Foreword

For 66 years NATO’s coherent, consistent and enduring Transformation has enabled its forces to respond to emerging crises whenever tasked to do so. Today it is crucial to keep, and even increase, the pace of NATO’s Transformation as our forces will likely face an increasingly hardened security environment for the foreseeable future. This ambiguous, complex and rapidly changing operational context will likely present significant challenges as well as opportunities.

Therefore, the Strategic Military Perspectives provided by the Framework for Future Alliance Operations (FFAO) FFAO will be instrumental to our continued Transformation. The FFAO is not a prediction, rather, it is a comprehensive analysis that draws upon the lessons of the past, fully informed by the present, and provides a long-term trajectory that should inform our strategic lines of effort with a better understanding of future operational challenges.

Although developed mainly to inform and orient NATO’s Defence Planning Process, FFAO has a potentially much broader application in the development of NATO’s strategic initiatives, including work on hybrid threats, Defence Capability Building, regional partnerships considerations, and Alliance strategic communications, to name only a few. The Nations may also find that FFAO provides insight on those future concepts and trends that should help align national defence planning with that of the Alliance and provide transparency to NATO’s long-term defence planning. Therefore, FFAO will be updated regularly to maintain its relevance and to maximize its utility for political and military leadership.

Finally, the FFAO is a reflection of the collective work of NATO’s futures community of interest. It would not have been possible without the extensive participation and assistance of subject matter experts from across a wide spectrum of professional disciplines. I would like to express my appreciation to the Nations, NATO’s commands, the Centres of Excellence, and headquarters as well as academia and think tanks, who supported this work which is so central to informing our military Transformation to meet the challenges of the future.

General Jean-Paul Paloméros
General, French Air Force
Supreme Allied Commander Transformation
Table of Contents

Executive Summary 5

Introduction 9

Chapter 1 11
The Future Security Environment Towards 2030
And Instability Situations

Chapter 2 15
Strategic Military Perspectives

Operational Agility
Security Networking
Shared Resilience
Strategic Awareness
Strategic Communications

Chapter 3 25
Military Implications

Prepare
Project
Engage
Sustain
C2 (Command and Control)
Protect
Inform

Conclusion 48

Annex A 52
Strategic Foresight Analysis 2013 Trends

Annex B 54
Instability Situations

Annex C 73
Common Challenges Derived From Strategic Foresight
Analysis and the Instability Situations
Executive Summary

1. Long-Term Military Transformation (LTMT) is Allied Command Transformation’s (ACT) process for anticipating and preparing for the ambiguous, complex and rapidly-changing future security environment. The first component of LTMT, the Strategic Foresight Analysis (SFA) 2013, provides a trend analysis, based on national and international studies, describing the long-term aspects of the likely future security environment in 2030. The second component, the Framework for Future Alliance Operations (FFAO) which uses the SFA 2013 report as a foundation, proposes how Alliance forces might transform and recommends abilities that the Alliance may need to develop over the next 15 years to be successful in the future security environment of 2030 and beyond. FFAO is intended to directly inform all steps of the NATO Defence Planning Process (NDPP). FFAO will also inform other transformation and defence planning efforts.

2. Allied Command Transformation collaborated with Allied Command Operations and the Member and Partner Nations, NATO staff, academia, and industry to develop a shared perspective of the future security environment. LTMT products provide this long-range perspective and are intended to inform senior leaders and defence planners as they prepare the Alliance to address future challenges and opportunities. Allied Command Transformation will update SFA and FFAO on a four-year cycle in concert with the NDPP.

3. SFA 2013 identifies a complex future for the Alliance. It is a future with risk and uncertainty, threats and opportunities, which will be fuelled by rapid social, scientific, technological and environmental change, and exacerbated by the pervasive effects of globalisation. To prepare for this complex future, the FFAO supports the three Core Tasks assigned in the 2010 Strategic Concept and plans for the current Level of Ambition into the future security environment of 2030. FFAO is divided into three sections: Instability Situations, Strategic Military Perspectives and Military Implications.

4. The ten Instability Situations, which are all equal in terms of importance and which are not listed in any order of priority, identify the following future events, crises or conflicts that NATO may face in 2030:

   - Access to and use of the Global Commons Challenged
   - Conflict in the Euro-Atlantic Region
   - Disruptive Impact of Mass Migration
• High-Impact Cyber Threat
• Large-Scale Disaster
• Mega-city Turmoil
• Non-State Actors Rival State
• Space Capability Disruption
• State-versus-State Conflict
• Weapons of Mass Destruction/Effect/Use/Threat

5. The five Strategic Military Perspectives provide broad military guiding principles that may be used to inform the NDPP, especially the Political Guidance, and other transformation processes:

• Operational Agility: Making military forces more flexible, adaptable, and responsive.

• Security Networking: Increasing capacities, opportunities, and influence by expanding partnerships.

• Shared Resilience: The ability to retain credible forces and conduct successful operations in spite of surprise or strategic shock.

• Strategic Awareness: Providing military leaders with a more comprehensive and precise understanding of the situation, available courses of action, and likely risks and threats to enable timely and accurate decision making.

• Strategic Communications: Developing, coordinating, and disseminating an Alliance narrative that sets the conditions for success.

6. The Military Implications are best military advice expressed as abilities, to inform Alliance transformation, including development of policies, long-term requirements, and capabilities. Military Implications are not defined requirements, nor are they expressed as required capabilities. They provide military-specific deductions, expressed as abilities, which NATO may require to accomplish its core tasks in the future. Derived from SFA 2013, Instability Situations and Strategic Military Perspectives, these deductions are categorised under seven key headings: Prepare, Project, Engage, Sustain, C2 (Command and Control), Protect, and Inform. Military
Implications are recommendations based on efficiencies in scale, effects, performance and cost. The key deductions are as follows:

- NATO technological superiority and access will be challenged. Access to the global commons and to areas of operations will be contested by anti-access and area denial methods, CBRN threats, and new technological advancements. The Alliance will need to develop abilities to gain and maintain access, and counter a wide range of proliferating threats posed by the rising capabilities of potential adversaries.

- Technology will increasingly provide both challenges and opportunities. The Alliance will be challenged by actors with access to sophisticated off-the-shelf technology. Private investment in research and development will continue to outstrip state funding, and innovative products will be available to all. Access to future technologies may enable some actors to achieve technological parity with NATO in certain fields, and allow non-state actors to rival states. However, rapid advances in technology could also revolutionise Alliance operations. Taking into account moral and ethical considerations, Member Nations can improve the efficiency and effectiveness of their capabilities while reducing the cost of modernisation through the flexible acquisition of new technologies. Improved manned and unmanned systems will reduce risk and the possibility of loss of life. Furthermore, a mixture of low and high-tech systems can improve resilience through the diversification of NATO systems. New tactics, including swarms of unmanned systems, have the potential to enable the Alliance to spontaneously mass on the battlefield while reducing operational risk.

- Future Alliance forces will need to increase their operational agility by being modular, scalable and trained for a wider variety of missions using innovative tactics. Flatter organisational structures and mission-command may be required to address complex and changing future threats. Future command and control will need to enable collaborative planning and decision-making, while ensuring connectivity of dispersed forces to the chain of command. NATO forces can be better sustained through streamlined logistics. Future technologies may enable the reduction of logistic footprints and improve the responsiveness of the supply chain.

- Increased urbanisation makes NATO operations in an urban environment more likely. NATO forces will need to understand, train for, and operate in complex urban environments with mass populations that are networked and mobile. NATO may also need to support civil authorities who become
overwhelmed in a crisis. This may necessitate the provision of key services so as to deny an adversary the opportunity to exploit a chaotic situation.

- New technologies and a dynamic environment will challenge traditional information and intelligence systems. NATO forces will need to be able to mine and analyse vast quantities of data to produce and share actionable intelligence, improve situational awareness, and support decision-making. While not necessarily owning data, NATO will need access to it, along with the ability to share information with an increasing number of actors and partners.

- The Alliance will continue to use cyberspace to facilitate communications and command and control. However, cyberspace will increasingly be threatened, and the Alliance will need to maintain access to resilient and robust cyber systems hardened against attack and develop alternative systems that are impervious or less vulnerable to cyber-attack. NATO must be able to generate a recognised cyber picture.

- Strategic Communications supports Alliance policies and operations and contributes positively and directly to the successful implementation of NATO military operations, missions, and activities by aligning words and actions. By placing information and communication at the heart of all levels of policy, planning and implementation, and ensuring they are a fully integrated part of the overall effort, Strategic Communications can make a major contribution to Alliance success.

7. The FFAO provides the Strategic Commanders’ best military advice concerning the long-term future and seeks to inform NATO’s transformation and defence planning efforts. The Instability Situations and Strategic Military Perspectives provide the context and general characteristics of future Alliance military forces that the Strategic Commanders deem necessary for future success. They are particularly useful for focus areas, scenario development, force modelling, capability development and discussion of proposed national targets. The Military Implications provide specific recommendations for defence planners to help focus long-term capability development activities and military planning. Finally, many nations may find the results of the SFA and FFAO and participation in ACT’s Long-Term Military Transformation process useful for national defence planning. FFAO provides a start point for discussion of the future perspectives and requisite abilities to help nations best determine how to participate in NATO’s long-term transformation efforts.
Introduction

Aim

1. The aim of the FFAO is to outline how Alliance forces might transform over the next 15 years and propose abilities that NATO may need to develop to be successful in the future security environment of 2030 and beyond.

Background

2. LTMT is ACT’s process for anticipating and preparing for the ambiguous, complex and rapidly-changing future security environment of 2030 and beyond. The LTMT consists of two parts. The SFA 2013, provides a trend analysis and describes the long-term aspects of the likely future security environment in 2030 based on national and international studies. Using the SFA 2013 report as its foundation, the second component, the FFAO, proposes how Alliance forces might transform and recommends abilities that the Alliance may need to develop over the next 15 years to be successful in the future security environment of 2030. FFAO is intended to directly inform all steps of the NATO Defence Planning Process (NDPP). FFAO will also inform other transformation and defence planning efforts.

3. SFA 2013 outlines a complex future security environment for the Alliance. It is a future security environment characterised by risk and uncertainty, challenges as well as opportunities that will be fuelled by rapid social, scientific, technological, and environmental change with the pervasive effects of globalisation.

Scope

4. Together SFA and FFAO products provide a shared perspective of the common challenges and opportunities anticipated within the future security environment. The products are intended to inform senior leaders and defence planners as they prepare the Alliance to meet future challenges and exploit opportunities. FFAO may be used by nations for long-term defence planning and, therefore, may assist in improving the cohesion of the Alliance.

5. Both the SFA and FFAO are iterative and adaptive documents that ACT will update on a four-year cycle in concert with the NDPP to provide an informed perspective of the challenges and opportunities facing the Alliance in the decades to come.
Method

6. Using the SFA 2013 as its foundation, FFAO is based on the outcomes of a series of ACT-led workshops, where experts from ACO and ACT, Member Nations, Centres of Excellence, Partner Nations, provided their input. ACT and ACO collected, refined, and elaborated this input in the format of the following three sections: Instability Situations, Strategic Military Perspectives and Military Implications.

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

   b. Strategic Military Perspectives: broad military guiding principles that inform long-term NATO defence planning and other processes, such as concept development, education, training and exercises. Strategic Military Perspectives identify the abilities and characteristics that NATO could build upon to prepare for the future.

   c. Military Implications: military-specific deductions, expressed as abilities that NATO may require to accomplish its core tasks in the future.

7. The Strategic Military Perspectives and the Military Implications provide the guiding military principles and military-specific deductions to help the Alliance transform to meet future challenges and exploit opportunities, and may be considered as inputs which inform defence planning. Both SFA and FFAO should be read in conjunction to ensure a broad understanding of their substance and potential application.
Chapter 1

The Future Security Environment towards 2030 and Instability Situations

1. As SFA 2013 identified that the future will be increasingly complex and uncertain, thereby presenting challenges as well as opportunities which are fuelled by a rapid rate of social, economic, scientific, technological and environmental change.

2. NATO may face adversaries consisting of states as well as non-state actors, that will work independently or in concert to challenge the Alliance in ways that complicate consensus response. Adversarial states may 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. NATO’s adversaries may not accept internationally established borders, treaties, rules of law or norms of behaviour. They may increase their use of asymmetric or irregular forms of warfare to counter NATO’s military superiority. Some states or non-state actors may seek to combine different forms of warfare – conventional, irregular and cyber warfare – and possibly, large scale terrorism including hostage taking. They may try to deny the Alliance clear, legitimate courses of action and identified targets and may seek to increase the ambiguity on the battlefield, posing the problem of indubitable attribution that is currently experienced in cyberspace. This hybrid and ambiguous model might complicate NATO’s
consensus, strategy and defence planning as it blurs the boundaries between conventional approaches of power.

3. 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. Future threats will seek to operate in the “grey areas” or “seams” of the Alliance. Future opponents could also seek to strike the Alliance within its own borders, in such a way as to limit the adequate use of Alliance forces and even the legitimacy to employ force.

4. Adversaries will seek to attack Alliance cohesiveness and seek to engage NATO in innovative ways that magnify possible divisions within the Alliance. Furthermore, the speed and pervasive nature of the flows of people, data, disease, money, drugs and weapons through the global commons and elsewhere allows state and non-state actors to move easily from one area to another converging for operations and then dispersing rapidly to evade detection and engagement. Future opponents will increase their capabilities and aim to impede NATO’s actions. They may be able to exchange and share lessons learned and techniques, using modern information technology and extensive strategic communication. They will be empowered by access to technologically advanced weapons dual use of technologies. As a consequence, environments will likely become less permissive. NATO’s ability to ensure first entry in a high intensity operational area may therefore be challenged as anti-access and area denial capabilities continue to spread. NATO’s adversaries may seek to increase the lethality and diversity of threats in the area of operations to step up Alliance dependency on force protection and affect Nations’ perceptions of risk and therefore our public opinion and political will to intervene.

5. While NATO is strong in conventional capabilities and prepared for traditional territorial conflict, the Alliance will also likely face states employing non-state proxies and using hybrid means to achieve objectives. Alongside conventional warfare, future threats are likely to combine special operations and irregular forces (including mercenaries, terrorists and criminal organisations as well as offensive cyber and space activities). Dedicated adversary psychological operations will exploit social and traditional media to win the battle of the narrative. As a result of access to an increasing range of new capabilities and technologies, future adversaries may achieve qualitative parity or symmetric advantage in some domains and will, therefore, pose a greater threat to the Alliance. NATO’s ability to plan and prepare for possible
contingencies may be challenged. Crisis could develop so swiftly that there would be insufficient time for traditional decision making processes to allow response in a timely manner.

6. Following in depth analysis of the trends contained in the SFA 2013, Phase 1 of FFAO developed ten Instability Situations, or generic descriptions of possible future events across a broad spectrum of crises or conflicts that NATO may have to face between now and 2030. The Instability Situations range from large-scale disasters and the disruptive impacts of migration, to state-versus-state warfare and give defence planners scenarios that are most likely to lead to NATO involvement in the future. They are all equal in terms of importance and are not listed in any order of priority:

   a. Access and Use of Global Commons: Alliance access to and use of the Global Commons challenged. Substantial increase of threats to global flows. Increasing lack of resources and climate change creating new contested areas, threatening lines of communication/commerce and limiting access to global commons.

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

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

   d. High-Impact Cyber Threat: A large-scale cyber-attack on a NATO member or affecting the Alliance, cyber challenges, cyber warfare and use of false identities.

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

   f. Mega-city Turmoil: Turmoil in a mega-city, the 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 mindsets.

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

i. State-versus-State Conflict: Spill over 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.
CHAPTER 2

Strategic Military Perspectives

1. Collective Defence, the raison d’être for the NATO Alliance, demands military forces that can defend against the hybrid blending of conventional and unconventional threats. Successful execution of collective defence will require NATO Nations to address a wider range of threats that operate in combination and across all domains. Whilst continuing to prepare forces for traditional territorial conflict by maintaining strong conventional and nuclear capabilities, Alliance forces may also need to improve their ability to deter and defeat a growing range of non-traditional threats. These threats will include states that employ non-state proxies and use hybrid means to achieve objectives.

2. SMPs provide five focus areas for enhancing Alliance forces to address the full range of future threats across all the core tasks. These perspectives constitute military advice from the Strategic Commanders that provides guiding principles and a common direction of travel to prepare the elaboration of the Military Implications. The SMPs are:

   a. Operational Agility: Making military forces more flexible, adaptable, and responsive will provide more options to Alliance leaders.

   b. Security Networking: Increasing capacities, opportunities, and influence within the security environment by expanding the number and type of partnerships and through continuous partner interaction.

   c. Shared Resilience: The ability to retain credible forces and conduct successful operations in spite of surprise or strategic shock.

   d. Strategic Awareness: Providing military leaders with a more comprehensive and precise understanding of the situation, available courses of action, and likely risks and threats to enable timely and accurate decision making.

   e. Strategic Communications: Developing, coordinating, and disseminating an Alliance narrative that sets the conditions for the success of its military operations and activities, and enhances their positive effects through the information domain, and countering adversary narratives coming through fabrication and deception.
Operational Agility

3. 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 using new and ever-changing methods to achieve their aims. Operational Agility preserves decision space and leads to multiple creative and scalable options for decision makers.

4. Adjusting complex operations effectively demands military leaders who demonstrate creativity while developing solutions to highly complex 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 advantages that maximise strategic options. Operational Agility also requires timely decision-making by military 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. 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. NATO 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 large networked urban areas or megacities.

6. To maximise combinations of Alliance power, NATO should enhance the ability to assemble and train diverse multinational units. Recognizing that challenges will adapt to initial responses, the Alliance should be able to bring together a mix of appropriate forces and capabilities quickly, for example security forces that can anticipate and counter interruptions within any domain.

7. 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 helps focus Defence Planning on the development of flexible units and creative leaders comfortable in situations that are characterised by ambiguity, complexity and rapid change.

**Security Networking**

8. 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 holistically and includes the ability to influence the security environment through continuous interaction via physical and virtual presence. Security Networking suggests cooperative, persuasive and proactive engagement with organisations and actors, both inside and outside of the Alliance, enabling NATO to anticipate crises as well as leverage a wider range of capabilities. NATO should strive to work with others to address security in a more comprehensive manner while maintaining responsibility for Alliance security. Such partnerships can be temporary or enduring and could include a range of law enforcement, intelligence, and non-governmental organisations.

9. Security Networking merges, coordinates, and builds upon ongoing NATO activities to anticipate and counter a diversified range of potential threats coming from a larger number of state and non-state actors. Before a crisis occurs, the Alliance could establish relationships with a range of partners who could work together to achieve mutual objectives. These actors may provide a variety of services like police and medical training, electrical power, water, or governing capacities and would act best in a complementary way that avoids duplication and maximises efficiency,
effectiveness, and affordability. Although Alliance interests are not always in complete alignment with other partners, NATO may consider playing a role as an enabler or facilitator in activities or operations by using assets to coordinate and assist participating actors. This coordination and cooperation might best be implemented from tactical through strategic levels to build a common view of the situation.

10. Viewing 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. New networking relationships also require expanded strategic communication roles. In this way, security networking supports the level of ambition by aligning tactical, operational, and strategic narratives from across a wide range of actors.

11. 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 may be variable in length and depth of commitment, allowing NATO to benefit from numerous temporary partnerships for specific aims without overcommitting the Alliance. Security Networking will help NATO shape the security environment by expanding both a network of partners and the set of activities to counter a broader range of potential threats. Through Security Networking, the Alliance will contribute to coordinating and merging 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.

**Shared Resilience**

12. 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, systems and processes necessary to provide NATO with a constant capability to analyse and manage information throughout a crisis despite potential interruption.

13. In the increasingly complex environment of the future, threats will be less foreseeable. Alliance planning should guard against the effects of complexity, surprise or strategic shock that might hamper 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 for shared resilience, 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 of shared risk among Alliance members and their partners, will be important to achieving this coordinated effort.

14. 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, through local contracting, on site manufacturing, and host nation support.

15. To achieve Shared Resilience, Alliance leaders must seek backups to critical systems wherever possible. However, Shared Resilience is more than redundancy, it is 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.
Strategic Awareness

16. 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 and other non-state actors 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.

17. 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.

18. 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. Mastering technologically in the collection and analysis of large quantities of information is key to Strategic Awareness. 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.

19. 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.
Strategic Communications

20. Strategic Communications supports Alliance policies and operations and contributes positively and directly to the successful implementation of NATO military operations, missions, and activities by aligning words and actions and ensuring they are understood. By placing information and communication aspects at the heart of all levels of policy, planning and implementation, and ensuring they are a fully integrated part of the overall effort, Strategic Communications can make a major contribution to Alliance success. Strategic Communications is the coordinated use of Public Diplomacy, Public Affairs, Military Public Affairs, Information Operations, and Psychological Operations coordinated across commands at all levels, which in concert with other military actions and following NATO political guidance, advances NATO’s aims and operations. In a networked world capable of employing unconventional and hybrid methods and empowered with the ability to drive the narrative within a continuous and global news cycle, the Alliance will need to enhance the speed, connectivity, and effectiveness of Strategic Communications. The proper use of Strategic Communications will help the Alliance to build lasting and close coordination and cooperation with NATO Nations, Non-NATO entities, International/Non-governmental Organisations, and the public by enhancing their awareness, understanding, and support.

21. By placing Strategic Communications considerations within policy, planning and implementation, NATO can proactively influence the security environment through a coordinated narrative that sets and then sustains the conditions for the success of military operations. Strategic Communications should be deliberate and continuous, firmly aligned with the overall strategy and characterised by accuracy, clarity and
conviction. Messaging and themes and the methods used should remain flexible enough to communicate to a range of internal and external audiences to ensure an accurate understanding of and support for Alliance actions and intentions.

22. Communicating NATO’s narrative via traditional and social media for reassurance, support-building and deterrence purposes can have a powerful, positive impact on stability. In developing and implementing a strategic narrative that promotes Alliance positions and policies NATO should establish communication and engagement goals, identify and understand relevant audiences, and provide clear content that resonates with its audiences. Given the long-term nature of many of our tasks NATO Strategic Communications should be sustained and consistent. When applied to potential hybrid threats, Strategic Communications becomes an even more vital part of the permanent task to prepare for counter and deter threats, and will remain a vital component of the comprehensive approach.

23. Future challenges to NATO will include both conventional and unconventional threats, hybrid warfare methods, and influential non-state actors, all striving to shape the information sphere, influencing public perception, slowing and disrupting political decision-making and undermining the credibility of the Alliance. It will be important for the Alliance to monitor and analyse adversarial messaging and narratives in order to contribute to the early network of indications and warning to help recognise, characterise and attribute an emerging hybrid threat. An adversary’s message may be sophisticated and nuanced to address the target audience in each respective nation, or organization but by rapidly assessing an adversary’s narrative, NATO may be able to get ahead and take the initiative.

24. The complexity in the ways and means of modern communication makes the analytical task even more challenging. Aspects of monitoring are likely to exist, but occur across a range of connected agencies and organisations, both state-owned and private sector. Information sharing will be a critical enabler as part of this wider security network, and will challenge established working practices. Strategic Communications should integrate analytical capabilities to support proactive permanent messaging, and to counter the adversary’s false messaging, propaganda, and strategic message across all media including traditional and social.

25. Strategic Communications will be central to sustaining and as necessary improving Alliance cohesion and its ability to assure Member and Partner Nations, other coalition partners, and other audiences, while likewise deterring threats and warning adversaries, especially in the context of hybrid warfare. Future security will require a real-time analysis of the competing narratives and adversarial messaging, particularly during the early stages of a crisis, in order to produce and deliver a credible message.
to support the Alliance policy, including its military operations. Strategic Communication should be integrated into Alliance planning, policy and implementation, and NATO needs to have the right structures, resources and policies to enable it to compete in the modern information environment.
Chapter 3

Military Implications

1. The final phase of the FFAO, the Military Implications, provides military-specific deductions, expressed as abilities that NATO may require to accomplish its core tasks in the future.

2. Military Implications translate the Strategic Military Perspectives into strategic, operational, and tactical detail. Military Implications are not defined requirements, nor are they expressed as required capabilities. Military Implications are best military advice expressed as abilities, intended to inform Alliance transformation, including the development of policies, long-term requirements, and capabilities. Alliance and Member Nations may take into account these long-term abilities during planning. Recommendations are based on efficiencies in scale, effects, performance and cost.

3. The Alliance developed Military Implications by domain and they are presented under the following key headings: Prepare; Project; Engage; Sustain; Command and Control (C2); Protect; Inform.

Prepare

4. Cooperation with Security Partners: In order to counter the full range of threats and be successful in the future security environment, the ability of forces to operate with a wide range of partners (both official Partner Nations and unofficial partnerships) will be critical. Forces from Partner Nations will continue to require necessary levels of interoperability with NATO. This should be facilitated through Partners’ adoption of NATO policies, doctrine, tactics, techniques, and procedures, and collaborative planning, training, exercises, education, and standardisation. Formal NATO Partnerships with nations and governmental organisations will continue to be based on established frameworks. NATO’s engagement with other partners will be facilitated through regular dialogue and could be agreed on an ad hoc basis.

5. Comprehensive Approach to Military Operations: To avoid duplication of effort, where advantageous and in accordance with the Alliance policy, NATO should endeavour to synchronise efforts with partners, other international organisations, other nations’ armed forces, state agencies and non-governmental organisations. The Alliance should also exploit the full potential of relationships with a range of relevant actors that can influence future operations, despite the fact that other actors may have different motivations and goals. Relationships should be forged with a wide range of
experts from across academia, industry, international aid, law enforcement and others.

6. Scalable and Modular Units and Organisations: NATO forces will need to prepare for a wide range of contingencies and offer maximum agility at the appropriate level of readiness. Future forces need the ability to rapidly adjust in scale and capability. Modular, flexible forces that can be tailored to specific missions may increasingly be required. Such forces should be capable of deployment and sustainment on missions across a wide range of environments and should be capable of operating at small scale, rapidly building to larger scale with the necessary capabilities when required.

7. Creative Use of Human Resources: To optimise interoperability and enable forces to adapt to a broad range of operational environments, personnel should increasingly be trained to build trust with stakeholders, share information and be culturally aware. Allied forces would also benefit from being able to rapidly incorporate reservists within their numbers as a primary means of adding strength, diversity, and resilience. This would also make use of the expertise reservists bring from their civilian employment in many areas, including government, medicine, law enforcement, education and other specialisations. NATO personnel with a secondary skill might be cross-trained to perform additional tasks without reducing the individual expertise and proficiency within a primary occupational skill or set of critical abilities.
8. Training and Exercises: Major NATO exercises that demonstrate capability and resolve across all domains will remain important. To facilitate training in all areas, reduce cost and environmental impact, and improve realism, training scenarios should continue to be enhanced by simulation and modelling. Training should increasingly leverage emerging technologies that accurately replicate environmental conditions including human behaviours and cultural context. To create operationally agile units, Allied and Partner forces will need to train for the most demanding operations and be prepared for diverse threats including hybrid, cyber, (T)BMD, anti-access, area denial, nuclear, radiological, biological, and chemical. Forces will need to be trained in joint intelligence, surveillance and reconnaissance, strategic communications and full-spectrum targeting, including social-media. Minimising the unintended consequences of operations on local non-combatants and their critical infrastructure requires specific training. This training is best when enhanced by local expertise, cultural advisors and their regional civilian and military counterparts. Forces will need to be trained to operate autonomously in order to overcome the loss of critical systems, such as global positioning systems, and communications, command and control systems. NATO will also need to prepare its forces, including special operations forces (SOF), to counter conventional and unconventional warfare and state as well as non-state actors by continuing to develop policies, rules of engagement, education, training, and equipment. A balance of live and simulation training will be required to provide realistic training in all areas. NATO should also explore options to further strengthen educational efforts in a multinational context.

9. Best Practices: The ability to test and quickly incorporate innovative best practices into Alliance operations will be important. A multi-domain network should be developed and maintained connecting basic tactical units to operational level leadership, to enable collaborative planning, create synchronised effects, and facilitate the timely exchange of tactics, techniques, procedures, and best practices. Forces will need to ensure the latest doctrine is incorporated within any tactics, techniques, and procedures databases. Near real time analysis of NATO operations and lessons learned will also be key, as well as the conduct of experiments that include new challenges such as autonomous systems and cyber, hybrid and space warfare.

10. Mission Command: The future security environment will be characterised by rapidly changing situations that are fluid and dynamic and which may require decentralised execution, the application of a mission command mindset, and flattened command structures where appropriate. The Alliance will require a decision-making cycle that works faster than our potential adversaries’, and might deliberately choose command and control relationships that maximise operational efficiency. A mission command culture often improves resilience by enabling forces to perform the correct actions that lead to mission accomplishment when a centralised command system is
not optimal. To accomplish this, forces should establish enduring relationships that will allow commanders to issue mission command style orders that convey intent, in keeping with political direction.

11. Leader Development: Future operations will increasingly require military leaders with greater political, technological, cultural and sociological awareness in order to better identify and mitigate risk while capitalising on opportunities. Future military forces will need to foster a culture of technological awareness where its people seek to understand technology and its impact on operations. Military leaders should be educated and trained in new technologies and capabilities, including autonomous and robotic machines, big data, cyber, and space systems. They should be taught to integrate technology into operations and contribute to the development of new concepts, doctrine and legal frameworks. Military personnel should continue to improve cultural understanding and language skills and train to develop specific regional expertise when necessary. Units should maintain adequate English language proficiency to ensure an ability to communicate clearly across the joint force.

12. Human Factors: Future technology will allow the human body to be fused with technology to enhance physical and cognitive performance. Training and technological solutions may be developed to mitigate the human limitations on operations resulting from lack of sleep, high stress, and high workloads. Many of these technologies will be available to both military and civilian users, including non-state actors, and may present a variety of challenges to NATO forces. While some of these innovations will undoubtedly cause significant ethical debate, NATO should not discount the possibility that these technologies will manifest themselves in the operating environment and forces will therefore have to train for them. Furthermore, some Member Nations may desire to improve their personnel through human enhancement, and these decisions will have policy and interoperability implications for the Alliance. While it is difficult to forecast many of the human enhancement technologies currently under development, it is plausible that human modifications could include medication, implants, computer aided cognition and decision-making, and enhanced training.

13. Urban Operations Training: Increased urbanisation will make urban operations more likely. Forces should train to operate in densely populated areas. Urban operations will require NATO forces to understand force restraint, apply proportional response and be proficient with non-lethal means. Training should include close human interaction, and interface with large distressed populations. Forces should be prepared to understand crowd mobilisation and conduct crowd control to cope with large movements and concentrations of people including refugees and armed civilians. Forces might also consider training capabilities and exercise scenarios
designed to reinforce Nations’ and partners’ ability to establish humanitarian assistance and effective quarantine measures in the event of pandemic. Such situations may overstretch local civilian police and impact on operations. Member Nations’ military police might develop an ability to adopt a constabulary and forensic role, for use in support of local civilian police, when requested.

14. Integrated Cyber Operations, Planning, Exercises and Training: Cyber activity will significantly impact the future operating environment. Forces will need to fully integrate defensive cyber operations with all other Alliance operations. They should also be able to share critical information on cyber threats and cyber best practices. Military personnel should be educated in cyber-security and modern communication threats and opportunities. Cyber defence should become a partner capacity building task. Forces should train and certify cyber experts to gain an enhanced understanding of emerging technologies and new areas of cyberspace. When required, military leaders should request adaptations of cyber policy, including Standing Operating Procedures.

15. ROE/Military Authorities: Forces should ensure that leaders are provided with sufficient guidance and rules of engagement to prepare them to act within their designated authorities. Authorities and jurisdictions should be clearly defined so that leaders are able to make sound decisions rapidly.

16. Acquisitions and Procurement: While it will remain a national responsibility to train and equip national forces prior to their assignment as part of a NATO force, the Alliance must continue to coordinate closely with Member Nations to ensure assigned forces meet operational requirements and have the necessary capabilities to perform all NATO’s core tasks. The capacity for collective defence should be the centre of the Alliance’s military capabilities.

To meet evolving threats and succeed in the future security environment, Member Nations will need to keep their procurement processes flexible, in close consultation with industry and in step with technology, to provide forces that can rapidly surge in size or adjust in capability. A combination of collaborative programs and advances in technology should be exploited for their potential to shorten acquisition cycles, reduce cost and provide greater economies of scale, while enhancing effectiveness and performance.

**Project**

17. Mounting: Alliance forces will continue to need to project operationally agile joint forces capable of conducting full spectrum operations across all core tasks of the
Alliance. NATO forces will need to maintain access to, and use of land, sea, air and space. They will need to mount and project joint forces at range onto land, to gain lodgements where necessary, by means of a broad array of theatre entry options including forcible entry, particularly in the urban littoral. NATO forces should be able to operate across all domains and succeed in hostile anti-access and area denial environments.

18. Deployment and Redeployment: To rapidly deploy, sustain and redeploy credible joint forces where needed, NATO should be able to guarantee access to sufficient and resilient air and sea lift. Forces will need the capability to project physical presence into an area of operations and to rapidly project advance force and force liaison capabilities. When Member Nations choose to deploy civilian response teams, forces should leverage civilian expertise and seek mutually beneficial areas upon which to cooperate. NATO forces and civilian response teams will often need to cooperate with local national authorities in areas where traditional military forces do not have knowledge, proficiency or jurisdiction such as energy production, waste management, finance, education, and public administration.

19. Reception and Staging: Both on NATO territory and during expeditionary operations, the Alliance should continue to plan and provide reception, staging, and onward movement and integration facilities in concert with host nations to support the timely transition of deploying forces (personnel, equipment and material). Member Nations should frequently update their reception and staging plans in order to accommodate changes to force structures and equipment.
20. Basing: To guarantee operational agility and shared resilience, NATO and Allies should be able to maintain a sufficient network of bases and logistic support facilities on NATO territory, and establish expeditionary ports and airfields in remote locations. Forces should be able to rapidly repair ports and airfields if damaged and return them to operational status.

Engage

21. Joint Manoeuvre: NATO forces should continue to improve their ability to manoeuvre jointly to gain positional advantage over the adversary. Force can then be threatened or applied, thus rendering adversaries incapable of resisting effectively throughout all dimensions of the operational area by shattering cohesion rather than destroying components through incremental attrition.

a. Enhanced Manoeuvrability: NATO forces should be able to maintain access to the global commons and to conduct the full range of operations where needed. Forces should be mobile and able to operate across all domains, in different terrains including arctic, littoral, and urban, and in the global commons, at the lowest possible military organisational level. Future Allied operations may be geographically dispersed within an area of operation, and may require the ability to influence larger geographical areas with minimal personnel and equipment. Such distributed operations will require enhanced manoeuvrability including engineering support, tactical air transport assets, long range communications, and agile logistical support.
b. Cyber Manoeuvrability: Forces should be able to maintain freedom of action and influence in all areas of cyberspace, to include new and emerging areas. Forces rely on cyberspace for communications and intelligence gathering and in many cases cyberspace may be the primary communications link.

c. Rapid Response: NATO SOF should maintain and improve the ability to quickly project forces to uncertain or contested environments with low visibility and small footprints.

22. Joint Fires: NATO forces should continue to improve the coordinated and efficient application of both lethal and/or non-lethal joint firepower to deny, degrade and destroy adversary forces, facilities and infrastructure throughout the operational area thus enabling decisive manoeuvre whilst avoiding unwanted collateral effects.

a. Enhanced Firepower: Whilst forces should maintain a broad range of conventional weapons, new technologies and threats will require them to enhance their firepower. This should be realised using Precision Guided Munitions with alternate (non-satellite) navigation capability beyond GPS, and long-range strike capability. Where possible, NATO forces should continue to field standardised munitions that can be employed from different national platforms and systems. To counter financial constraints, Member Nations should exploit lower cost-per-shot novel weapons such as directed energy.

b. Kinetic operations in urban areas require forces to use accurate and efficient joint strike capabilities in urban terrain with minimum possible collateral damage. Allied numerical inferiority can be mitigated through the accurate delivery of fires in close coordination with friendly forces, delivering the desired effects at the proper time and place.

c. NATO forces should maintain a persistent and networked strike capability to identify targets with precision, assess potential collateral damage and engage them accurately. Where possible, forces should employ scalable and multi-role weapons to cover a broad range of mission-types. The ability to vary weapon-yield post launch, to change effects from non-lethal through kinetic and to change targets in flight may be required. Following a strike, forces should improve their ability to conduct precise and timely Battle Damage Assessment to support follow-on operations.

d. Allied operations will remain heavily dependent on the electromagnetic spectrum and NATO forces should maintain freedom of action there. Advanced
electromagnetic protection, electromagnetic support and electromagnetic attack may be required.

e. Engagement with Unmanned and Autonomous Systems: The Alliance may consider increasing investment in new technologies to improve its engagement capabilities in these systems. Innovations in unmanned systems and swarm tactics may allow forces to increase the number of air, land, sea, and space systems and allow NATO to mass force while reducing financial costs and risk to life. Autonomous systems should be exploited as a force multiplier.

23. Joint Influence: Because influence is achieved through words and actions, NATO must better coordinate its communication activities across the Alliance. This requires the development and implementation of a political and military process to create NAC-approved communication strategies and narratives that can inform national narratives and guide NATO's message to support cohesion, consistency and unity of effort. Mission success depends to a large extent on how Alliance activities are perceived by different actors. Integrated and synchronised information activities create effects on perceptions, and thus shape opinions and decision making. Forces should gain and maintain public support by communicating timely and credible information to key audiences, while influencing approved audiences and adversaries and conducting counter propaganda activities. Forces need to better integrate all specialised communication functions (Strategic Communications, Public Diplomacy, Public Affairs, Military Public Affairs, Information Operations, and Psychological Operations) in order to maintain credibility, and to maximise the desired effects in the information environment.

a. Cyber Influence: Activities in cyberspace are conducted in a virtual domain that is largely unseen. These activities require a deliberate and well-planned communications strategy to place them in the correct context, to maximise their deterrent value, and to influence key audiences. Defensive cyberspace operations require the ability to assess and analyse cyber activities and effects. NATO forces need a holistic understanding of cyberspace that is not limited to technical implications but which also takes into account the effects on human behaviour and decision making.

b. Cyberspace Engagement: As activities and threats in cyberspace continue to increase, should the NAC decide to broaden activities in the cyber domain, then corresponding policies, SOPs, capabilities, and training need to be developed.

c. Engagement through the Comprehensive Approach: NATO should continue to provide its military contribution in concert with other relevant actors in
multiple environments (Diplomatic, Information, Military, and Economic). Wherever possible, forces should work with other actors towards a Comprehensive Approach to operations.

**Sustain**

24. Innovative Supply of Materiel and Services and Minimised Logistic Footprint: Alliance forces should seek to minimise logistic footprints, ensure uninterrupted logistic support, and where necessary, create backup sustainment systems. Future technological advances, including additive manufacturing (3-D printing), use of alternative energy sources, unmanned delivery and evacuation systems and robotics, have the potential to revolutionise the sustainment of Allied forces in maintenance, repair, replenishment, and health services. Forces should seek to take advantage of new technologies as they become available.

Forces might simplify and improve sustainment and logistics methods balancing smaller/shorter logistics support against operational risk. Prepositioned stocks and dispersed logistics hubs may still be required. In some circumstances sustainment could be locally contracted or optimised using enhanced host nation support. Furthermore, in-theatre production of consumables and reduction, exploitation, and conversion of waste will increase self-sustainment and reduce the environmental impact. However, NATO forces should seek to reduce unnecessary redundancy and streamline sustainment where possible.
25. In Theatre Movement and Transportation: Forces should have assured access to sufficient ground, air and sea transportation assets to support the sustainment, deployment, and redeployment of forces across the whole NATO mission.

26. Standardisation: Forces should strive to develop interchangeable modular structures, easily repairable standardised equipment and interoperable spare parts across the Alliance. Member Nations are encouraged to maintain standardisation within the Alliance as a high priority during their national acquisition processes. Where standardisation cannot be achieved, forces should train together to obtain interoperability.

27. Diversification and Impact of Logistics: Allied forces should identify a network of military and non-military partners to help sustain multi-domain operations with scalable logistics. Whilst balancing dependency against the impact on local economies, logistics networks may need to include local commercial vendors and third-party logisticians who are able to contribute to deliver logistics in austere or urban environments. However, NATO forces should retain their ability to be self-reliant on Member Nations’ logistics.

28. Future Force Sustainment: Forces are likely to be smaller, modular, multi-capable and agile units that will often operate in a distributed or logistically autonomous manner, but must be networked together. Future forces will therefore require more modular and flexible logistics structures, with common stock systems and procedures. Leaders should be trained to conduct operations from forward areas with limited logistic support, and a reduced reliance on local infrastructure.
29. Sea Basing and Resupply from the Sea: In future expeditionary operations, which will likely occur in contested and congested operating environments including the littorals, sea basing will continue to provide an attractive option for sustaining operations, provided that sea based assets are protected from long range anti-ship threats.

30. Military Engineering: Future Allied expeditionary and urban operations might see increased difficulty in accessing a theatre of operations due to the development and proliferation of new and emerging area denial methods. This will increase the demand for military engineering capability as a key enabler. In the future, in an increasingly contested environment and in restricted terrain, forces must fulfil a wide range of Military Engineering tasks to gain and maintain freedom of movement and support force protection within the theatre from operational to tactical level. Military Engineering support includes the provision of support to critical infrastructure and civilian and military life support. Developments in advanced technology may allow the Alliance to cope with future challenges. Alliance forces should maintain extensive interoperability and use civilian contracting to complement organic Military Engineering capability.

31. Networked Sustainable Medical Support: Large-scale health crises and pandemics can create situations which quickly overwhelm local health providers. For example, a Member Nation confronted with a health crisis may request international assistance. To respond to these contingencies forces will need the ability to rapidly deploy their medical personnel, equipment and facilities. Medical deployments may occur under austere or degraded conditions.

Future technologies have the potential to improve medical care while reducing logistical footprint. Reach-back through innovative methods using robotics, information systems, cameras, and other devices may make delivering healthcare viable even when health care providers are not present.

Forces will need the ability to coordinate more closely with local civilian and military health care providers, local governments, or international organisations, and ensure best medical practice.

32. Medical Support in Geographically Dispersed Operations & Enhanced Individual Resilience: Future operations will require units to be dispersed across the operational area, which will stress existing medical capabilities. New methods of monitoring and enhancing individual health and resilience may help ease this stress and could include networked sensors and self-healing. Where medical specialists are unavailable or impractical, it may be possible to provide front-line care through the use of first
responders and telemedicine. Additionally, semi-autonomous assets for patient transportation and medical supply may make healthcare more efficient.

**Command and Control (C2)**

33. Future C2 Systems: The future security environment will require command and control systems that are resilient and interoperable. C2 systems will need to facilitate command and control through automated data and information exchange, and should assist leaders with decision-making and data analysis tools to rapidly make sense of complex problems and support course of action development. When degraded, C2 systems should automatically and seamlessly transfer vital C2 functions to backup systems via pre-determined alternate paths. In some cases, segregated backup systems operating as stand-alone systems may be required. C2 systems should autonomously re-enable following denial or disruption. Additionally, the communication pathways that enable C2 must be reliable, robust, secure and have alternate/backup systems available.

34. Future Decision-Making and Information Processing Tools: Future technology will enable more rapid collection and dissemination of an increasing volume of information across Alliance networks. Senior leaders will require operational analysts and automated tools to support mission command style decision-making and assist them in achieving clarity concerning complex problems. Once the decision to act has been taken, C2 and CIS systems must enable the secure transmission of orders and facilitate coordination of actions across all command levels. Each ally should have
access to the information necessary to execute their duties, as well as possess an in-depth understanding of the orders and authorisations required to execute Alliance operations. Alliance information will require more secure collection, storage, and distribution.

35. Partner Integration and C2: The success of future Alliance operations will rely upon a better coordination of elements of both military and non-military power through an increasing number of partners. C2 systems will need to be interoperable allowing a wide range of partners to communicate, while securing and protecting sensitive and classified information. The future will demand a collaborative environment that requires the sharing of information with trusted partners containing different classification to meet mission requirements. The Alliance can expect to coordinate its activities in an operation with local government, non-government, and international organisations as well as business organisations and key individuals. Alliance C2 systems must enable communication amongst all actors and accommodate timely interaction to achieve mutual objectives.

36. Reduced Organisational Footprint: In order to handle the challenges and opportunities of complex environments, certain operations may benefit from flatter military organisational structures that accelerate decision-making and reduce the time required to take action. Units may need to be more scalable and modular in order to organise necessary capabilities at lower levels to accomplish Alliance missions. Furthermore, senior military leaders will require a comprehensive understanding of the operational environment, including an awareness of culture, ethnicity and religion and other important considerations such as diplomatic, information, and economic issues. C2 technology will enable real time reach-back to connect experts and senior leaders to geographically separated units operating with smaller and flatter organisational structures.

37. Integrated Command and Control: The future will require robust Strategic Awareness provided by a persistent operational picture across all domains. Integrating domain specific operational pictures into a comprehensive whole will enable commanders to understand more completely the actions of all actors, and to direct Alliance forces. Similar to the recognised air picture provided by NATO’s Integrated Air and Missile Defence System, NATO will need an integrated C2 system that conducts continuous surveillance from a multiple array of sensors, and which fuses data and information about the area of operations into an integrated operational picture. Using this comprehensive operational picture, networked C2 systems will assist in the command and control of Alliance units making the integrated operations of Alliance forces more efficient and resilient. The future security environment will require Alliance leaders to have awareness and influence that extends beyond
Alliance forces and operations. Alliance leaders will find it useful to monitor and interface with non-military organisations such as local governments, non-governmental organisations, and business enterprises and will need to understand non-military environments including financial, cultural, ethnic and religious networks to maximise the effectiveness of Alliance actions.

38. Communications: Command and control will continue to rely upon communications systems and paths. NATO’s distributed forces of the future will require dominance of the frequency spectrum and access to beyond line-of-sight communications. Critical communications networks will require robust and resilient networks and systems, and NATO forces will need to be operationally proficient in communications-degraded environments. Technology that allows individuals to be continuously connected and networked will continue to proliferate and the Alliance will need to seek ways to take advantage of mobile communication devices. The Alliance will need long-range communications that reduce equipment footprint, allow real-time reach-back, and enable the chain of command to exercise C2 over vast distances. NATO forces should possess sufficient bandwidth to allow mobile, secure, rapid and timely information flow between the tactical, operational, and strategic levels of command.

Protect

39. Counter Area Denial: NATO forces should be able to create a permissive environment for their operations. Forces should be able to enter and operate in an area of operations despite anti-access and area denial methods. Forces should detect, locate, exploit and neutralise or destroy the effects of landmines, naval mines, anti-ship and anti-aircraft weapons, Improvised Explosive Devices including conventional and improvised CBRN devices, electronic warfare, and other area denial systems.

40. Lines of Communication: In the future security environment, the global commons and Alliance lines of communication will be increasingly contested by empowered actors. The proliferation of anti-access technology and the congestion of the global commons will create significant challenges for Alliance power projection and sustainment. These challenges will be especially problematic at choke points common to each domain. NATO needs to retain assured access to the global commons and the continued use of its lines of communication.
41. Expeditionary Force Protection and Base Defence: Force protection and base defence will continue to be key to the success of expeditionary operations. This demands the ability to establish superior force protection measures, physical security and access control in high-threat environments to minimise risk to Alliance forces.

42. Extended Protection: Some future crisis may overwhelm local authorities and may exceed the capacity of civilian response thereby necessitating assistance or augmentation from NATO. In some cases, Allied forces may be requested to defend critical infrastructure, vital networks, or essential lines of communication against a full range of threats. While the protection of infrastructure remains a civilian national responsibility, in extremis, Alliance forces may need to be ready to respond when asked by a Member Nation, or when a crisis occurs external to the Alliance and it demands an allied response. To prevent an adversary from exploiting crisis situations and targeting vital interests and infrastructure, forces may be required to extend a “security bubble” to protect key services including: governance, health, emergency, security/law-enforcement, finance, transportation, power, communications, utilities, agriculture and food, national monuments and icons. In crises external to the Alliance, NATO Special Operations Forces can enhance force protection of NATO forces and critical assets by working with other security actors to further expand the security bubble. Nevertheless, coordination will be required across international boundaries and with public and private entities to ensure such critical infrastructure is protected.
Wherever possible, reception and staging plans for NATO forces should be coordinated in advance.

It is the responsibility of civilian national authorities to develop an ability to anticipate, detect and identify new threats and quickly assess associated risks to critical infrastructure, assets and resources. Member Nations should then be able to provide NATO with timely early warning to enable rapid development of countermeasures through the leverage of emerging technologies and innovative thinking.

43. Security of Communication and Information Systems (CIS) including Cyber Defence: NATO should be prepared to operate in a cyber-degraded or denied environment and be able to contribute to a comprehensive cyber-security strategy in all domains. The Alliance should be prepared to defend against all forms of external and internal cyber-attack. NATO will need to protect against manipulation of data and information within the cyber domain. Units and headquarters should be able to validate their data and perform non-repudiation to ensure data is accurate, reliable, and from trusted sources.

The Alliance should be prepared to operate despite the loss or disruption of cyber infrastructure and hardware, including loss of space assets, network servers, undersea cables, radio communications, and power generation. NATO should have the ability to track friendly and enemy activities in congested cyberspace, the ability to partner with states and corporations to prevent cyber disruption and the ability to restore cyber access to key areas rapidly once interrupted. Legacy or alternate technologies, for example celestial or map and compass navigation techniques, must be retained to provide resilience and help counter the cyber-threat.

NATO needs to be able to balance system interoperability and ease of use with encryption, segmentation, segregation, or stand-alone systems to mitigate risk. NATO may need a certain percentage of non-networked systems. If a cyber-disruption occurs, forces should understand how systems degrade and be able to transfer vital functions to other systems automatically. Vulnerability assessment teams should aggressively search to identify network vulnerabilities and recommend remedial action. Active and passive tools must be developed within the cyber domain to identify, analyse and react to incursions that occur at electronic speeds. A cyber-emissions control plan which predetermines an appropriate response to cyber disruptions needs to be developed.

44. Emerging Technology: Emerging technology will provide the Alliance with many opportunities, but will create significant challenges as nations and non-state actors seek to narrow NATO’s current technological advantage. Allied forces will need to
understand technology and be able to innovate new and creative tactics, techniques, procedures, capabilities and doctrine. The Alliance will need to be cognizant of the acquisition and innovative use of technology by others. Without incurring the cost of research and development, nations and non-state actors can capitalise on technological advancements and translate them into capabilities that threaten the Alliance. While it is impossible to predict all of the areas where technology could revolutionise warfare, some of the key areas to monitor include: directed energy, autonomous systems and sensors, quantum computing, unmanned systems, electromagnetically launched projectiles, renewable energy, artificial intelligence, 3D printing, additive manufacturing, biotechnology and nanotechnology. The Alliance will need to consider the ethical implications of technological advances as well as how to guarantee human control of autonomous and unmanned systems.

45. Unmanned Systems: A proliferation of unmanned systems conducting military and non-military missions has made them available to a wider range of actors and unmanned systems are being deployed in increasing numbers. Unmanned systems conduct surveillance, weapons delivery, resupply, and a host of non-military applications and are being used on land, air, sea, and in space. The Alliance needs to be able to exploit advances in unmanned systems, while limiting their advantage to potential adversaries.

46. Swarm Techniques: NATO forces should have the ability to use, and to counter, swarm capabilities in all domains. Swarm techniques could potentially help to overcome anti-access and area denial threats.

47. Protection from Surface and Sub-surface Threats: To exploit the advances in new maritime technologies for manned and unmanned water vehicles, both in deep water and the littorals, Member Nations should obtain the latest surface and subsurface maritime technologies including anti-submarine detection, underwater warfare capabilities, and anti-ship systems to include long range anti-ship missile defence. Similarly, in the land environment, forces should be capable of countering subterranean threats.

48. Alliance Integrated Air and Missile Defence: The increasing development of low-cost unmanned air systems and sophisticated manned aviation platforms will continue to challenge the Alliance and must remain an area of focus. NATO should be able to survey its airspace, identify, classify, and share information on air traffic, and have the means available to counter a wide range of air threats. Alliance air-defence will continue to require a highly sophisticated network of shooters and sensors.
49. Protection from Ground Based Air Defence and Integrated Air Defences: Forces will need an ability to operate despite the proliferation of adversarial air defence systems. Proliferation of man-portable air defence systems and advanced ground based air defence systems (surface to air weapons) will change the dynamics of Alliance air operations which have recently been conducted in permissive conditions. Adversaries will likely use information systems and sensors to create complex integrated air defence systems that create extensive defence in depth in an attempt to disrupt Allied air operations. NATO forces may encounter integrated air defences employed by non-state actors.

Air defence systems proliferation has extended the anti-air threat to military and civilian aircraft to non-state actors. Forces will continue to protect their air systems from air defence systems and in many cases ground-based fire support may replace air-delivered fires.

50. Defence Against Guided Rocket Artillery Mortars and Missiles: Technology proliferation will increase the risk to Alliance forces from Guided Rocket Artillery Mortars and Missiles (GRAMM) systems. GRAMM may require appropriate defensive measures, including Counter Rocket Artillery and Mortars systems.

51. Ballistic Missile Defence: Proliferation of ballistic missile technology will increase the need for ballistic missile surveillance and defence. Missiles will need to be identified, intercepted and destroyed prior to or during launch. The hazards of falling debris from successful ballistic missile intercepts will need to be reduced, including those from ballistic missiles loaded with CBRN warheads. To facilitate successful intercepts, NATO forces will need interoperable ballistic missile defence systems and be able to share targeting data.

52. Defence from Space Weapons: While international agreements seek to prevent space weapons, some nations may find space weapons attractive. NATO may need to develop and maintain an ability to defend against space weapons as well as an ability to detect and identify objects and threats from space. Member Nations will also need to protect their space-based systems and in some cases develop non-space alternatives.

53. Protection from WMD/E: The Alliance must be prepared to counter the threat from WMD/E. NATO will need the ability to detect, identify and disable such weapons when required.

NATO may take advantage of emerging technologies to enhance force protection against the WMD/E threat. For hazard management procedures the Alliance should
consider resource-saving technologies, such as enzymatic technologies, and should increase efforts to introduce nanomaterials for CBRN hardening of materiel and equipment. The Alliance may need to further develop smart materials to enhance individual CBRN protective equipment and detection capabilities for CBRN substances.

In the CBRN environment, NATO should also capitalise on semi-autonomous platforms to conduct surveillance, reconnaissance and exploitation, rescue and extraction, and hazard and consequence management.

54. Environmental and Hazard Protection: Forces should seek to minimise their environmental impact. The future security environment will likely be characterised by increased sensitivity to the environmental impact of operations. Forces should minimise collateral damage to infrastructure where known Toxic Industrial Material is produced, stored, or handled.

Inform

55. Collection: NATO should have the ability to detect, track, monitor and share information on threats in all domains including cyber and space. To enhance the collection of timely and accurate information, forces should increase the use of persistent unmanned ISR systems, to exploit multi-intelligence sources from alternative origins (commercial, private, national), and deploy robust military ISR. NATO should be able to detect and identify targets despite technological advances in stealth, camouflage, concealment and deception techniques, especially in urban and subterranean environments. The Alliance should continue to exploit open-sources including social media to gain, share and fuse information and help set the conditions for future success. Such fusion will enable NATO to better detect adversary information operations in the early stages of development.

NATO should be able to develop and maintain a recognised cyber picture of its networks and collectively maintain a shared situational awareness of national systems which process or transmit NATO information. This includes maintaining an awareness of NATO cyber capabilities and vulnerabilities and the development and execution of a cyber-intelligence collection plan to gain situational awareness of the cyber environment. NATO should be able to monitor cyber areas of interest, to detect cyber-attacks and cyber-espionage against NATO systems. The Alliance should be enabled to conduct cyber forensics to accurately attribute actions to their sources.

NATO should be able to rapidly detect "anomalies" in the activities that occur in the global commons on lines of communications and at choke points, as well as within big
data flows. The Alliance should use cost-effective technology including autonomous and disposable assets, remote sensors, and intelligence networks to enable early warning.

Besides technological collection, human sources related collection should be trained and cultivated. Particular attention should be paid to the Terrorism, Espionage, Subversion, Sabotage and Organised Crime threat. Counter Intelligence collection should be permanent as a way to detect non-conventional threat activities which could be an indication of larger scale adversarial operations.

NATO must have the ability to conduct Joint ISR collection from various areas to include the littoral areas, international waters, overland friendly airspace, and overland in contingency Joint Operating Areas. In regards to collection from within friendly airspace, sovereignty of national airspace is paramount and therefore procedures must be in place between NATO and Member Nations to specify any unique collection caveats or prohibitions. Furthermore, NATO must continue coordination with regional and national Air Traffic Managers to implement a robust Remotely Piloted Aircraft Systems (RPAS) Airspace Integration approach throughout Europe that facilitates effective JISR operational mission accomplishment.

56. Analysis: Due to the vast amount of available information and ever increasing number of sensors and sources, the Alliance will need to improve the conversion of information into intelligence. NATO needs to enhance the current NATO Indicators
and Warning System to better identify the early phases of a crisis and enable timely decision-making.

NATO will need the ability to access and analyse data, and share intelligence across all domains at the strategic, operational and tactical levels. The Alliance should maintain a repository of knowledge about the comprehensive planning operational environment that enables the conduct of collaborative planning using advanced technological methods, including artificial intelligence, virtual reality, modelling and simulation.

NATO will require the ability to analyse networks, and evaluate potential adversarial command and control structures. The proliferation and increasing complexity of networks, including anti-access and area denial and integrated air defence systems, will require a sophisticated ability to develop a detailed understanding of these networks, at strategic, operational and tactical levels.

The Alliance will need the tools and expertise to mine and analyse large amounts of unstructured data (big data) in order to inform decision-making and add to awareness at all levels. NATO needs regional experts to support intelligence collection, liaison, education and training at all times, including via reach-back.

57. Broad Mapping: To support operations in complex 3D-urban terrain, including high-rise/vertical buildings and underground structures, the Alliance should acquire the ability to develop and disseminate geospatial products - "maps of the future" - rapidly. These will need to include undergrounds, factories, high-buildings, slums and ISR products and imagery. To ensure the most accurate urban maps, urban areas may require tailored reconnaissance and surveillance. NATO should routinely update maps in near real time to take into account the impact of changes from operations, natural disasters and the organic expansion of cities.

In order to develop knowledge of the operating environment in densely populated areas the collection and analysis of information on networks (including possible impact of disruption), critical utilities, resources, and infrastructures, interoperability with local Air Ports of Debarkation and Sea Ports of Debarkation will be necessary. City assessments should be prepared to inform tailored doctrine, tactics, techniques and procedures.

A collaborative approach which enables shared intelligence would be mutually beneficial and may include intelligence exchange, a common database, network knowledge, forensics, and biometrics in order to detect unconventional threats. A human network analysis ability should be developed to analyse the relationship
between people at the individual, family, tribal, national, and international levels. This should also include a range of other potentially violent groups.

Social media and international real-time communications now enable rapid exchange of ideas and mobilisation of ad-hoc organisations. Adversaries are using modern communications to spread extremist ideology, recruit transnationally for foreign fighters and foster domestic terrorism. During operations, the Alliance may need to develop early warning capabilities to anticipate social unrest and detect rapid gatherings of people. Forces will need to detect, classify, and identify individuals in complex 3D terrain, including urban, using biometrics and other accurate methods.

58. Sharing: Sharing activities encompass obtaining contributions from other actors and conveying information and intelligence to those partners who need it in a timely manner. Improving NATO’s information and intelligence sharing capability requires the prior development of agreements, policies and principles to leverage nations’ military and non-military expertise together with relevant actors, partners, and entities. These activities may include the collection, processing, and dissemination of intelligence amongst stakeholders. NATO may need to obtain information which falls outside of the military domain and may require close coordination with other international organisations.
CONCLUSION

1. As SFA 2013 identified, the future will be increasingly complex and uncertain, thereby presenting challenges as well as opportunities fuelled by a rapid rate of social, economic, scientific, technological and environmental change. NATO may face adversaries consisting of states as well as non-state actors that will work independently or in concert to challenge the Alliance in ways that complicate a consensus based response. Adversarial states may use non-state proxies to deny responsibility for their actions and non-state actors will be more difficult to identify. They may also be more difficult to deter as they may not possess resources or assets that can be credibly threatened by military force. NATO’s adversaries may not accept internationally established borders, treaties, rules of law or norms of behaviour. They may increase their use of asymmetric or irregular forms of warfare to counter NATO’s military superiority. Some states or non-state actors may seek to combine different forms of warfare – conventional, irregular and cyber warfare – and possibly, large scale terrorism including use of WMD/E. They may try to deny the Alliance clear, legitimate courses of action and identified targets and may seek to increase ambiguity, posing the problem of indubitable attribution that is currently experienced in cyberspace. This hybrid and ambiguous model might make it more difficult for NATO to achieve consensus, and prepare for and conduct operations.

2. The SMPs provide the strategic commander’s guidance to prepare for the future security environment and are the essential characteristics required by the Alliance at the strategic level. The Strategic Commanders recommend that NATO develops operationally agile forces that are resilient, strategically aware, supported by proactive strategic communications, and networked with a wide range of security partners. Alliance military forces can improve operational agility by becoming more flexible, robust and responsive, through scalable military units and command and control structures that are able to aggregate and disaggregate quickly. Through cooperative, persuasive and proactive engagement with other nations, organisations and actors, NATO can enhance its ability to influence the security environment through continuous interaction by means of security networking via physical and virtual presence. Through the development of shared resilience, NATO’s ability to conduct sustained operations in spite of surprise or strategic shock and to quickly recover from setbacks can be enhanced. To seize opportunities and respond correctly to emerging crisis, NATO will require improved, credible and shared strategic awareness. Strategic awareness requires ISR capability that provides a real-time, comprehensive and operational picture. Underpinning all Alliance missions and operations, the development of proactive strategic communications will enable the Alliance to project a coordinated narrative by aligning words and actions.
3. Military Implications are not defined requirements, nor are they expressed as required capabilities. Military Implications are best military advice expressed as abilities, to inform Alliance transformation, including development of policies, long-term requirements, and capabilities. Alliance and Member Nations may consider those long-term abilities, which are plausible and sufficiently defined today, to warrant consideration during planning. Recommendations are based on efficiencies in scale, effects, and cost. The key deductions are as follows:

- NATO technological superiority and access will be challenged. Access to the global commons and to areas of operations will be contested by anti-access and area denial methods, CBRN threats, and new technological advancements. The Alliance will need to develop abilities to gain and maintain access, and counter a wide range of proliferating threats posed by the rising capabilities of potential adversaries.

- Technology will increasingly provide both challenges and opportunities. The Alliance will be challenged by actors with access to sophisticated off-the-shelf technology. Private investment in research and development will continue to outstrip state funding, and innovative products will be available to all. Access to future technologies may enable some actors to achieve technological parity with NATO in certain fields, and allow non-state actors to rival states. However, rapid advances in technology could also revolutionise Alliance operations. Taking into account moral and ethical considerations, Member Nations can improve the efficiency and effectiveness of their capabilities while reducing the cost of modernisation through the flexible acquisition of new technologies. Improved manned and unmanned systems will reduce risk and the possibility of loss of life. Furthermore, a mixture of low and high-tech systems can improve resilience through the diversification of NATO systems. New tactics, including swarms of unmanned systems, have the potential to enable the Alliance to spontaneously mass on the battlefield while reducing operational risk.

- Future Alliance forces will need to increase their operational agility by being modular, scalable and trained for a wider variety of missions using innovative tactics. Flatter organisational structures and mission-command may be required to address complex and changing future threats. Future command and control will need to enable collaborative planning and decision-making, while ensuring connectivity of dispersed forces to the chain of command. NATO forces can be better sustained through streamlined logistics. Future technologies may enable the reduction of logistic footprints and improve the responsiveness of the supply chain.
• Increased urbanisation makes NATO operations in an urban environment more likely. NATO forces will need to understand, train for, and operate in complex urban environments with mass populations that are networked and mobile. NATO may also need to support civil authorities who become overwhelmed in a crisis. This may necessitate the provision of key services so as to deny an adversary the opportunity to exploit a chaotic situation.

• New technologies and a dynamic environment will challenge traditional information and intelligence systems. NATO forces will need to be able to mine and analyse vast quantities of data to produce and share actionable intelligence, improve situational awareness, and support decision-making. While not necessarily owning data, NATO will need access to it, along with the ability to share information with an increasing number of actors and partners.

• The Alliance will continue to use cyberspace to facilitate communications and command and control. However, cyberspace will increasingly be threatened, and the Alliance will need to maintain access to resilient and robust cyber systems hardened against attack and develop alternative systems that are impervious or less vulnerable to cyber-attack. NATO must be able to generate a recognised cyber picture.

• Strategic Communications supports Alliance policies and operations and contributes positively and directly to the successful implementation of NATO military operations, missions, and activities by aligning words and actions. By placing information and communication at the heart of all levels of policy, planning and implementation, and ensuring they are a fully integrated part of the overall effort, Strategic Communications can make a major contribution to Alliance success.

4. The FFAO provides the Strategic Commanders’ best military advice concerning the long-term future, seeks to inform NATO’s long-term military planning processes and provides national military planners a sense of NATO’s broad direction of travel for the long-term. FFAO is intended to directly inform all steps of the NATO Defence Planning Process (NDPP). FFAO will also inform other transformation and defence planning efforts.

The Instability Situations and Strategic Military Perspectives provide the context and general characteristics of future Alliance military forces that the Strategic Commanders deem necessary for future success. They are particularly useful for focus areas, scenario development, force modelling, capability development and discussion of proposed national targets. The Military Implications provide specific
recommendations for defence planners to help focus long-term capability
development activities and military planning.

Finally, many Member Nations may find the results of the SFA and FFAO and participation in ACT’s Long-Term Military Transformation process useful for national defence planning. FFAO provides a start point for discussion of the future perspectives and requisite abilities to help nations best determine how to participate in NATO’s long-term transformation efforts.

Annexes:

A. Strategic Foresight Analysis 2013 Trends
B. Instability Situations
C. Common challenges derived from Strategic Foresight Analysis and the Instability Situations
Annex A. Strategic Foresight Analysis 2013 Trends

The Strategic Foresight Analysis 2013 Report built on principles described in NATO’s 2010 Strategic Concept as the basis for ensuring Alliance security in the future and was based on national and international studies that address the timeframe out to 2030 and beyond. The Strategic Foresight Analysis identified 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 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.
### Annex B. Instability Situations

| **Access and Use of Global Commons Challenged** | Substantial increase of pirate threat on global flows, Lack of resources and climate change create new contested areas, Lines of communication/commerce threatened, Virtual Organisations, Climate Change, Access to global commons |
| **Conflict in Euro-Atlantic Region** | Expansionism at NATO borders, Large-scale insurgency within NATO borders, Decreasing Defence Expenditures encourage challenges to the Alliance, Imbalance of military power, Breakdown of a NATO member caused by internal factors, Breakdown of a NATO member caused by external actors, War-like situation in Europe, NATO Alliance weakened or ineffective, Imbalance between availability of defence resources & security challenges, Testing of NATO/Partner Territory |
| **Disruptive Impact of Migration** | Massive immigration causing instability, Uncontrolled refugees, displaced persons, economic migration, Migration Wave |
| **High-Impact Cyber Threat** | Large-scale cyber-attack on NATO member or affecting NATO, Cyber Challenges, Cyber Warfare, False Identity |
| **Large-Scale Disaster** | Large-scale disaster occurs, opportunist actors take advantage of chaos, Pandemic strikes NATO Nations, Natural Disasters, Weak State Challenge, Disaster Relief in a World Financial Centre |
| **Megacity Turmoil** | Turmoil in a Megacity, Inability of the nation-state to provide security / basic needs in megacities, Urbanisation and Resource Competition |
| **Non-State Actors Rival State** | Attack on Critical Infrastructure, Virtual Organisations Climate Change, Competition to gaining the best security policy/market positions, Changes in Society being different from national position, Decline in existing systems – establishing new ones, Dependence on critical infrastructure, Failing/Shifting of Political Structures, State versus non-state actors, Use of Disruptive Technology by a Youth Group with different mindsets |
| **Space Capability Disruption** | Loss of Space Use, Space resilience and vulnerability, Space |
| **State to State Conflict** | Conflict spill over to neighbouring countries on NATO borders, Interstate conflict over access to resources, State to State Conflict, Resource wars, Frozen Conflict, New Spheres of Influence |
| **Weapons of Mass Destruction/Effect use/threat** | Terrorist attack with WMD/E affecting NATO, Weapons of Mass Effect, WMD/E crisis on the edge of NATO |
## Access and Use of Global Commons Challenged

### Statement of Context

The increased globalisation, technological advancement and interconnectedness of countries make global access both more valuable and more vulnerable. Actions that constrain access to the global commons could have great impact on global financial markets, transportation networks and energy supplies. With the increased dependence on the global commons, states and non-state actors may be able to disrupt the flow of commerce, communication, and resource collection/distribution and, thereby, impact military operations as a means of gaining leverage or for financial gain. Access to newly available trade routes and resources, e.g. the Arctic, may also generate more competition within the global commons.

### Main Contributing Trends


### Who:

State and non-state actors including multinational corporations will compete for access to the global commons. Extremist groups, criminal organisations such as pirate networks and states using proxy groups may seek to disrupt access to common areas.

### Why:

All actors will seek to gain financial, political or military leverage by controlling global commons. They will seek to control the commons to extend influence and provide a counterbalance to or simply disrupt the operations of the Alliance. They will demonstrate power through economic, civil, political and military means, and may deny access to the global commons in retaliation for political or military actions. States that lack energy supplies will seek new options for acquiring and controlling access to resources. To reduce damage to the climate, extreme environmentalists seek to disrupt resource discovery and extraction by using new technology.

### How (Ways and Means):

Actors may disrupt lines of communications and distribution networks to deny natural resources to states. They will challenge maritime freedom of navigation and commerce (e.g. pirates, undersea robots and sea mines) extending their reach beyond the littorals to blue water. They will seek to increase their technical capabilities to disrupt trade. They will interrupt the air freedom of movement via widely available air defence and missile systems, unmanned vehicles, and computer technology that provide global reach. They will work to control the cyber domain to interdict satellite and voice communications, undermine financial electronic systems and degrade intelligence collection systems. It will be more expensive in the future to prevent or counter an adversary’s use of low cost technology, such as the use of improvised explosive devices.
<table>
<thead>
<tr>
<th>Where:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actors will seek greater access to common use areas with a particular focus on new areas of exploration, resource development and trade. Examples of these new areas include the Arctic, outer space and cyberspace.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What is new in 2030?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-state actors will have more ability to exert some measure of influence over common areas due to increased access to technology. Multinational corporations and criminal organisations will be more competitive due to increasing economic power relative to states and will have greater global reach due to technology. The scarcity of resources will entice criminal and private security groups to develop more successful business models to control access to the commons. Cyber and space will become more contested. Coordinated competition will exist simultaneously in the physical dimensions, like air, polar regions, sea and outer-space, and also in the non-physical dimension of cyberspace. Legal aspects over commons will be disputed as more actors become dependent on international trade.</td>
</tr>
</tbody>
</table>
## Conflict in Euro-Atlantic Region

### Statement of Context

Conflict arises in the Euro-Atlantic region and expands into NATO territory. NATO confronts state and non-state groups that have formed new alliances with conflicting goals and values to those of the Alliance. For example, expansionism at NATO’s borders and profit-driven transnational actors (multinational corporations) could lead to internal instability within a NATO member. Super-empowered individuals, extremists or political parties driven by ideology and fractured identities could contribute to the internal instability of a NATO member or fuel a large-scale insurgency within the Alliance or at its borders. Assessments of security in Europe in recent years along with economic crises have resulted in lower defence expenditures. These current levels of defence spending could fail to provide an adequate deterrent against external challenges to the Alliance, e.g. non-NATO state uses aircraft or ships to violate NATO borders as means to test the Alliance and its reaction.

### Main Contributing Trends


### Who:

State and non-state actors; ethnic/religious groups; extremists/separatists, specific social classes, ideologically-driven groups, migrants/displaced populations, especially minorities, super-empowered individuals, profit-driven transnational actors (multinational corporations) could all or individually challenge a NATO member country in Europe. NATO Nations will face emerging powers that have interest in weakening the Alliance. Local populations inspired by nationalism/isolationism or regional defence cooperation entities will challenge a state in the Euro-Atlantic region.

### Why:

Historical reasons such as ethnic, religious, cultural or disputes will drive political change. Perceived weakness of the state or military and lack of security will result in increased political, economic and social instability. Emerging powers will seek to extend influence to gain political, social, and economic power and to access resources. The perceptions of peace and a high level of security in Europe in combination with the imposed austerity measures contributed to decreasing defence expenditures; therefore, NATO may face additional challenges in maintaining the capabilities needed to execute the core tasks in 2030. The ability of the Alliance to react to challenges is lost (especially in a polycentric world where rising powers have greater capacity to fund, supply, and maintain their defences). A state or new alliance seeks to protect their perceived interests by weakening the NATO Alliance.

### How (Ways and Means):

Hybrid actors exploit political, economic and social volatility to challenge governments through a range of traditional and new tactics like: demonstrations, boycotts, rioting, bank runs, market manipulation, cyber-attacks, asymmetric and conventional warfare including
the use of Weapons of Mass Destruction/Effect (WMD/E). Such actors will also manipulate the political narrative using mass communication, social media and advocacy networks, as well as employing economic tools to gain influence within NATO (e.g. energy dependency and financial interdependency). Actors will attempt to undermine democratic systems causing a member Nation to request NATO support. Multiple security providers will compete for limited budgets and manpower, for example police, military, intelligence and emergency services. Non-NATO aircraft or ships violate NATO borders to test NATO’s reaction, both politically and militarily. Due to the accelerating pace of events, deliberate NATO decision making may be unable to counter a challenge in time to prevent a crisis; i.e. the compression of decision cycles complicates NATO’s decision processes making rapid consensus unattainable.

<table>
<thead>
<tr>
<th>Where:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Euro-Atlantic Region; particularly NATO’s periphery.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What is new in 2030?</th>
</tr>
</thead>
<tbody>
<tr>
<td>NATO’s ability to reach consensus and act rapidly will in large part depend on a common understanding of the new security environment. Different national threat assessments within the Alliance may impede consensus, which would weaken perceptions of NATO’s value, relevance, and cohesion. Globalisation, political movement towards peaceful solutions and interdependence makes reaching a consensus on resorting to armed action more difficult; however, lack of deterrence because of decreasing defence expenditures opens opportunities for challenges to NATO. Reduced defence expenditures will result in loss of technical, quantitative and qualitative superiority and power projection capabilities, thus creating capability gaps and changing the regional balance of power in Euro-Atlantic region. New challenges to NATO in 2030 are: emerging powers and new alliances (state and non-state); the increasing power of the media and multinational corporations, the rise of new security providers such as Private Military and Security Companies (PMSC), the increased flow of populations, the growth of urbanisation, and the formation and vast expansion of networks (e.g. cyber, transportation, economic, energy, and human). New opportunities for NATO in 2030 are: increased membership/partnership, new security providers such as Private Military and Security Companies (PMSC), expanded space and cyber domains, network-oriented public diplomacy, the ability to mobilise, command, and control via networks.</td>
</tr>
</tbody>
</table>
## Disruptive Impact of Migration

### Statement of Context
Mass human migration caused by demographic, environmental, economic or political change or armed conflict will exceed the ability of governments to protect and provide services for their resident populations. This uncontrolled migration will increase the potential for inter-ethnic, cultural, racial and religious tensions.

### Main Contributing Trends

<table>
<thead>
<tr>
<th>(4) Changing Demographics</th>
<th>(5) Urbanisation</th>
<th>(6) Human Networks/Transparency</th>
<th>(7) Fractured Identities</th>
<th>(14) Environmental/Climate Change</th>
<th>(15) Natural Disasters</th>
</tr>
</thead>
</table>

### Who:
Nations with limited resources or infrastructure that have weak immigration control could become target nations for migrant source nations. Other nations could expel their populations to cause civil unrest in a target nation. Extremist, criminal, ethnic organisations interested in creating instability will establish their networks with large, displaced, urban, populations.

### Why:
Rapidly changing environments (economic, political, or physical) will cause massive migration. People will move to avoid epidemic, poverty, inequality, political oppression, climate change or natural disaster. Government authorities are under resourced to respond adequately to large migrant populations. Groups will use population displacement to gain power through ethnic cleansing.

### How (Ways and Means):
Actors will cause mass demonstrations to disrupt life support within urban areas. The increased communication and human networking capabilities available through the internet and social media will accelerate disputes within migrant populations. Migrants will use a range of transportation means, (air, rail, road, and sea), to move to urban areas. Open borders, global transportation network and ease of movement enable rapid migration between countries. Political groups, state actors or criminal networks use migration as a means to achieve organisational goals.

### Where:
People are moving from rural to urban areas. Megacities within poor countries will be less able to manage the mass of migrants. Regions at high risk for earthquakes, hurricanes, and other natural disasters, underdeveloped countries with autocratic regimes and lightly defended borders especially near coastal areas, as well as regions with politically oppressed populations will be the migrant source areas.

### What is new in 2030?
Control over the flow of mass migration will become a widespread security issue especially within urban areas. More areas will be at tipping points where thresholds leading to crises will be more easily exceeded. More populations will be at risk caused by greatly increased urban population growth; accelerating climate change and political unrest. The speed and rate of movement and size of migrant groups will increase thus degrading ability to control
migration. Multiple migration flows will occur simultaneously. Migrants provide opportunity for host nations to address declining populations by increasing human capital and supporting population growth. Disruptive migration also has the ability to increase the internal strife between government and immigrants as well as between residents from different subnational groups.
### High-Impact Cyber Threat

#### Statement of Context

The growing dependence and reliance on computer connected and networked systems increase NATO vulnerability to a range of asymmetric cyber-attacks that could degrade or destroy critical infrastructure, particularly within the financial, communication, transportation or energy sectors. The Alliance will face a broad range of vulnerabilities due to near total network connectivity. This will provide an opportunity for potential aggressors to impact NATO.

#### Main Contributing Trends


#### Who:

State and non-state actors may engage in asymmetric competition using technologically-empowered individual or groups, criminal organisations and internet connected activists as proxy agents. Attribution of attacks will continue to be difficult as proxies increase complexity.

#### Why:

To undermine international cohesion, reduce military capabilities, and mislead or discredit nations, or to gain an advantage through asymmetric attack, potentially anonymous asymmetric cyber attackers achieve physical impacts that influence political decisions.

#### How (Ways and Means):

State and non-state actors working through proxies or specialised cyber forces use robotic and artificially intelligent systems, customised software architectures, and highly sophisticated electronic warfare equipment to degrade national/NATO command and control systems. These actors will specifically hijack part of the cyber domain to target networks or computer systems. These cyber actions may support attacks in the physical world. State and non-state actors will collect, destroy and corrupt information or disrupt communication systems, financial centres, NATO and National defence institutions, as well as energy supplies.

#### Where:

State and non-state actors will seek to control network infrastructure including computer centres and servers, hardware and software, electronic and fibre optic transmission lines, internet providers, and anything located in the physical world that is critical to network security. These powers will focus on a range of locations and systems to conduct operations from healthcare, transportation, communication, financial, energy, military or civilian services. With the rise of the “internet of things”, these operations will move to include almost all tangible and physical objects. Also, actors will seek to control virtual worlds and will conduct operations entirely within a computer based virtual battle-space.
<table>
<thead>
<tr>
<th><strong>What is new in 2030?</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Essentially all things will be vulnerable due to near total interconnectedness and the blurring of physical and virtual worlds. The power of computing will be exponentially greater. The use of artificial intelligence and robotics will be pervasive throughout societies. The scale, speed, and impact of a cyber-attack combined with the use of new technologies such as additive manufacturing will have global reach and influence across any and all borders. The ability to remain unknown while targeting specific systems combined with the minimal cost and low barrier of entry to obtaining a cyber-capability enhances the impact of cyber-attacks and provides little or no warning, i.e. a highly accurate stealth attack capability will be available to almost everyone. Cyber defence will lag further behind offense technology widening the gap between attack and protect capabilities.</td>
</tr>
<tr>
<td>Large-Scale Disaster</td>
</tr>
<tr>
<td>----------------------</td>
</tr>
<tr>
<td><strong>Statement of Context</strong></td>
</tr>
<tr>
<td>Large-scale disasters, such as deadly pandemics (natural or manmade), famine or natural disasters result in governments seeking external support in the provision of health, security, and welfare of governed populations. Entities like nations, criminal organisations or extremist groups exploit the chaos to achieve goals.</td>
</tr>
<tr>
<td><strong>Main Contributing Trends</strong></td>
</tr>
<tr>
<td>(5) Urbanisation, (6) Human Networks, (14) Environmental/Climate Change, (15) Natural Disasters</td>
</tr>
<tr>
<td><strong>Who:</strong></td>
</tr>
<tr>
<td>The government and people who live within an area impacted by a disaster will be the most involved. However, a disaster will attract a range of opportunistic groups including state and non-state actors, extremists, and criminal organisations. Also there will be a large number of other actors who will respond or be impacted by the disaster including state military and disaster relief agencies international organisations (IO), non-governmental organisations (NGO), private sector or commercial entities, and security organisations.</td>
</tr>
<tr>
<td><strong>Why:</strong></td>
</tr>
<tr>
<td>Although disasters negatively affect the people in impacted regions, such crises also create opportunities for others. Since vulnerability to a disaster is increased by heavy urbanisation, limited resource availability, and weak governments, any disruption of transportation, energy supply or communications may challenge civil services and degrade the ability to respond. This lack of control allows state or non-state actors to use disaster as an opportunity to destabilise a government. Also as a consequence of globalisation populations tend to concentrate and people can move rapidly between urban population centres thus increasing the potential for epidemic or pandemic. Climate change will increase the frequency and severity of weather-related natural disasters.</td>
</tr>
<tr>
<td><strong>How (Ways and Means):</strong></td>
</tr>
<tr>
<td>Large-scale disaster (natural or manmade) will significantly increase the flow of people creating mass movement of populations. National capabilities in underdeveloped areas will be unable to cope with large-scale disasters and some regions will experience transnational impacts that could cascade across borders and lead to widespread humanitarian catastrophe. Some actors will take advantage of such situations to gain or consolidate influence over established governments, or to take control of vital infrastructure. Such a regional or global disaster provides a profit opportunity for business or criminal organisation by providing relief at a premium cost to impacted people. Opportunistic actors will seek to control resource distribution and may engage in hoarding or extreme market inflation of food, water, medical supplies, housing and energy. Competition for and authority over resource allocation during the chaos of a disaster will challenge security providers.</td>
</tr>
</tbody>
</table>
Where:
Large-scale disasters, either natural or manmade, can occur anywhere but are especially challenging to governmental control in locations with high densities of population and in littoral areas. Disasters in such regions can rapidly become a global challenge. Also, the continued and effective operation and populations of any one of the world’s financial or commercial centres are especially vulnerable to large-scale disaster.

What is new in 2030?
The frequency and severity of large-scale disasters will increase due to climate change and urbanisation. The threshold is reduced for the collapse of a state or region. Increased globalisation, urbanisation and interconnectedness make the spread of disease easier and more devastating. Faster information flows will spread fear and panic at an accelerated rate. Multinational corporations and criminal organisations play a bigger role disaster relief. Megacities in weaker states raise the probability of a collapse. Private security organisations will play an increased role in providing security.
<table>
<thead>
<tr>
<th>Megacity Turmoil</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Statement of Context</strong></td>
</tr>
<tr>
<td>Confrontation between multiple actors with varying levels of external support and competing interests create or aggravate chaotic situations to cause turmoil within megacities.</td>
</tr>
<tr>
<td><strong>Main Contributing Trends</strong></td>
</tr>
<tr>
<td><strong>Who:</strong></td>
</tr>
<tr>
<td>Local and/or national authorities, political parties; tribal and/or ethnic groups; criminal organisations, extremist/terrorist organisations; super-empowered individuals; resource starved neighbours; new politically competitive groups (e.g. during the Arab Spring established soccer fan clubs became empowered actors of revolution) will all compete for political power within large urban areas.</td>
</tr>
<tr>
<td><strong>Why:</strong></td>
</tr>
<tr>
<td>Highly urbanised populations are not resourced to be self-sustaining and will therefore consume more food, water, and energy than they produce, which further increases competition for limited resources in the urban area. Urban actors who lack political power will seek to replace governments that fail to provide security or respond sufficiently to economic distress or social unrest and that cannot prevent pervasive criminal activities or provide basic city services. Such actors will have large incentives to gain political power because of their requirement to obtain a greater share of scarce resources and to ensure security. Also, confined spaces within cities create tension and fracture identities.</td>
</tr>
<tr>
<td><strong>How (Ways and Means):</strong></td>
</tr>
<tr>
<td>Megacities amplify tensions between people and cause a fragility that lowers the security threshold (the point where governments cannot protect most of the people). Urban actors will seek to use unidentifiable crowds to take control over scarce resources. They will blend into large populations to challenge the ability of military forces to operate and will cause a human disaster to increase chaos. They will seek to disrupt services and influence populations by use of physical attacks and the spread anti-establishment narratives that are designed to provoke people to act against the government and security forces. For example, street-gangs or organised crime syndicates with military capabilities can produce no-go areas, distribute weapons, and provide misinformation to persuade local inhabitants to support their goals.</td>
</tr>
<tr>
<td><strong>Where:</strong></td>
</tr>
<tr>
<td>Urban actors will operate within densely populated areas or megacities and in places with insufficient infrastructure and services to provide for the population. They will live and work in areas with limited vehicle access and in the complex 3-dimensional terrain of urban areas with underground spaces, like subways and sewers, and within tall buildings and the dense entanglements of residential slums, abandon buildings, factories, and power plants.</td>
</tr>
</tbody>
</table>
They will target resource exporting countries in regions of high-density traffic and data flow with potential global communication nodes and strategic choke points, and cities near coastal locations.

<table>
<thead>
<tr>
<th>What is new in 2030?</th>
</tr>
</thead>
<tbody>
<tr>
<td>New alliances are formed to challenge existing powers and control capacities of established authorities are unable to govern. Non-state actors will have greater influence due to the spread of technology. Large populations of unemployed youth connect via networks to form groups that alter resource provider/consumer relationships. All Main Contributing Trends are amplified. Urbanisation will increase substantially and result in resource scarcity, reduced resilience, and will expose people to more vulnerability (e.g. disease, famine, economic, and social disorder).</td>
</tr>
</tbody>
</table>
Non-State Actors Rival States

Statement of Context

Non-state actors from around the world use a range of symmetric and asymmetric means to influence internal governance outside NATO. A combination of political, human, and technological trends lead to unpredicted actions undertaken by groups who use disruptive technologies, like computer viruses and robotics, to harm security interests of the states. In developing nations, there will be a larger cohort of unemployed young people. Such a large mass of youth is likely to become a source of social and political instability. A super-empowered individual or group of non-state actors working via virtual networks will empower these youth to oppose established authorities and generate political, economic, or social changes within states. Non-state actors will use new information channels, like social media, to promote a political agenda. Multiple actors will work together to destabilise an existing political, economic, or social system.

Main Contributing Trends


Who:

A range of non-state actors will challenge state authority, for example single-issue activists, youth groups from developing countries, private organisations with increasing economic and military capability, extremist groups, criminal syndicates, insurgency groups, tribal communities, extreme religious groups, and emerging regional powers. Any of these could be state-sponsored.

Why:

Actors will unite to challenge state authority because of demographic changes, unemployment, lack of political representation, the rise of radical ideologies, and the creation of fractured identities. Such groups will seek to gain political, economic, or social power and legitimacy, and will form new identifications. Individuals with fractured identities associate with a group that supports their struggle for political recognition, resource sufficiency, and social stability.

How (Ways and Means):

Actors organise in a variety of ways forming new transnational organisations and movements attempting to discredit the current political, economic, or social systems and develop and strengthen an alternative system to change society. These new organisations use technology to coordinate, communicate, and manipulate the narrative to influence others. Networked groups of non-state actors will spread ideological principles, alter international and national law, and selectively obey treaties. These groups may to produce long-term pressure on established government systems by conducting political manipulation, executing strikes, inciting riots, spreading propaganda, and fomenting insurgency. These non-state actors will also have military capabilities and use networks to enabled organisation.
Where:
This will occur along the border of NATO. These organisations will form by drawing globally members with similar agendas.

<table>
<thead>
<tr>
<th>What is new in 2030?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-state actors will organise, plan, and act through human networks, avoiding national law to achieve political, military, economic, and social goals. Actors will use the emergence of new technology and the exponential increase in the flow of information to gain an advantage over states. The influence of individuals will be greater than ever significantly increasing the capabilities of non-state actors. Ideas and methods will spread at far greater speed among all populations. Increased number of marginalised youth will provide a recruiting base for new transnational organisations. There will be a proliferation of ideologically driven groups.</td>
</tr>
</tbody>
</table>
**Space Capability Disruption**

**Statement of Context**
State or non-state actors compete for control over the space domain, e.g. freedom of operation in and through space. A broad range of multiple actors could take advantage of Alliance dependence on space enabled technologies which will increase vulnerability to NATO.

**Main Contributing Trends**

**Who:**
State and non-state organisations with space capabilities and technologies may compete directly. There is also an advantage for those actors who are less dependent on space to attack space capabilities of those more dependent on space.

**Why:**
Less technology-dependent actors will use a vulnerability of space dependency to gain an asymmetric advantage, e.g. economic, and/or military advantage. These actors will seek to gain political power by attacking or disrupting space dependent powers and will compete for limited space resources (e.g. orbital and launch locations).

**How (Ways and Means):**
Actors will hijack or employ piracy of space infrastructure to achieve virtual or physical disruption or destruction of military, financial, navigation and communication capabilities. These actors will deny access to space, destroy or deny use of satellites, execute offensive space to space, earth to space, and space to earth operations. They will seek to gain either permanent or temporary control over space assets including communication, intelligence and navigation.

**Where:**
Actors will compete in space, within cyberspace, and on terrestrial based installations of geostrategic significance, e.g. launch sites and communication centres.

**What is new in 2030?**
Diminished redundancy because of greater dependence on space based systems creates new vulnerabilities, e.g. widespread dependence on Global Positioning System (GPS) and communication. Decreases in costs; proliferation of space technology; and increases in the number of potential actors in space, including private or commercial actors, increases competition and vulnerability to those who depend upon space capabilities and technology. There will be new actors in space including emerging powers. These emerging powers will have such an increased interest in the space domain to make the space increasingly more contested in 2030. There will be greater pressure to locate weapons in space. There will be a range of actors in space who are not directly controlled by any government.
State to State Conflict

Statement of Context
Regional instability resulting from conflicts between states over territory, resources or historical tensions (e.g. border, ethnic, cultural, or religious disputes) will have global consequences due to globalisation, shifting political structures, and the expanding size and mobility of populations.

Main Contributing Trends

Who:
States will compete globally resulting in armed action. This will involve a range of actors including private contractors, militias, religious or ethnic minorities, multinational corporations, and insurgent groups, as well as intergovernmental organisations, regional frameworks and alliances, like NATO, EU, and African Union.

Why:
States will resort to armed conflict because of fear, honour and/or interests. States will seek to increase national power and prestige by gaining resources, expanding territory, controlling populations, influencing supply lines, gaining or increasing economic power, bolstering national pride, rebalancing power and influence, forming new alliances, developing buffer zones, integrating territories or ethnic minorities, spreading ideologies, and reacting to crises in their geographic vicinity.

How (Ways and Means):
States will use all conventional means including the full range of military capabilities and operations, including all political, economic, and diplomatic means. States will also employ non-conventional means to deter or compel other states including offensive cyber capabilities, irregular militias and special forces and unconventional capabilities, like Weapons of Mass Destruction or Effect. States will demonstrate power with kinetic and non-kinetic means and will seek new international conventions and laws and will build new alliances and political blocks to enforce them. States will attempt to influence their narrative via new technology i.e. through social media and extending pervasive internet connectivity. States will provide economic and military support of minorities and implement embargos.

Where:
States will compete globally in all dimensions and domains, including space and cyberspace; particularly in densely populated, littoral and other regions rich in resources.

What is new in 2030?
States will possess wide-spread access to the most advanced technology, such as space-based weapon systems; artificial intelligence (AI), robotic systems, enhanced human capabilities, additive manufacturing, advanced electronic warfare, and WMD/E. Population increasing will exceed the ability of states to provide basic needs. New resources will be available due to new technologies and climate change. Urbanisation will drive the need for
more resources. Global transparency will allow rapid dissemination of ideas (political, economic, religious, cultural, and social), highlighting the disparity between developing and developed regions. Multipolar competition will replace unipolar hegemony and bipolar competition.
## Statement of Context

More actors have access to WMD/E leading to increased possibility of their use. Specifically, chemical, biological, and radiological weapons will be universally available to almost anyone with enough financial resources. Moreover, the impact of these weapons will increase significantly within the large urban populations of 2030.

## Main Contributing Trends

1. Urbanisation, 2. Fractured Identities, 3. Technology Accelerates Change, 4. Increased Access to Technology; 5. Centrality of Computer Networks

## Who:

States and state-sponsored groups; emergent powers, non-state actors including super-empowered individuals, separatist groups and liberation movements or single issue political groups e.g. environmental politics.

## Why:

In a multipolar world, actors use WMD/E to achieve a strategic shock that alters the power balance. These actors will also use WMD/E for deterrence, to influence negotiations or to blackmail an adversary. Use of WMD/E is a way for actors to achieve goals when other means like political, military, or financial are not available.

## How (Ways and Means):

Having gained the capability to use WMD/E through widespread proliferation, actors can then threaten or actually conduct an attack. Actors will convert the opportunity of availability and access to these weapons and the increasing diversity in types of Weapons of Mass Destruction / Effect (e.g. atomic, chemical, biological, and cyber) as the means to empower weak actors.

## Where:

WMD/E attacks will target overcrowded urban areas; critical infrastructure, water and food supplies, as well as communication nodes. These attacks may impact or threaten populations within regions of significant political tension. However as a tool for changing the balance of power, the attackers are more likely to target regions of established low political tension to create widespread chaos that will result in new governments.

## What is new in 2030?

Due to globalisation and technological proliferation, actors will have far greater access to WMD/E technology and the ability to rapidly transmit the weapon components anywhere. The high speed of movement of any contagion, especially within urban areas, will greatly increase the appeal of megacities as a target for biological attack. The increased access to WMD/E technology within the commercial sector greatly improves the ability of radical and extremist groups to use WMD/E. Computer networks and the near total interconnectedness of all things will increase the ability of actors to execute a WMD/E attack via networks.
Annex C

Common Challenges Derived From Strategic Foresight Analysis and the Instability Situations

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, and 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:

(1) Greater proliferation of WMD/E will increase the difficulty in preventing their use.

(2) Area access and denial capabilities will increase in range and lethality.

(3) 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.

(4) 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 mega-cities 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.