuation, with incremental improvements, of activities in which NATO is already engaged. In confronting a complex and uncertain future, however, principles such as resilience, agility, awareness and shaping, facilitated by networking and foresighted policies, will only increase in importance for the Alliance.

9-2   Developing these Strategic Military Perspectives was the second phase in the Framework for Future Alliance Operations effort. In the next phase, domain-specific Military Implications will be developed to inform capability requirements determination within the NATO Defence Planning Process and other future-focused processes. The overall aim remains the same: to provide a coherent long-term perspective that will strengthen the Alliance's ability to plan for the future.

LONG-TERM MILITARY TRANSFORMATION OVERVIEW

1. Long-Term Military Transformation is the Supreme Allied Commander Transformation's process for anticipating and preparing for the ambiguous, complex and rapidly-changing future security environment. This process consists of two parts; the Strategic Foresight Analysis (SFA) and the Framework for Future Alliance Operations (FFAO).

2. The SFA is a trend analysis that describes the long-term aspects of the future security environment. The Strategic Foresight Analysis 2013 Report describes a world in 2030 that will remain complex, uncertain, and increasingly dangerous, presenting threats as well as opportunities, and fuelled by an accelerating rate of social, scientific, technological and environmental changes.

3. The FFAO is currently under development and will describe how the Alliance can prepare for the long-term future security environment. It uses the findings of the SFA and discusses how Alliance forces might transform in anticipation of future. The FFAO will include:

    1) **Instability Situations**: generic descriptions of future events, crises or conflicts that may lead to NATO military involvement.

    2) **Strategic Military Perspectives (SMPs)**: Bi-SC military guiding principles that inform long-term NATO defence planning and other processes, such as concept development, education, training and exercises. Strategic Military Perspectives provide guidance from the Strategic Commanders on the abilities and characteristics that NATO could build upon and can inform the Alliance's transformation efforts.

    3) **Military Implications**: military-specific deductions, derived from the SFA, Instability Situations and SMPs, that may drive change in how the military prepares for and executes operations to accomplish NATO's core tasks.

4. SFA and FFAO inform the decision making process of defence planners and senior leaders as they prepare the Alliance to meet future challenges. Using the trend analysis from the SFA, NATO, national leaders and defence planners can understand the emerging trends that may lead to Instability Situations and possibly require NATO action. Both the SFA and FFAO are iterative and adaptive processes that ACT will update on a four-year cycle in concert with the NDPP to provide an informed Bi-SC perspective of the challenges and opportunities facing the Alliance in the decades to come.

5. SMPs evolved from foundational futures work developed over the past two years. Through this effort, the Strategic Commands collaborated with NATO

headquarters staff, partners, academia, and industry to develop a shared perspective of the common challenges anticipated within the future security environment as derived from an exploration of trends through the Instability Situations.

6. During the Strategic Military Perspectives Workshop, groups of NATO officers and civilians produced ideas for further development and consideration as potential SMPs. Following the Workshop, the ACT team refined, analysed, and expanded upon the Workshop data to arrive at six SMP.

STRATEGIC FORESIGHT ANALYSIS 2013 TRENDS

1. The Strategic Foresight Analysis (SFA) 2013 Report builds upon the principles described in NATO's 2010 Strategic Concept as the basis for ensuring Alliance security in the future. The SFA is based on national and international studies that address the timeframe out to 2030 and beyond. The SFA found the following 15 trends:

    a. **Shift of Global Power**: Rebalance of power from the west to other regions will present political and economic challenges to NATO members.

    b. **Shifting Political Structures**: The transition of autocratic / theocratic regimes towards democracy will continue.

    c. **Polycentric World**: The world is becoming increasingly interconnected and polycentric.

    d. **Changing Demographics:** Future demographics will be driven by diverse effects such as youth bulges, aging populations, and imbalance in proportions of male to females in society.

    e. **Urbanisation**: Cities will contain 65% of the world's population by 2040, and 95% of this urban population growth will occur within developing nations' mega-cities.

    f. **Human Networks / Transparency**: Human networks are expanding at an exponential rate with many varying effects.

    g. **Fractured Identities**: Several contributing factors may lead to a fracturing of national identity.

    h. **Technology Accelerates Change:** The accelerating cycles of exploration, discovery and exploitation of technologies along with the innovative fusion of existing, emerging and new technologies will combine to bring about change rapidly in the future.

    i. **Increased Access to Technology:** Commercial research and technology has begun to outpace that of governments in the development of new technologies.

    j. **Centrality of Computer Networks:** A globally connected and networked world creates a universal availability of information.

k. **Globalisation of Financial Resources:** The financial networks and communication systems that manage the world's critical resources are increasingly intertwined.

l. **Increased Resource Scarcity**: Nations need increasing amounts of energy and raw materials to sustain growth and maintain an advantage in the globalised economy.

m. **Decreasing Defence Expenditures:** Governments faced with slow or non-existent growth, rising unemployment and increasing debt burdens will continue to have many competing priorities.

n. **Environmental / Climate Change**: Global environmental change and its impacts are becoming readily apparent and are projected to increase in the future.

o. **Natural Disasters**: The effects of natural disasters will become more devastating.

INSTABILITY SITUATIONS

1. The Instability Situations cover a broad spectrum of crisis and conflict that NATO could face in 2030, from the low end consisting of large-scale disasters and the disruptive impacts of migration, to the high end of state-versus- state warfare. Below are the ten Bi-SC approved Instability Situations used to develop Strategic Military Perspectives:

   a. **Access and Use of Global Commons Challenged**: substantial increase of threats to global flows, increasing lack of resources and climate change create new contested areas, lines of communication/commerce threatened, access to global commons is threatened.

   b. **Conflict in Euro-Atlantic Region:** expansionism at NATO borders, large-scale insurgency within NATO borders, imbalance of military power, breakdown of a NATO member caused by internal factors or external actors, war-like situation in Europe, NATO alliance weakened or ineffective, imbalance between availability of defence resources and security challenges.

   c. **Disruptive Impact of Migration:** Massive migration causing instability, uncontrolled refugees, displaced persons and economic migration.

   d. **High-Impact Cyber Threat:** large-scale cyber-attack on NATO member or affecting NATO, cyber challenges, cyber warfare, false identity.

   e. **Large-Scale Disaster:** large-scale disaster occurs; opportunistic actors take advantage of chaos, pandemic strikes NATO Nations, natural disasters, weak state challenge, and disaster relief in a world financial centre.

   f. **Megacity Turmoil:** turmoil in a megacity, inability of the nation state to provide security / basic needs in megacities, rising urbanisation and resource competition.

   g. **Non-State Actors Rival State:** attack on critical infrastructure, virtual organisations, climate change, competition in gaining the best security policy/market positions, changes in society which conflict with the national position, decline in existing systems – establishment of new ones, dependence on critical infrastructure, failing/shifting political structures, state versus non-state actors, use of disruptive technology by groups with different mind-sets.

   h. **Space Capability Disruption:** loss of space use, space resilience and vulnerability

i. **State-versus-State Conflict:** spillover of conflict from neighbouring countries along NATO borders, interstate conflict over access to resources, state-on-state conflict including Article V situations, resource wars, frozen conflict, new spheres of influence.

j. **Weapons of Mass Destruction/Effect use/threat:** attack from terrorist groups possessing Weapons of Mass Destruction/Effect (WMD/E) affecting NATO, using WMD/E to create a crisis on the edge of NATO.

COMMON CHALLENGES DERIVED FROM SFA AND THE INSTABILITY SITUATIONS

1. These Common Challenges were derived from an analysis of the Instability Situations during a workshop in Amsterdam, The Netherlands in June 2014.

    a. Empowered non-state actors, including single individuals or groups, are organisations with the ability to influence change within international relations without formal control by an institution of state. These groups may seek to engage NATO by operating around Alliance policy and by eluding international law. Such actors, working by themselves or within collaborations of similarly structured groups, will challenge NATO most critically when functioning as state sponsored proxies. States may use these proxies to avoid the clear legalities of war and peace and to challenge the Alliance in ways that evade NATO's current advantages in conventional military capabilities. These groups may employ a range of activities like kidnapping, smuggling, propaganda, economic and political disruption, as well as a wide range of violent acts intended to create fear in a new, revived and expanded form of asymmetric or hybrid warfare. Such threats may challenge the ability of NATO to achieve consensus on missions. Whether called hybrid threats ambiguous attacks, hybrid warfare or non-linear warfare, these types of threats may find gaps in existing policies delineating Alliance responsibilities. Soft-entry into conflict by a state proxy may decrease NATO awareness at the early stages of a crisis. Legal systems may face a growing number of operations that, because of plausible deniability, are not directly attributable to nation-states.

    b. NATO will be engaged in non-traditional domains outside of territorial defence, such as in the energy, space, cyber, information, and economic domains, where the Alliance may not have the necessary or appropriate capabilities or authority to respond. NATO policies and international legal frameworks in many areas lag behind advances in technology and the rapidly changing security environment (i.e., hybrid warfare, access to global commons, strategic communication, cyber and space operations).

    c. NATO's technological edge will be decreased by the rapid proliferation of sophisticated military capabilities (A2AD, cyber, unmanned systems) and through the innovative use of civilian technologies (e.g., exponential increases in computing power, popular activism via social networking) to achieve military and/or political objectives. These new capabilities and technologies may be available both to

developing nations and to non-state actors, even small groups or single individuals. Examples of the expanded capabilities available to empowered non-state actors include:

- o Greater proliferation of WMD/E will increase the difficulty in preventing their use

- o Area access and denial capabilities will increase in range and lethality.

- o Due to the increased availability of advanced technology to state and non-state actors, NATO use of space assets may be challenged or denied. Space is increasingly likely to be weaponised.

- o Adversaries' ability to disrupt NATO Consultation, Command, and Control (C3) capabilities will increase.

d. The number and variety of crises will increase due to climate change, increasing populations and the resulting strain on infrastructure. Potential adversaries may take advantage of insufficient infrastructure and inadequate security, particularly in the wake of a natural or man-made disaster, to achieve their aims. These actors may be especially effective in filling power vacuums or using chaos created by a disaster to build a powerful narrative or to mask true intentions.

e. Military forces may operate in areas that are already resource limited where the introduction of large numbers of troops will negatively affect the existing balance.

f. Rapid urbanisation across the globe increases the likelihood of operating in urban areas or megacities where complex, three dimensional, terrain will increase the difficulty of military operations by eliminating safe or rear areas and thereby causing forces to maintain a continuous focus in nearly every direction. Most of these urban areas will be located in littoral regions.

g. The rapid flows and increasing volume of information, people, disease, money, drugs, and weapons through the global commons will allow adversaries to move easily from one area to another converging for operations and then dispersing rapidly to evade detection, tracking and targeting. Small groups will benefit from a lack of traceability and anonymity which will be afforded to them by new technologies. They may be able to rapidly emerge, engage, and disappear before Allies can detect a hostile action. The difficulty in engaging these groups, combined with a lack of traditional military targets, may make traditional deterrence ineffective against them.

h. NATO may be confronted by potential operations in which the lines between military, law enforcement and other security organisations are blurred. These various

organisations could have divergent missions and aims that are not identical with those of NATO forces. These other organisations could include private military security companies, used by either NATO or other organisations.

i. Differing threat perceptions and national priorities, in conjunction with the use of sophisticated strategic communications operations conducted by external actors, may open the possibility of fractures developing within the Alliance.

j. The importance of worldwide distributed information, the speed at which information is communicated, the role of social media, and the reliability of information systems have created conditions where Alliance decisions and actions must consider the potential impact on the information environment. This environment has seen significant changes in recent years and will change dramatically in the future due to advances in computing technology.

k. The increased speed of events related to operations may challenge NATO decision making processes, at both the political/strategic and operational/tactical levels.

Examples of Military Implications

STATE VERSUS STATE CONFLICT						
Capability Hierarchy Framework						
Prepare	**Project**	**Engage**	**Sustain**	**Consult, Command and Control**	**Protect**	**Inform**
Adaptive Shaping - Proactively influencing the future security environment to enhance Alliance freedom of action.	Establish key cyber diplomacy concepts to shape opinions and spread information (*R.4*)	Conduct "expeditionary" operations in cyberspace by using strategic communications and social media (*D.3*); Deploy NATO Vulnerability Assessment team for deployment (*D.3*)	Execute selective active cyber defence options (*E.2.6*); Counter/Degrade opponents selective filtering and segmentation efforts (*E.1.X*); Employ operational honeypots (*E.1.X*)	Execute the TPFDD with regards to using cyber assets (virtual/logical, physical, people).	Establish indicators of success (*C.2*)	Release counter-messages to opponent efforts (*P.3*) ; Permit a "DMZ" environment for NATO military networks or to change traffic patterns into requesting nations or forces (*P.3.1.1*)	Release messages to NATO alliance society (*I.4*)
Military Operational Guidance - Establishing predetermined, military specific authorizations, boundaries and guidance that Alliance Forces may require to engage future challenges and exploit opportunities successfully.	Cyber rules-of-engagement that mesh with the concept of Unified Action; Develop TPFDD for using cyber assets (logical, physical) (*R.5.1*); Clarify the roles and responsibilities of operational commanders (*R.7.1*); Instil cyber operations with normal operational battle rhythm (*R.7.2*); Determine which nations will permit cyber operations to be executed from (*R.3.2*); Develop cyber operational level of war capable commanders (*R.1.2*)	Pre-emptively deploy technical sensor, systems, devices, and assets (*D.2.1*)	Permit Operational Commanders to decide if cyber, cognitive, or physical attack is appropriate to meet NAC guidance (*E.3*); Define a time/space/logical dependent (changing) cyber areas of operations where authorities differ from those outside the CAOA (*E.1.X*)				Release guidance to forces; Train forces in the offensive kill chain for cyber so that the defensive protection chain is applied correctly (*I.1, I.3*)
Operational Agility - Providing decision makers more options by making military forces more flexible and responsive**.**	Permanently embedded integrated cyber teams at operational level (*R.5.1*); Develop combined Blue Teams for FMN; Exercises with Operational planning will prepare decisions makers for flexible and proper use of cyber capabilities. (*R1.1, R1.2, R1.4*)	Practice integrated cyber/other warfare domain operations (*D.3*)	Execute integrated cyber/other warfare domain operations (*E.2*); Employ operational tarpits (*E.2.6*); Employ cyber adjunct operations (*E.2*)	Operate multiple watch centres from multiple sites; Deploy cyber assets to reinforce known weak points and possible breaches. (*S1.1, S1.2*)	Develop procedures to optimize rapid decision-making process in responses to developing threats(*C.2, C.3.4*).	When needed, execute use of protected dark sites and pathways (*P.3.2*)	Cyber Intel preparation: Integrate Cyber into normal INTEL cycle. (*I1-4*).
Security Networking - Enhancing Alliance capacity and options through an expanded network of partners.	Develop a tiered cyber security engagement plan for both individual nations and non-state actors (*R.4*); Engage and partner with civil society and specific commercial organizations	Incorporate/execute CD in any project involving ICT or CII (*D.3.4*)	Deploy cyber assets to reinforce known weak points (*E.1.X*)		Inform leadership of residual issues for deliberate integration in sequels, branches, decision-making on RFI/RFF/modifications to ROE, and strategic communications (*C.2, C.3.6*)	Incorporate non-NATO partners (*P.4*)	Release messages to partner nations
Shared Resilience - Ensuring Alliance capacity and options through an expanded network of partners.	Encourage nations that participate in FMN to develop additional capacity that could be provided to a partner when that partner's element of FMN needs to be severed from the network (*R.2.6*); Develop C3 procedures with civilian authorities and private sector entities for crisis response as well as military operations (*R.4.1, R.4.2, R.4.3*); Establishing "Sharing and Pooling" capabilities (R2.6, R3.1)	Help correct vulnerabilities noted by Vulnerability Assessment team; Sharing and Pooling policy utilization (*D3.4*)	Use flexible and complementary means to execute cyber operations within and outside the home nation and/or the 'commons' we operate from	Practice operations in a cyber disadvantaged and unavailable environments	Decision-making based upon residual risk and risk exploitation	When needed, utilize cyber safe zones (via segmentation from the rest of the global network in order to protect people, equipment, or the mission (*P.3*)	Educate partner leadership
Strategic Awareness - Increasing decision-space for senior leaders by providing information on potential sources of instability sooner and in greater detail.	Develop a visual methodology to display complex cyber threats, integrated with real world threat intelligence and operational psychology (*R.2*); Develop evolution models (*R.2.1*); Develop robust understanding of cyber cultural landscape (relationships, tensions, potentials) (*R.2.1*); Define a time/space/logical dependent (changing) cyber area of influence (*R.2.5*)	Automate sharing of threat intelligence needs regarding technical signatures and behaviours, as well as, the actors that employ them (*D.3.4*); Selective "deep-dive" traffic analysis at key nodes	Be able to positively designate CI targets and associated actors as Hostile, Neutral, Unknown or Friendly (*E.1*)			Develop means to verify information and analysis displayed (*P.4.7, P.4.8*)	Educate all warfighters of the principles of the cyber fight and how it applies to unified action

(Left vertical label: Strategic Military Perspectives)

Main new ideas: *(main findings)*

Military Implication Development: Please review the following spreadsheet. Consider the future using your area of expertise. Apply the Strategic Military Perspectives (SMPs) and the Capability Hierarchy Framework (CHF), to evaluate the future needs of the Alliance within the context of each Instability Situation. Enter your answer into the spreadsheet. Answers will be discussed at the upcoming Military Implication workshop in Brussels during November 2014.

Military Implication (Definition): are military-specific deductions that may drive change in how the military prepares for and executes operations to accomplish NATO's core tasks and that inform long-term NATO defence planning, specifically NDPP Step 2. Military Implications identify how NATO can adapt the way it accomplishes its current mission types and may suggest new mission types. Military Implications are derived from Strategic Military Perspectives and informed by both Instability Situations and the Strategic Foresight Analysis trends.

Military Implication Examples: 1) The military must seek to gain advantages associated with the use of mobile devices, but must also understand the vulnerabilities of such devices. The military should also be able to exploit adversaries use of mobile devices. 2) To counter ambiguity, we must improve multi-domain ISR capabilities that identify the weapon – be it kinetic or non-kinetic – and also the perpetrators and their support networks.

Capability Hierarchy Framework Definitions

The Capability Hierarchy Framework (CHF) is comprised of seven broad capability areas. These seven areas were identified through comparison and harmonisation of a broad range of national and multi-national capability hierarchies. These areas are used as a framework by defence planners to support expression of the Minimum Capability Requirements. While this workshop seeks to stay at a strategic level in analysing Instability Situations, the CHF provides a useful starting point to explore different aspects of these situations in the future. The seven areas are as follows:

Prepare: Enhance NATO's effectiveness continuously and prior to operations. Potential areas include Training, Education, Exercising, Planning, Concepts & Doctrine Development, Lessons Learned, Experimentation, Installations, Procurement, Research and Development, standardization, Status of Forces Agreement (SOFA) negotiation and building multinational capacity.

Project: Conduct strategic deployment to project both NATO and national capabilities to a desired Joint Operations Area (JOA) in support of NATO operations in accordance with the Commander's requirements and priorities.

Engage: Engage adversaries, either directly or indirectly, by the application of physical or cognitive effects through the combination of joint manoeuvre and joint fires in conjunction with, where appropriate, other operational capabilities and a range of mechanisms and control measures.

Sustain: Planning and execution of the movement and sustainment of forces. Potentially includes movement and transportation, military engineering support, contracting, supply/maintenance/services management and medical provision.

Consult, Command & Control (C3): Direct Allied forces and HQs for the accomplishment of Alliance missions or tasks.

Protect: Protect personnel, facilities, materiel and activities from any threat and in all situations, to preserve freedom of action and contribute to mission success.

Inform: Support Situational Awareness and the provision of timely, tailored and accurate intelligence.