FFAO Workshop Read-Ahead Material

1. **CORE DOCUMENTS**

    - Framework of Future Alliance Operations (FFAO) 2015 Report,

    - Lucerne Workshop Final Report,

    - Bydgoszcz Workshop Final Report,

    - Rome Workshop Final Report,

    - FFAO 2018 - Working Draft (Attached).

    The core documents are available at our [future work website](http://www.act.nato.int/futures-work) (http://www.act.nato.int/futures-work)

SUMMARY OF THE ROME WORKSHOP FINDINGS

2. The FFAO workshop at the NATO Defence College (NDC) in Rome consisted of over 115 participants from NATO organizations, NATO and Partner Nations, NATO Centres of Excellence, academia, industry, and other key stakeholders in the community of interest. Syndicate discussions made solid progress on improving Chapter 2 of the FFAO. Major take-aways from the session are as follows:

    - Overall, although the concept of a central idea was largely accepted, the FFAO should keep the idea of a simple list of Strategic Military Perspectives (SMPs) to stay consistent with the previous version of the FFAO. The FFAO needs to keep the ideas discussed in the tenets and enabling elements but keep them in the background with the SMPs as the big message of the FFAO.

    - The FFAO should increase the emphasis on strategic communication, operating and adapting at the same time, innovation, adaptability, being multipurpose by design and the ethical questions.

    - The syndicates discussed at great length idea of "federation" as a key and persistent characteristic of the future force. Many syndicates felt that the term federated itself is not clearly understood and we need to clearly and succinctly define what we mean by the word. Other words discussed as possibilities to use instead were "cooperative," "networked," "synchronized," or "integrated." Despite how the FFAO

addresses it the document should clearly and succinctly define how we are using the word (see next bullet).

- The syndicates developed a draft definition of federation for consideration during the workshop as follows: Efforts to enhance strategic awareness to leverage and explore options via dialogue, linkages, synchronization, deconfliction and collaboration with a broad cross-section of stakeholders (both internal and external, without ceding autonomy) to promote a unity of effort and efficiency to achieve a well-defined end-state.
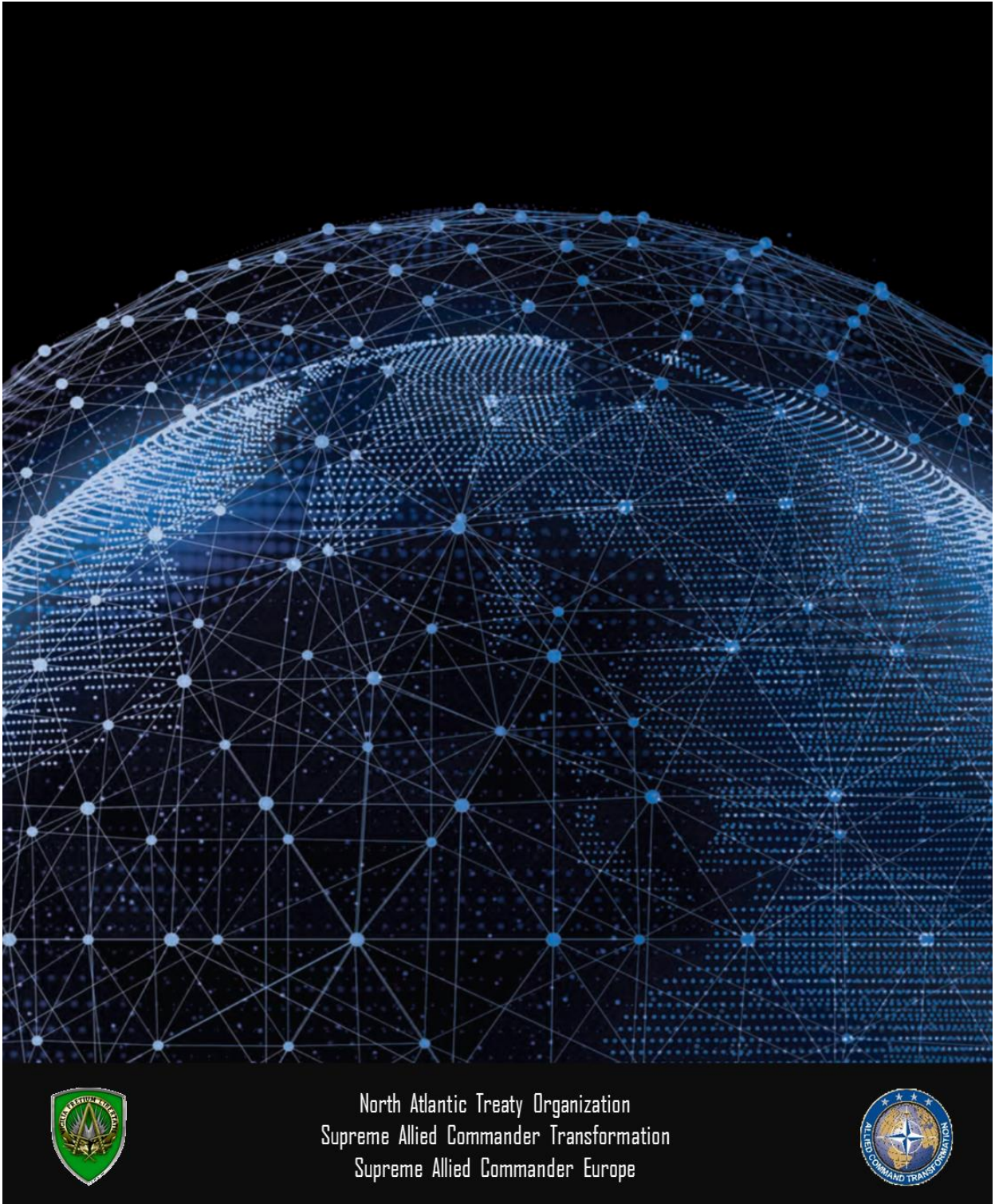
STAVANGER WORKSHOP OVERVIEW

3. The FFAO workshop will be a three-day working-level event held at the Joint Warfare Centre in Stavanger, Norway. The first day will begin with a large group plenary for introductory remarks, discussion of workshop concept and objectives, and survey results. Then the workshop participants will be broken down into small syndicates for detailed group work to discuss selected topics concerning to address the core question: In 2035 and beyond, what abilities will NATO forces require in the areas of prepare, project, engage, sustain, C3, protect, and inform in order to accomplish NATO core tasks? Following the discussions the first day, the workshop participants will be invited to attend a brief icebreaker event.

4. The second day of the workshop will begin with a large group plenary session on STO Technology Trends. Following this session, participants will break into groups for continued syndicate work. Day three will consist of continued syndicate work, with out-briefs commencing after lunch in a large group plenary session. Closing remarks from senior leaders present will conclude the workshop session on day 3.

DELIVERABLES

5. The primary deliverables for this conference are recommended changes to the draft Chapter 3 of the FFAO. Following the conference, Chapter 3 of the FFAO will be finalized and submitted through the official staffing process for adjudication and approval.

Framework for Future Alliance Operations

North Atlantic Treaty Organization
Supreme Allied Commander Transformation
Supreme Allied Commander Europe

Foreword - PLACEHOLDER

For almost 70 years, NATO forces have helped provide security and stability for an often unsecure and unstable world. It is impossible to predict the future, but as we look to the horizon today, we see more uncertainty and challenges. We should take an active role and do our best to influence the future, as it will be the legacy we leave behind. Simply put, we should do what we can today to help the next generation uphold and defend the core values that we hold dear as an Alliance. This is our shared responsibility and one we should not take lightly.

As NATO prepares its forces to meet future challenges, the Alliance should assist Nations in the continuous improvement of military structures and capabilities. This document helps us think clearly about opportunities to improve NATO's defence and deterrence posture to ensure it remains continuously proactive, ready and responsive. Perhaps most importantly, this document also describes how NATO's military forces can keep the edge and retain the ability to defeat our enemies on the battlefield of the future.

We would like to express our personal thanks to all that provided their wise counsel, including Nations, Alliance leadership, commands, Centres of Excellence, industry, academia, think tanks and all others who supported this effort. Thank you!

Curtis M. Scaparrotti
General, U.S. Army
Supreme Allied Commander
Europe

Denis Mercier
General, French Air Force
Supreme Allied Commander
Transformation

Table of Contents

Executive Summary

1. Today, the Alliance military forces face a challenge in that they should adapt, evolve and innovate to meet an ambiguous, complex, and rapidly changing security environment. To help inform the discussion options on how best to transform, this document seeks to identify the abilities of a future Alliance pool of forces to meet the potential demands of the security environment today through the foreseeable future, 2035 and beyond.

2. Overall, the future security environment through 2035 and beyond will likely be increasingly complex and both present challenges and offer opportunities to NATO's military forces. The analysis of the future security environment indicates that NATO military forces will likely face challenges that could unfold in exponentially accelerated and increasingly complex fashion. A wide variety of drivers could lead to instability situations resulting in the Alliance's decision to employ military forces. NATO military forces will need to apply the existing tenets of the law of armed conflict in new contexts, including emerging areas of ethical concern (e.g., human enhancement, cyber, automation/artificial intelligence, and blurring lines between combatants and non-combatants). However, there are many opportunities that NATO military forces could seize in the future, including building and strengthening relationships, addressing emerging challenges, capitalising on innovative technology and ideas to maintain the military edge, and understanding and influencing the human aspects of conflict.

3. To keep the operational edge today and in the future, NATO joint forces and partners continually evolve, adapt, and innovate to improve their ability to act together comprehensively across all domains to communicate and achieve the political –military objectives of the Alliance. As such, the strategic commanders recommend NATO develop forces that are credible, federated, aware, agile and resilient.

4. There are many abilities that NATO may require to accomplish its core tasks in the future. Military Implications are best military advice intended to inform Alliance transformation, including the development of policies, long-term requirements, and capabilities. Military Implications are not defined requirements, nor are they expressed as required capabilities. Alliance and Member Nations may take into account these long-term abilities during defence planning. In the future the core abilities NATO may require fall into the areas of: prepare; project; engage; sustain; command, control, and consult (C3); protect; inform.

Introduction

Background

6. Long-term military transformation is the process for anticipating and preparing for the future security environment. Using the Strategic Foresight Analysis (SFA) reports as its foundation, this document proposes how Alliance forces might plan to transform and recommends abilities that these forces may need to develop over the next 15 years. The Strategic Commands completed the first edition of this document in 2015. The Military Committee noted that the Framework for Future Alliance Operations (FFAO) could be used to inform the NATO Defence Planning Process and be taken into consideration by defence planners to expand the NDPP into the long-term. The Military Committee also concluded that the next iterations of the SFA and the FFAO should be developed in time to inform all steps of the following cycles of the NDPP and taken into account in the development of the Military Committee's input to the political guidance. The North Atlantic Council noted this on November 20, 2015.[1]

Problem Statement

7. The Alliance's military forces should operate today while adapting to meet an ambiguous, complex, and rapidly changing security environment.

Aim

8. To identify characteristics and abilities of a future Alliance pool of forces to meet the potential demands of the future security environment today and in the foreseeable future through 2035 and beyond.

Scope

9. This document is updated on a four-year cycle in concert with the NATO Defence Planning Process to provide an informed perspective of the challenges and opportunities facing the Alliance forces in the decades to come. It is intended to inform National defence planning; strategic discussions and white papers; NATO defence planning; capability development; concept development; and doctrine, training, exercises,

---

[1] MCM 0199-2015, Military Committee Advice on the Utilisation of the Framework for Future Alliance Operations; PO(2015)0624 North Atlantic Council Notation.

leadership, and education. Currently, countries report using this document to inform:

a. Assessment of the future operating environment and security situation

b. Development of national security and strategy documents

c. Capability and concept development

d. Defence planning and scenario development

e. Career courses, leadership, education and development

10. Overall, this is a strategic level document, and although it will discuss abilities NATO forces may require in the future, it is not intended to constrain NATO's decision making, National-defence planning, nor detailed capabilities development efforts. Of note, this document is unclassified and disclosed to the public to stimulate discussion and debate.

Figure 1. ACT's Long-term Military Transformation Process

11. This document provides Bi-Strategic Command's best military advice, focused on both challenges and opportunities for the Alliance. This document represents an analysis and assessment on the plausible aspects of the future security environment and is not intended as an intelligence estimate. This document is intended to complement rather than compete with other products developed by NATO and countries.

12. In development of FFAO 2018, the goal was to retain the best parts of the FFAO 2015 but expand analysis into new areas both adding depth and relevance, to describe current thinking on the military implications of the future security environment.

Key Assumptions

13. This document is intended for multiple audiences and may affect audiences outside of NATO. In addition, NATO's foundational documents will remain unchanged. The SFA and other references used in development of this document are assumed as valid indicators of the future. Finally, due to the nature of forecasting, it is important to note that the future security environment is inherently complex and continually changing and therefore, as the future unfolds, further work is necessary to continually refine this document and challenge the conclusions herein.

Method

14. ACT developed this document in concert with ACO as a Bi-Strategic Command effort. The project used a qualitative, focus-group methodology that brought together subject matter experts through a series of workshops and independent reviews, including experimentation. This project included subject matter experts from: (a) NATO Command and Force Structure, (b) Nations and Partner Nations, (c) NATO Accredited Centres of Excellence, (d) intergovernmental organisations and non-governmental organisations, (e) academia and think tanks, and (g) industry. ACT staffed this document through representatives of all Nations and all appropriate NATO bodies, including their input and recommendations as appropriate.

Chapter 1

The Future Security Environment through 2035 and Beyond

15. The Strategic Foresight Analysis and other futures documents describe the future security environment as dynamic, ambiguous, and uncertain. Globalisation and technology are expected to provide many opportunities and risks. The increasing interdependency amongst countries has potential to create stability in the long-term. However, the ongoing move from a unipolar to a multipolar and multi-dimensional world has created instability that is likely to continue or even escalate.[2]

16. Cultural, ideological and religious divides between and within societies and social inequality have the potential to promote the growth of extremist, radicalised groups. In the future, today's global terrorist threat may become decentralised and diffuse creating long-term consequences for global peace and stability.

17. Climate change is likely to increase instability globally and compound these effects. The global economy is changing, with power shifting from the West to other regions. Additionally, economic power is shifting regionally and away from the nation-state system.[3] Advances in technology and the worldwide sharing of ideas and ideologies, research and education, supported by social media, big data, and artificial intelligence (AI) are converging and thereby accelerating the scale, scope, and rate of

---

[2] NATO-ACT, *Strategic Foresight Analysis 2015 Update Report*, http://www.act.nato.int/strategic-foresight-analysis-2015-report, (November 2, 2016); NATO-ACT, *Strategic Foresight Analysis 2013*, http://www.act.nato.int/futures-ws-1 (November 2, 2016); NATO-ACT, *Strategic Foresight Analysis 2017,* Currently Under Development.
1 John Browne, "The Role of Multinational Corporations in Economic & Social Development of Poor Countries: Leading Toward a Better World?" Science Direct,
http://www.sciencedirect.com/science/article/pii/S1066793802000659?np=y. (November 2, 2016).

change. This will test the ability of military forces to adapt to the challenges of a rapidly changing global security environment.

Future Challenges

A Rapidly Changing Security Environment

18. In the study of war and armed conflict, there are some factors that change over time and some that remain the same. By its nature, armed conflict has always been a contest of wills driven by fear, honour and interest.[4] War remains a phenomenon where three key factors interact: (1) primordial violence, hatred, and enmity; (2) the play of chance, fog, and friction, and (3) its use for political purposes.[5] However, as evidenced by current threats involving non-state actors, each instance of armed conflict is different from the last as the character of conflict changes over time. Factors such as technological advances, new operating concepts, changes in the security environment, and shifts in the geopolitical landscape will greatly influence the security environment of the future.[6]

19. Since its founding, NATO has seen many shifts in the character of armed conflict. Although it is impossible to determine with absolute certainty what conflict will be like in the future, analysis of trends of the past and present indicate that conflict in the future may be characterised by:

   a. An increasing pace of the emergence and escalation of armed conflict.

   b. Greater complexity of armed conflict where the dense linkages between populations might result in cascading instability and gray zones which blur the lines between military and non-military aspects of conflict.

   c. Increased interconnectivity across the operating environment and the domains of warfare (air, land, sea, cyber) and space and strategic communications.

   d. A compression of the traditional levels of war where strategic, operational, and tactical events become difficult to differentiate.

---

[4] Thucydides, *History of the Peloponnesian War,* http://www.gutenberg.org/files/7142/7142-h/7142-h.htm, (November 2, 2016).

[5] Carl von Clausewitz, *On War* (Princeton; Princeton University Press, 1984).

[6] Colin Gray, "War – Continuity in Change, and Change in Continuity," *Parameters*. http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/2010summer/gray.pdf, (November 2, 2016). NATO-ACT, *FFAO Bydgoszcz, Poland Conference Report 2016,* http://www.act.nato.int/futures-ws-5, (November 2, 2016).

e. Rapidly emerging technologies in areas such as cyber, autonomous systems, robotics, hypersonic weapons, digital data, artificial intelligence, communication, surveillance, electronic warfare.

f. Increased likelihood of human enhancement through mechanical and biological means to improve military performance and the increasing importance of the human-machine interface.

g. The increased use of automated systems in warfare and eventually some military operations may not directly involve humans in the decision cycle.

h. Smaller numbers of forces may fight over greater distances.

i. New classes of weapons of mass destruction / effect may emerge.

j. Increased numbers of sensors and the ubiquitous "internet of things" could influence operational security and increase the impact of social media on the battlefield.

k. An increase in the likelihood of armed conflict involving global commons, space, densely populated areas and subterranean areas.

l. Widely accessible and cheaper technologies and the increasing role of individuals that could produce uncontrolled and hard to predict effects.

m. Increased access to knowledge could enhance and speed up the emergence and mobility of threats. This will likely include an increase in use of innovative ways and means to exploit the weaponization of information activities to influence populations alone or in support of armed conflict.

n. Increasing overlap between criminal activity and war / armed conflict.[7]

Future Instability

20. Instability is a state of likely change.[8] Not all instability in the security environment will result in a need and decision by the Alliance to employ military forces. To focus on the specific operational impacts on NATO's

---

[7] NATO-ACT, *FFAO Bydgoszcz, Poland Conference Report 2016*, http://www.act.nato.int/futures-ws-5, (November 2, 2016).

[8] Merriam-Webster, "Simple Definition of Instability," http://www.merriam-webster.com/dictionary/instability, (November 2, 2016).

military forces in the future, it is critical to clearly define and differentiate between instability drivers and instability situations.

21. Instability drivers are defined as any conditions, events, or circumstances that increase the tendency for the security environment to be unpredictable, changeable, or erratic. Some instability drivers are slow-emerging, underlying conditions that lead to unstable situations progressively over time. Others may act as catalysts that quickly change the security environment. For example, climate change, mass migration, and competition for resources may cause instability, as might differences in beliefs, values systems, and disruptive technologies. Disintegrating political, economic, rule of law, social systems and increasing population density could further complicate the security environment. Arguably, the greatest drivers of instability are the activities of hostile state and non-state actors.[9] Such activities span a wide range, from isolated terrorist attacks, continued nuclear proliferation to the escalatory use of force.

22. Instability situations are defined as generic descriptions of possible future events of critical significance that could reach the threshold requiring the Alliance's use of military forces.[10] Instability situations are not mutually exclusive and could occur in isolation or at the same time as others, resulting in a compounded effect, or hyper-instability. In the future, there exists a wide range of instability situations, including:

   a. **Weapons of Mass Destruction/ Effect (WMD/E) Use**: Hostile state and non-state actors could seek access to, and use WMD/Es to cause widespread devastation and loss of life against targets such as political leadership, population concentrations, the global financial system, or locations of symbolic importance.[11] This could include Chemical, Biological, Radiological, or Nuclear (CBRN) or weapons of mass destruction based on new technologies.

---

[9] NATO-ACT, *FFAO Bydgoszcz, Poland Conference Report 2016*, http://www.act.nato.int/futures-ws-5, (November 2, 2016).
[10] NATO-ACT, *FFAO Bydgoszcz, Poland Conference Report 2016*, http://www.act.nato.int/futures-ws-5, (November 2, 2016).
[11] UN, "Weapons of Mass Destruction: Threats and Responses,"
http://www.un.org/sustainabledevelopment/blog/2015/01/weapons-of-mass-destruction-threats-and-responses/, (November 2, 2016); NATO, *AAP-6 Edition 2015*, https://nso.nato.int/nso/sPublic/ap/aap6/AAP-6.pdf, (November 2, 2016).

INSTABILITY SITUATIONS

- **WMD/E Use**
- **Conventional War**
- **Escalatory Use of Force**
- **Hybrid War**
- **Irregular War**
- **Terrorist Activities**
- **Global Commons Disruption**
- **Critical Infrastructure Attack**
- **Information Warfare**
- **Cyberattack**
- **Governance Challenges**
- **Endangerment of Civilian Populations**
- **Pandemic Disease**
- **Natural/Man-made Disasters**

b.   **Conventional War:** State-on-state war between conventional forces will remain within the realm of the possible. This could include two or more states in open confrontation where the forces on each side are well defined and fight using weapons that primarily target the opponent's military.[12]

c.   **Escalatory Use of Force:** Hostile actors may use threats or the use of force increasingly over time that destabilises the security environment. This could lead to a strategic miscalculation or increase the likelihood of a wider conflict.[13]

d.   **Hybrid War:** Hostile state actors will likely use a combination of conventional and unconventional means to avoid being held directly accountable for their actions while retaining the option to employ conventional forces, if directly threatened. One of the major characteristics of hybrid warfare is that it often aims to leverage all elements of power while limiting the conflict below the threshold of conventional war thus complicating the timely and effective use of rigid collective defence mechanisms.[14]

e. **Irregular War:** A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). This can include military activities conducted through or with underground, auxiliary or guerrilla forces to enable a resistance movement or insurgency to coerce, disrupt or overthrow a government or occupying power.[15] In these types of conflicts, propaganda could be used in an attempt to influence populations.

---

[12] David Barno and Nora Bensahel, "The Irrelevance of Traditional Warfare?" *War On the Rocks,* http://warontherocks.com/2015/01/the-irrelevance-of-traditional-warfare/, (November 2, 2016).

[13] ICRC, *Violence and the Use of Force*, https://www.icrc.org/eng/assets/files/other/icrc_002_0943.pdf, (November 2, 2016).

[14] NATO, International Staff Memo, IMSM-0043-2016, (January 15, 2016).

[15] NATO, *AAP-6 Edition 2015*, https://nso.nato.int/nso/sPublic/ap/aap6/AAP-6.pdf, (November 2, 2016).

f. **Terrorist Activities:** In the future, non-state actors may unlawfully use or threaten the use of force and violence against individuals or property at an increased scale, scope or duration in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives. Terrorism can be used to create fear or terror in an attempt to gain control over the population. Additionally, hostile states will likely continue to use proxies that employ terrorism to further their own interests.[16]

g. **Global Commons Disruption:** Hostile actors may directly challenge international laws and norms in the global commons through threat or use of force.[17] Increased resource competition and commercialisation of space may lead hostile actors to challenge international treaties in new ways. Additionally, space disruption could be executed by kinetic or non-kinetic means, such as direct attack, jamming or cyberattacks.[18]

h. **Critical Infrastructure Attack:** Physical and virtual infrastructure nodes and installations remain essential to the enduring interests of the Alliance (e.g. energy facilities, ports, internet infrastructure, etc.). Hostile actors could attack these nodes in an attempt to disrupt vital societal functions and global stability.[19] This could also include an attack to deny the electromagnetic spectrum, position navigation and timing, radar, and other key systems. Such attacks can occur as physical attacks or in the form of cyber-attacks.

i. **Information Warfare:** When hostile actors deliver messages, themes and narratives to shape decision makers perceptions and lead them towards a choosing a certain course of action. Often, the aspiration of information warfare is to challenge the unity of target societies by disguising real goals externally, while at the same time, strengthening cohesion internally. To pursue information warfare, there are various

---

[16] Melissa Clarke, "Globally, Terrorism is on the Rise," *ABC News*, http://www.abc.net.au/news/2015-11-17/global-terrorism-index-increase/6947200 (November 2, 2016).; NATO, *AAP-6 Edition 2015*, MC-472/1 "Military Committee Concept on CT", endorsed by MC and approved by NAC, December 2015) https://nso.nato.int/nso/sPublic/ap/aap6/AAP-6.pdf, (November 2, 2016), Institute for Economics and Peace, Global Terrorism Index 2015, November 2015, http://economicsandpeace.org/wp-content/uploads/2015/11/2015-Global-Terrorism-Index-Report.pdf; NATO, PO(2015)0045, (November 2, 2016).
[17] Gerald Stang, *Global Commons: Between Cooperation and Competition*, http://www.iss.europa.eu/uploads/media/Brief__17.pdf, (November 2, 2016).
[18] Lee Billings, "War in Space May Be Closer than Ever," *Scientific American*, https://www.scientificamerican.com/article/war-in-space-may-be-closer-than-ever/, (November 2, 2016).
[19] Sarah Kuranda, "Experts: Recent Critical Infrastructure Attacks a Sign of Major Security Challenges Coming in 2016," *CRN*, http://www.crn.com/news/security/300079278/experts-recent-critical-infrastructure-attacks-a-sign-of-major-security-challenges-coming-in-2016.htm, (November 2, 2016).

channels that a hostile actor can employ (e.g., cyber, print, television, radio, multimedia, etc.) and categories of information (e.g., false, half-true, true) to propagate a storyline that furthers the achievement of their political-military objectives.

j. **Cyberattack:** Hostile actors could conduct a cyberattack of significant scale, scope or duration to disrupt, deny, degrade, modify, steal, or destroy information resulting in a large physical, emotional or financial impact.[20] Hostile actors could use cyberattacks in isolation or in support of conventional, hybrid, or unconventional approaches.

k. **Governance Challenges:** Some governments may fail to provide administration and basic functions that could threaten internal and external security and destabilise the environment. Furthermore, ungoverned spaces may exist where there is no legitimate rule of law resulting in a security vacuum and increasing the chance of armed conflict. Additionally, the future migration and population flows could contribute to the emergence of governance challenges.

l. **Endangerment of Civilian Populations:** There exists the potential for hostile actors to conduct large-scale acts of violence directed against civilian populations. These events could include mob violence, post-conflict revenge, insurgency, predatory violence, communal conflict, government repression, ethnic cleansing, destruction of cultural property and genocide.[21]

m. **Pandemic Disease:** There exists the possibility of an outbreak of a disease that occurs over a wide geographic area and affects an exceptionally large proportion of the population exceeding response capacity.[22]

n. **Natural/Man-made Disaster:** There is the possibility of a sudden large-scale man-made or natural event that could result in serious damage, widespread death, and injury that exceeds response capacity. These events could occur as a culmination of several smaller individual

---

[20] Jason Healy, *The Five Futures of Cyber Conflict,* http://journal.georgetown.edu/wp-content/uploads/2015/07/110_gj124_Healey-CYBER-20111.pdf, (November 2, 2016).
[21] Stian Kjeksrud, Alexander Beadle, and Petter Lindqvist, *Protecting Civilians from Violence,* https://www.ffi.no/no/Publikasjoner/Documents/Protecting-Civilians-from-Violence.pdf, (November 2, 2016). NATO Policy for the Protection of civilians http://www.nato.int/cps/en/natohq/official_texts_133945.htm?selectedLocale=en (July 9, 2016)
[22] Regina Parker, "Prevent Disease to Prevent War," *The Strategy Bridge*, http://www.thestrategybridge.com/the-bridge/2016/10/6/prevent-disease-to-prevent-war, (November 2, 2016).

disasters in a way that may have an effect similar to a large-scale disaster.[23]

Ethical Challenges

23. Numerous ethical questions arise that should be discussed today so that military forces are prepared for the future and that new international laws are developed if required.[24] The primary question that NATO should continually address is: Based on the rapidly changing character of conflict and the potential instability situations, how do forces apply existing tenets of the Law of Armed Conflict (e.g., distinction, proportionality, military necessity, prevention of unnecessary suffering, etc.)?[25] Some of the specific questions of the future could include the following:

  a. **Human Enhancement:** Should forces use emerging human enhancement techniques to enhance the military effectiveness and efficiency of the Alliance? If so, how? How does human enhancement align with NATO's core values? Conversely, how can forces fight and defeat adversaries that use advanced human enhancement techniques? What responsibility does the military have to reintegrate service members following enhancement and return to civilian life?[26]

  b. **Autonomous Systems, Artificial Intelligence, Cyber and Other New Technologies:** How should forces use lethal autonomous systems and artificial intelligence in the future, alone or integrated with traditional systems? To what degree will NATO accept the use of autonomous systems in the future? How do forces address adversaries that use lethal autonomous systems? How do forces utilise the electromagnetic spectrum to achieve the desired political ends? In the cyber domain, what constitutes an attack that would warrant a military response? How far should forces pursue offensive cyber capabilities as an Alliance? How do forces balance personal privacy with the need for timely

---

[23] Peter Baxter, "Catastrophes – Natural and Manmade Disasters," *Conflict and Catastrophe Medicine*, http://link.springer.com/chapter/10.1007%2F978-1-4471-0215-1_3, (November 2, 2016).

[24] St. Anne's College, Human Enhancement and the Law Regulating for the Future, https://www.law.ox.ac.uk/sites/files/oxlaw/field/field_document/human_enhancement_programme_-_final.pdf, (January 24, 2017); The Royal Academy of Engineering, Autonomous Systems: Social, Legal and Ethical Issues, http://www.raeng.org.uk/publications/reports/autonomous-systems-report, (January 24, 2017); Phillip W. Gray, Weaponised Non-Combatants: A Moral Conundrum of Future Asymmetrical Warfare, http://www.tandfonline.com/doi/citedby/10.1080/15027570.2014.975009?scroll=top&needAccess=true, (January 24, 2017); ICRC, What limits does the law of war impose on cyber attacks?, https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm, (January 24, 2017)

[25] NATO-ACT, *FFAO Bydgoscs, Poland Conference Report 2016*, http://www.act.nato.int/futures-ws-5, (November 2, 2016).

[26] Ibid.

intelligence? How do forces find the right balance between information security and the need for transparency?[27]

c. **Combatants and Non-Combatants:** In the future, the lines between combatants and non-combatants may blur even more. If so, how do forces deal with this? What capabilities do forces need to separate combatants from non-combatants in congested high-population areas? How do forces deal with child soldiers on the battlefields of the future? How do forces address civilian corporations that provide defence services in combat areas in the future? How do forces address a future where non-combatants can become combatants at any moment? How will adversaries exploit traditional safe or neutral zones (e.g., schools, hospitals, etc,) to protect their forces as well as increase the likelihood of civilian casualties and negative strategic communications impact on the Alliance?[28]

Future Opportunities

24. Despite the many challenges anticipated in the future security environment many there are many opportunities that NATO forces could seize upon to improve the security environment.[29] Innovation and technological changes during this period will offer military advantages that NATO forces or adversaries could seize upon. Innovation is not only the adoption of new technologies but includes the combination of old technologies in novel ways. In this period, developments are likely to be the greatest in five broad areas, or BRINE: (1) biology, biotechnology and medicine; (2) robotics, artificial intelligence, new smart weapons, and human enhancement; (3) Information and Communication Technology (ICT), surveillance and cognitive science; (4) nanotechnology and

---

[27] Ibid.

[28] Ibid.
[29] Ibid.

advanced materials; and (5) energy technology. These developments could have an impact on organisational structures, culture, and processes.[30] Although states will continue to develop new technologies, in many areas, the greatest advances will likely come from civilian entities. As such, relationships with academia and industry may become more critical to maintain the military advantage. Additionally, the Alliance has an opportunity to harness the creative thinking of its forces and society to develop innovative solutions to problems. The key here is experimentation and the ability to embrace failure as way to learn and grow.[31]

25. Increased interconnectedness and globalisation offers military forces new opportunities to build and strengthen relationships.[32] By taking a proactive stand towards achieving increased partnership and cooperation forces could better address emerging multidimensional threats.[33] To help balance hard and soft power, military forces should also improve upon their ability to coordinate a wide network of trusted relationships and partnerships with other international organisations around the globe. This would serve to increase situational awareness, to help ensure regional security, deter conflict, and deescalate conflict situations.[34]

26. Increased complexity, rapid changes in the security environment, and advances in awareness may create opportunities for military forces to address challenges and provide a stabilising presence in an unstable world. The capacity of military forces to respond to global events in a timely manner enables management of emerging issues that pose a threat to the security of territory and populations. Military forces may also have more opportunities to engage in a wide array or activities, deter and prevent conflicts, or help resolve conflicts, all of which could change the future security environment for the better. Additionally, NATO forces in the future may find themselves in a supporting role to assist non-traditional partners in addressing the root causes of instability.[35]

27. NATO Forces will likely have many opportunities in the future to help impact the human aspects of conflict. NATO forces will be able to seize upon these

---

[30] Ibid.
[31] Ibid.
[32] NATO-ACT, *Strategic Foresight Analysis 2015 Update Report,* http://www.act.nato.int/strategic-foresight-analysis-2015-report, (November 2, 2016); NATO-ACT, *Strategic Foresight Analysis 2013,* http://www.act.nato.int/futures-ws-1 (November 2, 2016); NATO-ACT, *Strategic Foresight Analysis 2017,* Currently under Development.
[33] NATO-ACT, *FFAO Bydgoszcz, Poland Conference Report 2016,* http://www.act.nato.int/futures-ws-5, (November 2, 2016).
[34] Ibid.
[35] Ibid.

opportunities if they are able to develop and adopt a mind-set that recognizes that, even in our technological age, war is primarily a human endeavour. Properly cultivated and applied, this mind-set could serve to improve how the forces visualize the environment and interact with relevant actors within the context of the situation.[36]

Conclusion

28. Overall, the future security environment through 2035 and beyond will likely be increasingly complex both present challenges and offer opportunities to NATO military forces. The analysis of the future security environment indicates that NATO military forces will likely face challenges that could unfold in exponentially accelerated and increasingly complex fashion. A wide variety of drivers could lead to instability situations resulting in the Alliance's decision to employ military forces. NATO military forces will need to apply the existing tenets of the law of armed conflict in new contexts, including emerging areas of ethical concern (e.g., human enhancement, cyber, automation/artificial intelligence, and blurring lines between combatants and non-combatants). However, there are many opportunities that NATO military forces could seize in the future, including building and strengthening relationships, addressing emerging challenges, capitalising on innovative technology and ideas to maintain the military edge, and understanding the human aspects of conflict.

---

[36] U.S. Joint Concept for Human Aspects of Military Operations, http://nsiteam.com/social/wp-content/uploads/2017/01/20161019-Joint-Concept-for-Human-Aspects-of-Military-Operations-Signed-by-VCJCS.pdf (April 10, 2017).

Chapter 2

Strategic Military Perspectives

Introduction

29. Strategic Military Perspectives are the characteristics NATO military forces should possess to address the full range of potential future instability situations as well as seize the opportunities that arise.[37]

30. NATO's fundamental and enduring purpose is to safeguard the freedom and security of all its members by political and military means. In the future, the Alliance should remain an essential source of stability in an unpredictable world, building from security to stability, and then from stability to prosperity. In the future, the Alliance will remain firmly committed to the purposes and tenets of the Charter of the United Nations, and to the Washington Treaty, which affirms the primary responsibility of the Security Council for the maintenance of international peace and security. Since the signature of the Washington Treaty in 1949, NATO has remained unified and resolute in defending its shared interests, namely:

   a. The desire to live in peace with all peoples and all governments

   b. The principles of democracy, individual liberty and the rule of law

   c. Stability and well-being in the North Atlantic area and

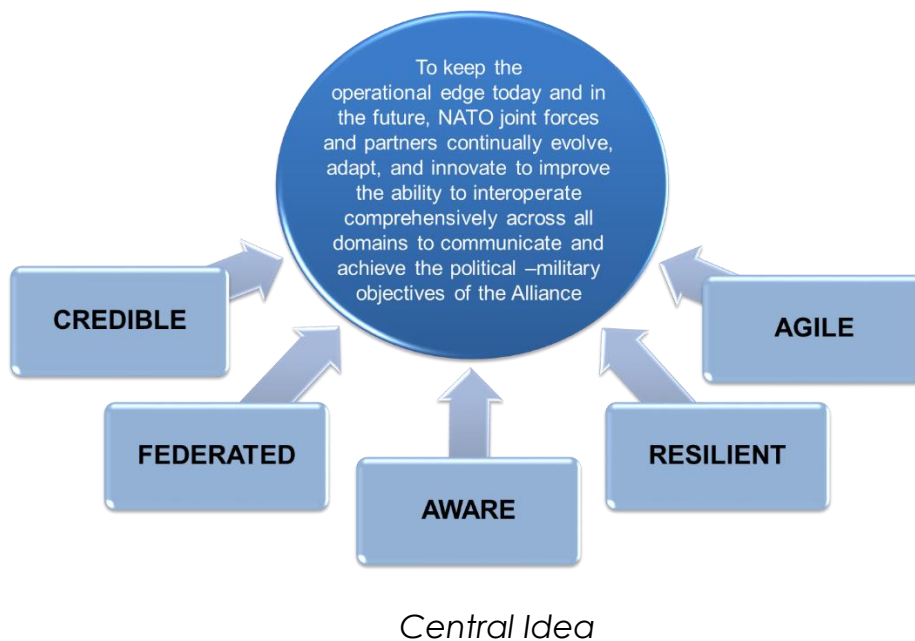   d. Collective defence for the preservation of peace and security.[38]

30. Building on this foundation, the shared political will of the Alliance directs the military instrument of power. This direction sets the level of ambition and guides the development of an overarching strategic concept, and is

---

[37] NATO-ACT, *FFAO Rome Conference Report 2017*, http://www.act.nato.int/futures-ws-5, (May 1, 2017). Please note that the entirety of this chapter was developed using the outcomes of this report unless specified otherwise with notation.

[38] NATO, *The North Atlantic Treaty 1949,* http://www.nato.int/cps/en/natolive/official_texts_17120.htm, (May 22, 2017).

described in summit declarations and other official statements. Military forces use this direction and guidance to develop operational goals and objectives. As reaffirmed by the 2016 Summit, NATO's core tasks will remain as collective defence, crisis management, and collective security executed through deterrence and defence, counter-terrorism, and projecting stability.[39]

31. As the Alliance continues to maintain its cohesion – its centre of gravity, forces will likely face the following military problem in the future: *Based on the possible instability situations in the future security environment through 2035 and beyond, what is a framework that will enable NATO military forces to accomplish the core tasks?*

Central Idea

32. NATO forces should have a common understanding of a unifying central idea that helps form a common understanding and guide actions for future force development. To keep the operational edge, today and in the future, NATO joint forces and partners should continually evolve, adapt, and innovate to improve the ability to interoperate comprehensively across all domains to communicate and to achieve the political–military objectives of the Alliance. As such, the strategic commanders recommend NATO to develop forces that are credible, federated, aware, agile, and resilient.

---

[39] NATO, *Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*, http://www.nato.int/cps/en/natohq/official_texts_133169.htm, (May 22, 2017).

Credible

31. The characteristic of credibility is defined as leaders, forces, and equipment that are recognised as possessing the ability to deter and defend against potential adversaries. In the future, the entire command structure and force structure needs to have the capability, preparedness, and readiness to defend against any threat from any direction. As a means to prevent conflict and war, credibility is an essential component to both deterrence and defence. The future security environment may require a holistic approach, spans civil preparedness and national forces as first line of defence, to cyber defence, missile defence, special operations/conventional forces, and nuclear deterrence as the fundamental guarantee of security. In the future security environment, the credibility of military forces is a critical factor in maintaining the regional and global balance-of-power.

32. In many ways, credibility can only be judged by understanding the perceptions and the actions of adversaries. How an adversary perceives the professionalism, capabilities, readiness, and lethality of military forces may determine how they may choose to act in any given situation. In the future, it is likely that adversaries may seek to exploit perceived weaknesses, whilst avoiding strengths. Therefore, the credibility of forces requires both the development and demonstration of their abilities through realistic and challenging training and exercises. In times of conflict, NATO should have the ability to rapidly deploy forces into non-permissive combat environments and achieve the political objectives the Alliance sets forth. Strategic Communication underpins credibility.   In the future, Alliance forces need to match what they do with what they say.

33. Robust military capability and capacity are indispensable elements of credibility. Without a wide-rage military capability and capacity across DOTMLPF-I, potential adversaries could judge NATO forces as weak, and may seek to take advantage of the circumstances. In addition, NATO forces should have a sufficient level of readiness to act quickly in times of crisis. Finally, if a major conflict occurs, NATO forces should have a high-level of lethality in order to produce quick and decisive operational results on the battlefield of the future and mitigate risks where possible.

Federated

34. Being federated means leveraging and exploring options via dialogue, linkages, synchronization, and collaboration with a broad community of internal and external stakeholders, with the aim to promote unity of effort and improve efficiency in achieving a well-defined operational end-state. Being federated results in increased capacities, opportunities, and influence within the security environment. By expanding the number and type of partnerships and through continuous holistic interaction, the ability and will to cooperate, coordinate, adapt and fight together improves and it will maximize the intended effect. Through persistent federation, the Alliance adds value in its ability to optimize capability and capacity, increases awareness, accelerates speed of adaptation, and improves anticipation and timely response. All that translates to a force that better addresses the drivers of conflict.

35. Federation presents an opportunity for NATO to develop formal relationships and act in concert with a variety of state and non-state actors to address future security threats holistically. It includes the ability to influence the security environment through continuous interaction via physical and virtual presence. Federation suggests cooperative, persuasive and proactive engagement with organisations and actors, both inside and outside of the Alliance, enabling forces to anticipate crises as well as leverage a wider range of capabilities. Forces should strive to work with others to address security in a more comprehensive manner while maintaining responsibility for security. Such partnerships can be temporary or enduring and could include a range of stakeholders, including those inside nations, with other intergovernmental organisations, industry, or non-governmental organisations.

36. Federation helps merge, coordinate and build upon ongoing 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, military forces 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 in building a common view of the situation might best be implemented from tactical through strategic levels.

37. Countries always retain the right to act alone, which could have an impact on the Alliance in the form of follow-on action. This requires NATO forces to be prepared to act in support of one another at any time; before, during, or after a crisis emerges. Viewing security as a federated network would build upon existing agreements and develop new relationships of varying scope. This new expanded understanding of partnerships would include pre-arranged collaboration with a large variety of actors through education, training, and exercises and would help forces improve their ability to respond to crisis or conflict. New federated relationships also require expanded strategic communication roles. In this way, federation supports the level of ambition by aligning tactical, operational, and strategic narratives from across a wide range of actors.

38. Federation also includes aspects of interoperability. In many ways, the Alliance has been building for the ability of forces to work together since its founding in in 1949. Interoperability has become even more important, and may continue to grow in importance in the future when creating federations with external partners. Interoperability is the ability to act together coherently, effectively and efficiently to achieve tactical, operational and strategic objectives. Specifically, it enables forces, units and/or systems to operate together and allows them to share common doctrine and procedures, each other's infrastructure and bases, and to be able to communicate. Interoperability reduces duplication, enables pooling of resources, and produces synergies among forces; and whenever possible with partners. One risk when working with non-traditional partners is that NATO oversteps it bounds. In the future forces must be comfortable with the fact they may not control these partners, rather coordinate activates toward a common end.

39. Interoperability does not necessarily require common military equipment. Important is that the equipment can share common facilities, is able to interact, connect and communicate, and exchange data and services with other equipment. Through its technical (including hardware, equipment, armaments and systems), procedural (including doctrines and procedures) and human (including terminology and training) dimensions, and complemented by information as a critical transversal element, interoperability supports the implementation of such recent initiatives as Smart Defence and Connected Forces. Interoperable solutions can only be achieved through the effective employment of standardization, training, exercises, lessons learned, demonstrations, tests and trials. By strengthening relationships with the defence and security industry, and by using open

standards to the maximum extent possible, forces should continue to pursue interoperability as a force multiplier and a streamliner of national efforts.[40]

Aware

40. Awareness means developing a comprehensive and accurate shared understanding of the operational environment, the adversaries, and courses of action along with likely risks and threats to enable accurate and timely decision-making. By increasing awareness, the Alliance improves cohesion through a shared assessment of current and future strategic level challenges and opportunities, and allows 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 helps prevent strategic surprise, and supports timely decision-making. By promoting a shared understanding of future challenges and opportunities, the Alliance can influence developing instability at an early stage.

41. Due to the increased ability of highly empowered individuals and small groups to threaten security, there will likely 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 Awareness. Information fusion, management and dissemination may be vital, since they are on the critical path of allowing leaders to start decision-making processes to exploit possibilities and address threats at an early stage. Sharing this achieved awareness within the Alliance is a prerequisite for timely decision-making. A comprehensive and long-term understanding of the environment and associated cultures in the areas of interest should enable forces to make more informed decisions about appropriate mitigation activities, either in the pre-crisis or subsequent phases of crisis or conflict.

42. Awareness leverages new and emerging technologies to collect, process, and analyse a vast amount of data. A shared assessment can be gained

---

[40] Ibid.

by fusing this analysis with traditional intelligence in a fusion centre. This shared assessment can increase cohesion and can be used to create an advantage that may allow improved anticipation of crises and conflicts and expand decision space for senior leaders.

Resilient

43. Resilience is the ability to retain capable forces and conduct successful operations in spite of surprise or strategic shock. 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, may demand increased resilience from Alliance forces in the future. 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.
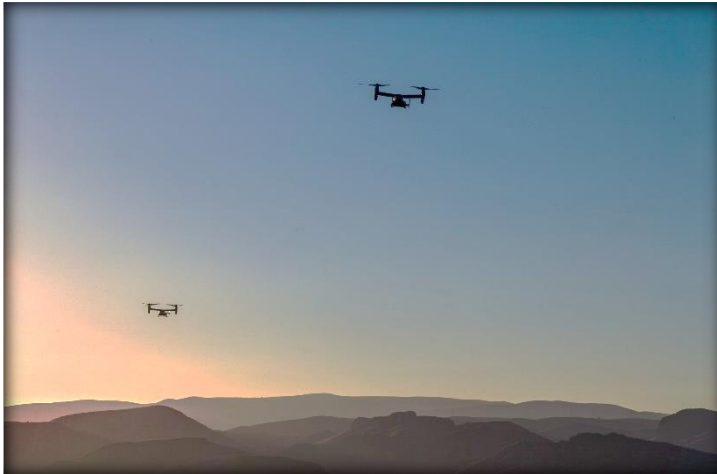

44. In the increasingly complex environment of the future, threats may be less foreseeable than they are today. Alliance planning should guard against the effects of complexity, surprise or strategic shock that might hamper forces from accomplishing operations associated with the core tasks. This level of resilience may require forces to connect with a range of different actors across the military and civil security spectrum. Under this construct for resilience, all organisations that play a role in security, stability, and safety may 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, may be important to achieve this coordinated effort.

45. Sustainment is another key aspect of resilience. Forces should possess both the capabilities to sustain 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 may be essential in this case. The Alliance may 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.

Agile

46. Agility is the ability to respond effectively to dynamic, complex and uncertain operational challenges with appropriate, flexible, and timely actions. Future NATO forces may need to be multi-purpose by design to maximize agility. Future operations may 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. Agility preserves decision space and leads to multiple creative and scalable options for decision makers.

47. 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 may be necessary in order to act boldly and decisively in a measured way to achieve advantages that maximise strategic options. Agility also requires timely decision-making by military leaders. Efficient information management, as well as a mission-command type leadership philosophy that allows decentralised, flexible decision-making within the overall commander's intent can aid this decision-making. Agility also includes the ability of leaders to understand and address complex ethical and moral questions that may arise with new technologies in the future.

48. In addition to innovative and creative leaders, the Alliance may need flexible, tailorable and robust forces. Interoperability, facilitated by the evolution of doctrine and standardisation, may be crucial for Alliance forces in the future. Forces may 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 may enhance responsiveness. Alliance forces should increase their ability to operate in complex terrain, including large networked urban areas or megacities.

49. To maximise combinations of Alliance power, nations should enhance the ability to assemble and train diverse multinational units. Recognizing that challenges may 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.

50. Agility places significant importance on the development of human capital to enhance creativity, initiative, and the ability to make timely, effective decisions that support their unit's mission. Implementing lessons learned and continual improvement is a part of agility. Agility 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. 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.

Enabling Elements

51. Key to success includes enabling elements that future forces need during operations to accomplish the core tasks and address instability in the future security environment. Even if NATO develops the perfect force for the future, without these enabling elements this force could very well fail to achieve the desired political ends.

52. One such enabling element is strong public support, which should manifest as forward-looking policies, proper authorisations, leadership and timely decision-making. Another is national civil preparedness, which will serve to make the Alliance even more resilient at home as well as abroad. Additionally, NATO requires timely and effective defence /security investment with strong ties to new concepts, innovative industry and new technology.

53. Fundamental to the internal functioning of NATO is its ability as a learning organization that acquires and manages relevant knowledge. This involves lessons observed, identified and learned, including developing standards that codify how NATO operates. In addition, in the realm of human capital, research, education and empowerment of leaders will be critical to success. This should include realistic and sufficient individual and collective training and exercises to prepare for the expected as well as the unexpected. This also requires a holistic partnership strategy as well as responsive and tailored logistics structures. Key to this is coherent and timely capability development and orchestrated and effective command, control, and consultation mechanisms.

Cohesion Factors

54. With every choice NATO makes, there is a degree of risk. In looking at the future security environment, a number of risks to the cohesion of the Alliance could emerge. A weakening or absence of a clear external threat could weaken cohesion. Additionally, internal challenges such as asymmetric burden sharing, lack of investment into the defence sector, and lack of coherent narrative on security threats could play an important role. Rigid

decision-making procedures, increased use of ad hoc coalitions, and Alliance overstretch, could arise as institutional challenges that pose risks as well. Other risks that could arise are technology and innovation challenges, which may manifest in the lack of political will to share the latest strategic technology and a differing pace of innovation among the Allies. Finally, if the core values of an individual country or countries become misaligned with the core values of the Alliance writ large, this could present a significant risk to cohesion of NATO in the future.[41]

Conclusion

55. NATO military forces should possess to address characteristics that allow them to adreess the full range of potential future instability situations as well as seize the opportunities that arise. The strategic commanders recommend that to keep the operational edge today and in the future, NATO joint forces and partners continually evolve, adapt, and innovate to improve the ability to interoperate comprehensively across all domains to communicate and achieve the political–military objectives of the Alliance; as such, NATO countries should develop forces that are credible, federated, aware, agile and resilient.

---

[41] This is a draft section and will be developed further though the FFAO innovation hub project and modified accordingly.
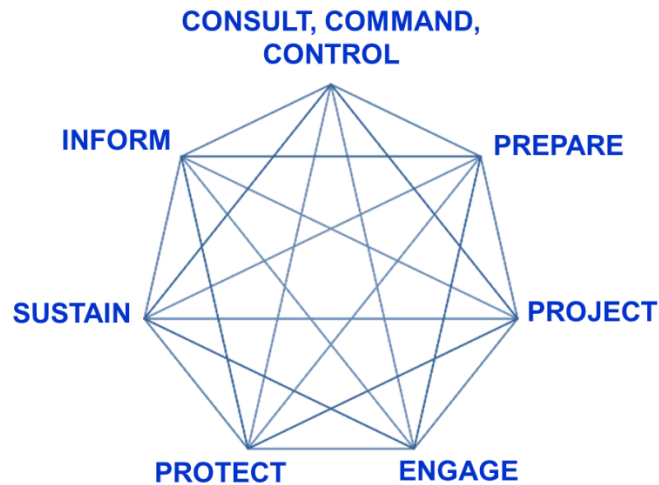
Chapter 3

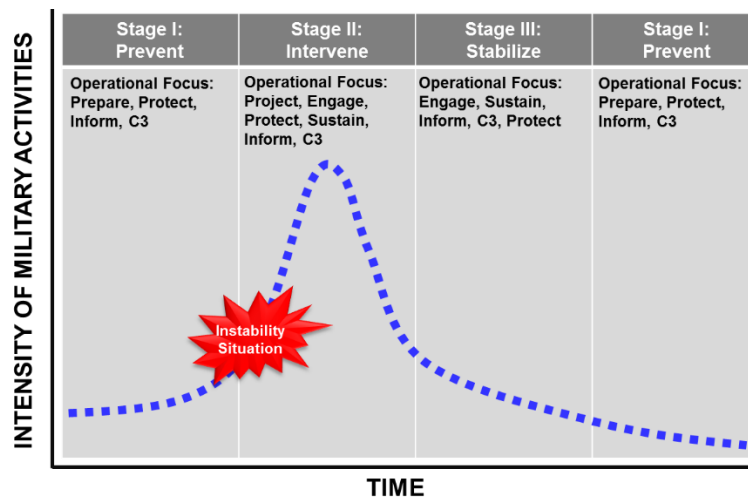# Military Implications

Introduction

56. This chapter provides military-specific deductions, expressed as abilities that NATO may require to accomplish its core tasks in the future. Military Implications are best military advice intended to inform Alliance transformation, including the development of policies, long-term requirements, and capabilities. Military Implications are not defined requirements, nor are they expressed as required capabilities. Alliance and Member Nations may take into account these long-term abilities during defence planning. In the future the core abilities NATO may require fall into the areas of:

   a. Prepare – The ability to establish, prepare and sustain sufficient and effective presence at the right time, keeping sufficient flexibility to adapt to possible changes in the strategic environment.

   b. Project – The ability to conduct strategic (re)deployment and RSOI of both NATO and national headquarters' forces in support of Alliance missions.

   c. Engage – The ability to perform the tasks which contribute directly to the achievement of mission goals, including all abilities required to defeat adversaries.

   d. Sustain – The ability to plan and execute the timely logistical support of forces.

   e. Command, Control, and Consult (C3)- The ability to exercise authority over and direct full spectrum of assigned and attached forces in the accomplishment of the mission.

   f. Protect – The ability to minimise the vulnerability of personnel, facilities, materiel and activities, whilst ensuring the Allies freedom of action and contributing to mission success.

   g. Inform – The ability to establish and maintain the situational awareness and level of knowledge required to allow commanders at all levels to make timely and informed decisions.

Core Abilities

57. In general, NATO military operational activities fall into the NATO capability heirarchy areas across the curve of militiary intervention. On a continual basis, forces are preparing, protecting, informing and performaning command, control, and consult functions. In times of crises, the political decisions of the Alliance could lead to a change in focus resulting in the need to project, engage, and sustain military forces in order to accomplish the desired political ends. Some members or partners may decide to act unilateraly or bilateraly as first responders to crisis. NATO forces should remain flexible and retain the ability to integrate abilities and activities seamlessly with those of other countries based on the context of the situation.
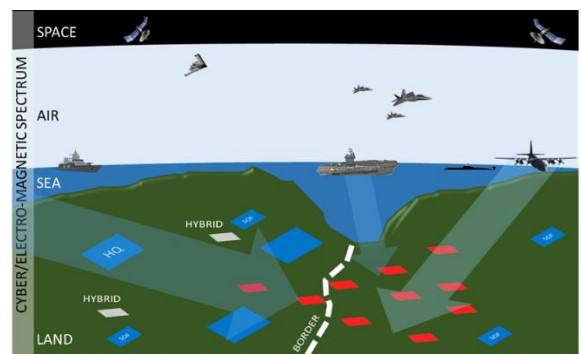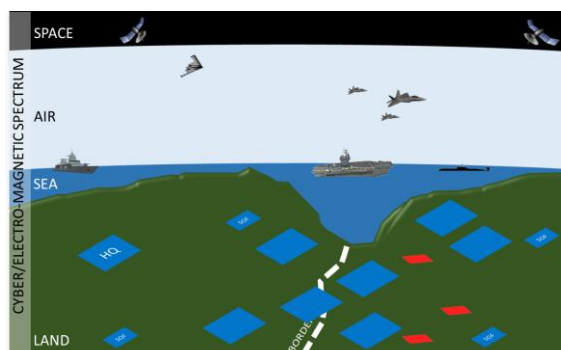

Curve of Military Intervention

58. During the first stage, prevention, the operational of forces is to keep instability situations from arising. However, if an instability situation does arise, forces are prepared, trained, and ready. This means that forces prepare themselves to deal with a wide array of instability situations and can protect themselves from hostile action. In this stage, it is important to inform key stakeholders to reduce the likelihood of instability, increase resilience and establish and maintain robust command and control structures. Important during this stage is that NATO forces can use consultation mechanisms to maximize trust and cohesion.

"Prevent"   *"Intervene"*

"Stabilize"

59. During the intervention stage, the goal is for forces to respond on a timely basis to address instability by communicating and achieving the political-military objectives of the Alliance. This means that military forces must have the ability to project combat power, engage comprehensively, as well as pprotect civilian populations and forces. If necessary, forces must be able to sustain operations over the long term. Important during this stage is that forces lead action with information and use mission command to maximize initiative within the commander's intent.

60. During the next stage, stabilization, as the root causes of instability are addressed; military forces return to a prevention role. This means that forces must have the ability to engage in sufficient duration and effectiveness to address the root causes of instability. Additionally, forces must sustain efforts and support non-military efforts if required as well as communicate with key stakeholders to improve capability and capacity. Throughout, NATO forces should seek to establish and maintain robust command and control structures as well as protect civilian populations and forces. Overtime, the character of military action returns to the prevention stage.

Future Abilities

Prepare

61. 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.

62. 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.

63. 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.

64. 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.

65. 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.

66. 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.

67. 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.

68. 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.

69. 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.

70. 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.

71. 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.

72. 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.

73. 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

74. 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.

75. 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.

76. 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.

77. 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

78. 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.

79. 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.

80. 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

81. 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.

82. 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.

83. 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.

84. 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.

85. 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.

86. 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.

87. 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.

88. 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.

89. 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.

90. 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, Control, Consult (C3)

91. Future C3 Systems: The future security environment will require command and control systems that are resilient and interoperable. C3 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, C3 systems should automatically and seamlessly transfer vital C3 functions to backup systems via pre-determined alternate paths. In some cases, segregated backup

systems operating as stand-alone systems may be required. C3 systems should autonomously re-enable following denial or disruption. Additionally, the communication pathways that enable C3 must be reliable, robust, secure and have alternate/backup systems available.

92. 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, C3 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.

93. Partner Integration and C3: 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. C3 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 C3 systems must enable communication amongst all actors and accommodate timely interaction to achieve mutual objectives.

94. 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. C3 technology will enable real time reach-back to connect experts and senior leaders to geographically separated units operating with smaller and flatter organisational structures.

95. 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 C3 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 C3 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.

96. 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 C3 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

97. 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.

98. 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.

99. 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.

100. 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.

101. 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.

102. 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.

103.   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.

104.   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.

105.   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.

106.   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.

107.   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.

108. 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.

109. 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.

110. 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.

111. 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.

112. 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.

113.   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

114.   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 include-ing 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

115.   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.

116.   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.

117.   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.

118.   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

119.   Military Implications are best military advice intended to inform Alliance transformation, including the development of policies, long-term requirements, and capabilities. Military Implications are not defined requirements, nor are they expressed as required capabilities. Alliance and Member Nations may take into account these long-term abilities during defence planning. In the future the core abilities NATO may require fall into the areas of: prepare; project; engage; sustain; command, control, and consult (C3); protect; and inform.

Annex A

Strategic Foresight Analysis Summary

THEMES	TRENDS	IMPLICATIONS
POLITICAL	**1. The redistribution of geostrategic power.** The predominance of NATO and the West is likely to be increasingly challenged by emerging and resurgent powers.	**a.** Challenges to the rule-based world order. **b.** Euro-Atlantic relations and Alliance cohesion challenged. **c.** Increased requirement for cooperation with other actors including rising powers.
	2. Use of power politics. The importance of NATO has increased for collective defence of the Euro-Atlantic region as it is the main framework that maintains a robust and an appropriate mix of nuclear and conventional capabilities.	**a.** Increased potential of confrontation and conflict. **b.** Nationalism and divergent risk and threat perception. **c.** Requirement for a robust and credible defence and deterrence
	3. Non-state actor influence in domestic and international affairs. Non-state actors are expected to exert greater influence over national governments and international institutions and their role is likely to expand.	**a.** Growing complexity due to a wide variety of non-state actors. **b.** Requirement for closer cooperation with non-state actors. **c.** Increased role of private actors for security. **d.** Increasing concerns for the Protection of Civilians.
	4. Challenges to governance. Emerging powers are increasingly challenging established global governance institutions and requesting greater roles. Existing governance structures, particularly in weak and failing states, are not sufficiently addressing the requirements of the broader population.	**a.** Duplication of existing global governance structures **b.** Increased requirement for partnership and inclusive governance. **e.** Projecting stability beyond the Euro-Atlantic region.
	5. Public discontent/disaffection and polarization. In western countries, risks such as undermined legitimacy of the government mandate, political impasse and the difficulty of implementing reforms and social polarization are likely to be increased.	**a.** Lack of trust in governments and institutions. **b.** Increasing polarization in the West and developing countries.
HUMAN	**6. Asymmetric demographic change.** The worldwide ageing populations will cause major challenges for some economies and government budgets. Gender inequality will further destabilize demographic change. However, the population in countries with a high fertility rate will remain relatively young, as seen in Africa, thus creating a youth bulge and potential for migration.	**a.** Ageing populations will strain resources. **b.** Youth bulges leading to instability and migration. **c.** Failed integration of migrants.
	7. Increasing urbanization. Urbanization is increasing at different rates globally, with the highest growth rates in the least developed parts of the world thus creating the challenge of providing adequate basic services and a functioning infrastructure to ensure a minimum quality of life for citizens.	**a.** Increasing urbanization might lead to resource competition. **b.** Ownership and control of critical infrastructure could be contested. **c.** Governance challenged by uncontrolled urban growth. **d.** Dependence of littoral urban areas on sea lines of communication. **e.** Increased urbanization may require NATO involvement in urban areas.
	8. Fractured and/or polarized societies. Polarization of societies has become a worldwide phenomenon; however, western developed nations are particularly vulnerable due to increased empowerment of individuals. Polarization can also exist between countries.	**a.** Polarization causes instability and civil war. **b.** Instability along NATO's border causing large-scale migration to Europe. **c.** Fractures in society might undermine trust and legitimacy.
	9. Increasingly connected human networks. Human networks are expected to continue to be increasingly decentralized thereby allowing unforeseeable threats.	**a.** Increasingly decentralized and diverse human networks. **b.** An increasing need to understand human networks. **c.** The need for influencing human networks with effective and precise strategic communication is increasing.

THEMES	TRENDS	IMPLICATIONS
T E C H N O L O G Y	**10. Rate of technology advance.** The advances in technology and innovation accelerate as they are fuelled by continued exponential increases in supporting computing power and advances in augmented intelligence.	**a.** Rapid development of technology challenges interoperability. **b.** Increasing legal and ethical concerns. **c.** The rate of technical advancement challenges acquisition and life-cycle management processes.
	11. Access to Technology. The ability of individuals, non-state and state actors to access technology has significantly increased.	**a.** Access to technology enables disruptive behaviours. **b.** Uncontrolled access to technology challenges existing frameworks.
	12. Global network development. Global networks will increasingly enable access to and provide information on commodities and capital assets. Global networks will increasingly be used for dissemination of post-truth information.	**a.** The increasing number of sensors, access to data and global networks generates operational vulnerabilities. **b.** Opportunities to exploit the sensors, data, and global networks. **c.** Adversaries will use global networks for dissemination of false or misleading information.
	13. Dominance of the commercial sector in technological development. The advances in defence technology developments/sales and space exploration /exploitation by commercial sectors have taken away the monopoly that used to be held by governments.	**a.** State approaches are not keeping up with the commercial sector. **b.** The Alliance will lose perishable skills that cannot be easily recovered.
	14. Technological dependencies. Both society, and defence and security, have increasingly depended on certain technologies which have become essential in everyday lives.	**a.** Reliance on certain technologies will create vulnerabilities. **b.** Necessity to protect critical civilian infrastructure. **c.** Over expectations from technological solutions.
E C O N O M I C S	**15. Globalization of financial resources.** An increasingly interconnected global financial system makes it more vulnerable to attacks by both state and non-state actors.	**a.** Erosion of trust in increasingly fragile financial institutions. **b.** Lack of visibility on transactions supporting criminal and terrorist activities. **c.** Growing interdependencies may reduce potential for interstate conflict.
	16. Geopolitical dimension of resources. Emerging technologies and the exploration opportunities availed by climate change may allow the discovery of mineral and energy resources in previously inaccessible and possibly disputed regions such as the High North.	**a.** Natural resources will play an increasing role in power politics. **b.** Resource-driven crises remain a constant. **c.** Climate change has the potential to disrupt traditional areas of food production as well as offer new opportunities.
	17. Increased inequality. The bulk of the world's population, the middle class, particularly in western society has felt the squeeze due to stagnation in real earnings after inflation adjustments, loss of benefits and overall compensation as the private sector has sought to reduce expenses by outsourcing support and labour costs and shift to part time versus full time employment.	**a.** Differences between the 'haves and have-nots' will increase. **b.** Global inequality will drive migration.
	18. Defence expenditures challenges in the West. A majority of NATO Nations were able to change a decreasing defence spending trend into an increase in real terms in 2016. Political and national will would be required to sustain defence expenditures in competing priorities with limited national budgets.	**a.** Increased defence spending due to rising regional tensions and fair burden sharing. **b.** Realignment of expectations with national fiscal priorities.
E N V I R O N M E N T	**19. Environmental / Climate Change.** The changes in climate will bring challenges and opportunities. The changes to the climate impose stresses on current ways of life, on individual's ability to subsist and on governments' abilities to keep pace and provide for the needs of their populations.	**a.** Increased range of activities in the Arctic due to growing accessibility. **b.** Climate and Environmental challenges to governance. **c.** Increased requirements for environmental awareness. **d.** Impacts of climate change adaptation and mitigation measures.
	20. Natural disasters. Natural disasters will have increasing impact, partly due to overall increases in the severity and prevalence of severe weather events, but also due to changes in the regions and times of the year where these events may occur.	**a.** Increased requirement for humanitarian support. **b.** Unavailability of national military assets due to natural disaster. **c.** Increased requirement to improve resilience.

Annex B

Urbanization Study

Introduction

1. The UN reports that urban areas world-wide will absorb 3 billion new people in the next generation.[42] Many of these people will go into under-governed, under-resourced and overstretched cities on coastlines. Studies based upon global demographic trends suggest that an increasing percentage of armed conflicts are likely to be fought in urban surroundings. The trends already exist and the continuation of urbanisation in the future will only exacerbate the likelihood of NATO involvement in urban operations.

The Future Urban Environment

2. The future urban system will be characterised by a high degree of density and complexity expressed through multi-dimensional subsystems. The physical subsystem consists of the complex terrain of an urban settlement, along with the natural environment within and surrounding it

3. The social subsystem consists of the individuals, groups and populations linked to the urban environment and their characteristics. This subsystem is not static but includes the population flows within the city as well as from and into the city.

4. Functional systems of governance in future urban areas are likely to have their own informal structures. Well-off populations may become independent of the state through internal secession and feral cities may emerge where the rule of law has been replaced by near anarchy and the only security available is attained through brute power.

5. The information subsystem has seen the most significant change since the beginning of the 21st century with the explosion of technology, especially communication technology that increases connectivity within and between cities. This enables rapid exchange of concepts, data, and technology-enabled techniques among urban populations, including criminal and terrorist organisations.

---

[42] United Nations Department of Economic and Social Affairs, New York – World Urbanisation Prospects dated 2014.

Future Threat

6. Future threats will incorporate both state and non-state actors, including politically and criminally motivated groups. While many of these threats already exist, future technological developments and the characteristics of future cities will further exacerbate them. Technological advances will enable a proliferation of capabilities such as drones, 3D-manufactured weapons systems, sophisticated IED s and indirect fire weapons. Adversaries can be expected to adopt swarming tactics at the level of individual weapons (swarm weapons) and by applying combat groups that aggregate and disaggregate as needed, massing and dispersing in response to changes in the tactical environment.

7. The city itself, along with its infrastructure and systems, will become a target of enemy action, requiring hardening and protection as well as a degree of specialist knowledge to keep it running. Decoupling humans from weapon systems and increasing electronic connectivity will enable adversaries to disrupt or control larger urban areas with smaller forces.

Emerging Aspects

8. In order to counter the future threat and operate within the future urban environment NATO will need to develop key capabilities, described here within the Joint Functions format of AJP-1:

   b. Command and Control / C3 – a flatter structure enabling rapid allocation of resources to the lowest level; the ability to aggregate and disaggregate forces rapidly; the ability to utilise the urban environment's technology but retain the ability to fight 'unplugged'.

   c. Intelligence – the management of vast quantities of information; the identification of friend or foe in a densely populated environment; city specific databases built and populated prior to any conflict to include governance structures and key leaders; greater resilience and hardening of ISR assets.

   d. Manoeuvre and Fires – delegated authority to utilise fires to prosecute opportunities; greater organic ISR capabilities; an understanding of key cultural sensitivities in order to prevent collateral damage to symbolic buildings; three dimensional battlespace management.

e. Force Protection – dynamic logistic and headquarters structures in order to reduce known and therefore vulnerable force concentrations; rapidly harden systems against physical, electronic and cyber-attack.

f. Information Operations – influence key populations through information operations; operate at the speed of 'social media' to avoid or counter false attribution; withstand cyber or electronic attacks.

g. Sustainment – avoidance of fixed points of supply; the provision of medical support closer to the site of injury.

h. Civil Military Cooperation – an understanding of urban power structures, their leaders and the city management services.

Recommendations for NATO Forces

9. Based on the characteristics of the future urban operating environment, the future threats and the emerging aspects for NATO, the following recommendations have been developed within the DOTMLPFI framework:

a. Doctrine - NATO may have to develop an Allied Joint Urban Operations Doctrine that would provide a sufficient level consideration and guidance to the operational commander. This will come into effect only, if the doctrinal gap cannot sufficiently be addressed by inclusion of urban operations specifics into existing doctrine.

b. Organisation - NATO should: conduct Joint NCS and NFS experiments based on an urban environment, in order to determine the most effective agile organisation and force composition; establish an urban operations centre including a specialist intelligence function; continue to maintain relationships with civil authorities to ensure that military operations are integrated into civilian-led contingencies as part of a comprehensive and federated approach; increase the availability and number of stability policing personnel and strengthen the capacity of the already existing military police capabilities.

c. Training - NATO training exercises should; replicate the intellectual, physical, psychological and emotional challenges posed by urban operations; include higher levels of civil-military interaction and the integration of external stakeholders. A full training needs analysis should be conducted to include aspects of urban operations, as well as major urban exercises included in the NATO MTEP in 2019.

d. Material - The following specific capabilities/technologies should be considered in the development of the NDPP Minimum Capability Requirements (MCR):

   i. Persistent Deployable C3

   ii. Information Domain Superiority

   iii. Persistent Autonomous Sustainment from the Air

   iv. Persistent Autonomous Air ISR

   v. Vertical lift and Rooftop Landing System

   vi. Electronic Warfare superiority

   vii. Delegated authority for Strategic and Tactical Messaging

   viii. Cyber fires – lethal and non-lethal to deny an adversary freedom of manoeuvre

   ix. Protection against kinetic fires and improvised explosive devices in urban environment

   x. Effective information management systems

   xi. Effective underground operations

   xii. Technologies to enable military operations among dense civilian populations, including when civilians are manipulated by the enemy

   xiii. Enhanced capability, trained animals

e. Leadership - Training for future leaders at all levels should include: practical training in how to work with and develop relationships with city officials in order to integrate into the urban and urban littoral system; operate independently in a dispersed manner.

f. Personnel - NATO will require: policing-like skills for activities such as crowd control and curfew enforcement but also skills to enable interaction with the civilian population, including local authorities; skills and knowledge to understand and effectively use the new types of sophisticated technologies; a review of national military selection and training practices for those who may deploy to an urban area.

g. Facilities - A joint training facility is required to simulate the complexities of the urban and urban littoral environment.

h. Interoperability - NATO will need to be interoperable at all levels and additionally its forces should be able to coordinate with coastal constabulary, commerce policing, safety enforcement, patrolling, customs enforcement, raiding, and secure critical infrastructure.

Conclusion

10. The future character of conflict in the future urban battlespace has been described by the 5Cs: it will be more Congested, more Cluttered, more Contested, more Connected, and more Constrained. As such, it is critical for NATO to think in this space, and remain adaptable and resilient enough to operate in the most challenging physical and human environment.

11. Cities will quickly 'swallow' and disperse military troops. NATO is unlikely to be able to build up overwhelming force in terms of mass to control these cities and is more likely to require a footprint as small as possible inside the city. Urban operations will require the conduct of concurrent multidimensional military tasks. NATO will require an agile organisation that is able to integrate into the urban system, supported by an in-depth understanding of the entire urban environment.

12. NATO's Conceptual Study on Urbanisation, from which this Annex is drawn, is available in full at: https://urb.transnet.act.nato.int

13. If you have questions or comments concerning this study please contact: natocde@act.nato.int
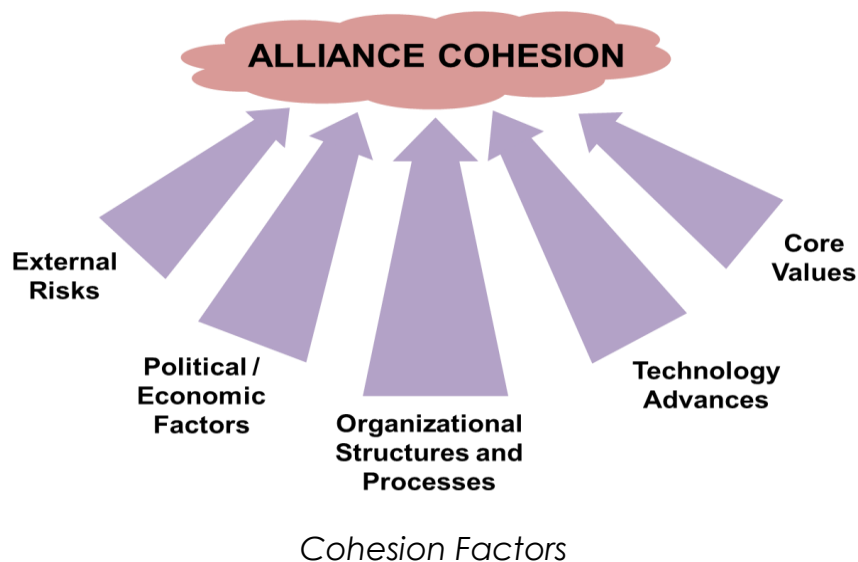
Annex C

Cohesion Perspectives Project

Introduction

1. The Framework for Future Alliance Operations (FFAO) defines the abilities required for NATO Forces to accomplish core tasks in the future. Fundamentally, the Alliance should strive to maintain cohesion – its centre of gravity –to achieve the desired political–military objectives. This project sought to identify factors that would affect Alliance cohesion through 2035 and beyond.

2. The FFAO Cohesion Project targeted students and professionals as the next generation of leaders from different backgrounds (e.g,. academia, military, industry, etc.) to understand their perspectives on NATO's Cohesion. The primary question that guided this research was: *Which factors are likely to affect NATO's cohesion through 2035 and beyond?*

3. The study followed a grounded methodology and employed both quantitative and qualitative methods, triangulated with the scholarly literature on alliance cohesion theory. Between March and June 2017, the Cohesion Project gathered data through a series of focus groups, an online survey, and a workshop prepared in cooperation with the ACT-sponsored Innovation Hub. In total, almost one hundred persons participated in either of ways from all over NATO and Partner Nations.

Cohesion Factors

4. The findings of this study indicated that NATO's cohesion lies on two pillars: trust and reciprocity. This means the ability of NATO Nations to respond as a group and to develop shared interests, values, and common standards and rules. Cohesion is a manifestation of unity, when members stay together despite differences and look beyond self-interests. The ultimate element of cohesion is the willingness to commit and sacrifice for others; an expression of "something bigger than ourselves."

5. As to the risks, the findings indicated that in terms of probability, NATO will face could face a weakening of its core values, accompanied by internal threats to its cohesion. The latter will also have the most severe impact on NATO's cohesion. Technology and organizational frictions also emerged as primary areas of concern. The findings indicated that five primary factors contribute directly to NATO cohesion in the future:

6. **External Risks.** The lack of common existential threat to allies' sovereignty and diverging threat assessment is the major negative element associated with the external threat theme. Although findings sugessted the failure to activate Article 5 in case of attack as a potential risk, non-Article 5 missions could constitute a major test for NATO's cohesion. However, many opportunities may emerge in the future. NATO leadership should seek to develop a common understanding of external threats and a holistic common threat picture. Additionally, future humanitarian/non-military operations could improving cohesion by uniting the countries to pursue common goals.

Cohesion Factors

a. **Political / Economic Factors**. Further crisis of political leadership in NATO Nations, together with undermining international institutions and multilateralism, could lead to weakening of the transatlantic bond, disintegration tendencies within the EU, and even withdrawal of a NATO Nation from the Alliance. Additionally, domestic pressures and concerns over sovereignty could supersede the relative value of the good provided by the Alliance and pull limited funds away from NATO to address them. In addition, continued unequal burden sharing could result in larger states lessening their support and interest for the Alliance and for the defence of free-riding states. However, opportunities do exist as evidenced by an (inter) connected generation of millennials: communication technology tools and internet, in confluence with the

demographic change, can enhance cohesion by increasing the interconnectedness and interactions between NATO Nations to foster understanding.

b. **Organizational Structures and Processes.** Bureaucratic politics that hold on to the past could result in slow adaptation of Alliance to evolving national preferences and interests of NATO Nations. Additionally, long decision-making processes and civil-military frictions on both NATO and national levels could affect readiness of the forces and overall operational effectiveness. Overall, size matters in the Alliance, where cohesion is could become more difficult to maintain as members and partners are added over time. However, opportunities do exist. If NATO can transform its organizational structure to be more efficient, flexible, functional, and agile would be able to adapt to changing national interests on a day-to-day basis. Additionally, strong leadership in NATO's international structures may overcome civil-military frictions. Other opportunities exist in the areas such as increasing the fairness of burden sharing through multinational projects, smart defence, and shaping national capability packages.

c. **Technology Advances.** NATO risks losing the innovation game to private defence industrial sector as in the future, private companies will continue could be ahead of NATO in designing and setting standards for platforms. Additionally, some nations may be reluctant to share their latest technology, thereby increasing the interoperability gap between nations on the battlefield. However, this factor could favour NATO and presents many opportunities as well. If NATO can develop a well-defined framework to clarify what the Nations can do under the NATO flag it could help address challenges created by the emergence of novel technologies, especially cyber and space. If members share innovation and technology in a federated fashion, it can serve to help the Alliance keep its aggregate technological edge.

d. **Core Values.** The Preamble and Article 2 of the North Atlantic Treaty, establish NATO as a security community of liberal-democratic states. Unknown or unclear purpose of NATO can result in the lack of public support for Alliance among NATO Nations and the lack of perceived shared identity; NATO provides an intangible common good - if the alliance is successful, then "nothing happens," since peace, security, and stability are a non-event and can be easily taken for granted. Additionally, differing perceptions of reality, miscommunication, and disinformation could erode NATO's common identity and shared sense

of purpose. Another variable is the uncontrolled growth of populism and radical nationalism, together with a rise of anti-democratic and authoritarian movements will be a source of friction that could weaken NATO's core values. The NATO narrative is extremely important in countering fake news and propaganda that aim to destroy Alliance cohesion and drive wedges in-between members on various issues. Finally, effective strategic communication and public diplomacy targeting the NATO Nations should be able to explain the relevance of NATO (how NATO continues to add value), especially to clarify the purpose and the benefits of membership to the less motivated Nations in terms of reputation, prestige, and legitimacy.

Conclusions

7. Overall, the purpose of this project was to raise awareness of possible future risks to cohesion and to provide NATO and NATO Nations with an informed perspective on how to prevent the Alliance's cohesion from eroding. Although an absence of external threats to Alliance is very unlikely, the future risk will lie in the lack of common understanding of the external threats among NATO Nations. Even though there was no consensus on the degree to which the common values play role in NATO's cohesion, sufficiently aligned interests of NATO Nations, together with a shared purpose of NATO, constitute a definite precondition for a cohesive Alliance.

If you have questions or comments concerning this study please contact: SACTSPPSTRTANBranchDistro@act.nato.int

Annex E

Technology Implications

Placeholder for Technology Implications being developed by STO.

Annex E

First Principles of Future Operations

In development of FFAO 2018, the following were developed as first principles upon which military forces base success on during operations to accomplish the core tasks and address instability in the future security environment. These tenets are intended as essential maxims that will help leaders at all levels understand and adopt the key aspects described in the FFAO, as follows:

- **Know your adversaries better than they know themselves**

- **Understand how the human aspects matter**

- **Train leaders to push power down to the lowest level**

- **Always drive the narrative, matching what we say with what we do**

- **Work together across all domains, with all partners**

- **Fight to win - improvise, adapt, overcome**

- **Never give up the moral high ground**

Annex F

Glossary of Working Definitions

Ability – A critical attribute needed to achieve success in the execution of a future military activity. Abilities are informative statements and not intended to restrain formal capability development processes (see capability).

Adaptation - Learning and changing to keep pace with the challenges of the security environment.

Agility - The ability to respond effectively to dynamic, complex and uncertain operational challenges with appropriate, flexible, and timely actions.

Aware - Comprehensive and accurate shared understanding of the environment and courses of action along with likely risks and threats to enable accurate and timely decision-making.

BRINE - (1) biology, biotechnology and medicine; (2) robotics, artificial intelligence, and human augmentation; (3) Internet and Communication Technology (ICT) and cognitive science; (4) nanotechnology and advanced materials; and (5) energy technology.

Capability – A critical attribute needed to achieve success in the execution of a military activity as developed by the NATO Defence Planning Process (See ability).

Challenge - To confront or defy.

Character of Armed Conflict - A set of qualities that make an armed conflict different from other instances of armed conflict.[43]

Characteristic - A feature or quality belonging typically to a person, place, or thing and serving to identify it.[44]

Collective Defence – Deterrence and defence against any threat of aggression, and against emerging security challenges where they threaten the fundamental security of individual Allies or the Alliance as a whole.[45]

Command, Control, Consult – The ability to exercise authority over and direct full spectrum of assigned and attached forces in the accomplishment of the mission.

Conventional War - Armed conflict between two or more states in open confrontation where the forces on each side are well-defined, generally use conventional weapons and fight using weapons that primarily target the opponent's military.[46]

Cooperative Security – Active engagement to enhance international security, through partnership with relevant countries and other international organisations; by contributing actively to arms control, non- proliferation and disarmament; and by keeping the door to membership in the Alliance open to all European democracies that meet NATO's standards.[47]

Credibility - Leaders, forces, and equipment possessing the ability to deter and defend against potential adversaries and the full spectrum of threats that could confront the Alliance from any direction.[48]

---

[43] Colin Gray, "War – Continuity in Change, and Change in Continuity," *Parameters*. http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/2010summer/gray.pdf, (November 2, 2016).
[44] https://www.google.com/search?q=characteristics&oq=characteristics&aqs=chrome..69i57.2671j0j4&sourceid=chrome&ie=UTF-8
[45] NATO, *Strategic Concept, http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf,* (November 2, 2016).
[46] David Barno and Nora Bensahel, "The Irrelevance of Traditional Warfare?" *War On the Rocks,* http://warontherocks.com/2015/01/the-irrelevance-of-traditional-warfare/, (November 2, 2016).
[47] Ibid.
[48]

Critical Infrastructure Attack - Hostile actors could attack physical and virtual infrastructure nodes and installations in an attempt to disrupt vital societal functions and global stability.[49]

Crisis Management - The full spectrum of crises – before, during and after conflicts.[50]

Cyberattack - When hostile actors could conduct a virtual attack of significant scale, scope or duration to disrupt, deny, degrade, modify, steal, or destroy information resulting in a large physical, emotional or financial impact.[51]

DOTMLPF-I - Doctrine, organization, training, materiel, leadership and education, personnel, facilities, and interoperability.

Endangerment of Civilian Populations - When hostile actors conduct large-scale acts of violence directed against civilian populations. These events could include mob violence, post-conflict revenge, insurgency, predatory violence, communal conflict, government repression, ethnic cleansing, destruction of cultural property and genocide.[52]

Engage - Ability to perform the tasks which contribute directly to the achievement of mission goals, including all abilities required to defeat adversaries.

Escalatory Use of Force - When hostile actors use threats or the use of force increasingly over time that destabilises the security environment that could lead to a strategic miscalculation or increase the likelihood of a wider conflict.[53]

Federated - The efforts to enhance awareness to leverage and explore options via dialogue, linkages, synchronization, de-confliction and collaboration with a broad community of stakeholders (both internal and external, without ceding autonomy) to promote a unity of effort and efficiency to achieve a well-defined end-state.

Future Ethical Questions - A question concerning a developing set of circumstances of events that may require a future moral judgement and decision.

Future Security Environment - The composite of global conditions (e.g., political, military, economic, social, infrastructure, information, etc.) that may be of importance to NATO's military operations in the future.

Global Commons Disruption - Hostile actors challenging international laws and norms in the global commons through threat or use of force (includes space disruption).[54]

Governance Challenges – When governments fail to adequately provide administration and basic functions that could threaten internal and external security and destabilise the environment.

Human Augmentation - Used to refer to technologies that enhance human productivity or capability, or that somehow add to the human body.[55]

Hyper-instability - A situation where more than one instability situation occurs at one time, thereby compounding the negative effects.

---

[49] Sarah Kuranda, "Experts: Recent Critical Infrastructure Attacks a Sign of Major Security Challenges Coming in 2016," *CRN,* http://www.crn.com/news/security/300079278/experts-recent-critical-infrastructure-attacks-a-sign-of-major-security-challenges-coming-in-2016.htm, (November 2, 2016).
[50] Ibid.
[51] Jason Healy, *The Five Futures of Cyber Conflict,* http://journal.georgetown.edu/wp-content/uploads/2015/07/110_gj124_Healey-CYBER-20111.pdf, (November 2, 2016).
[52] Stian Kjeksrud, Alexander Beadle, and Petter Lindqvist, *Protecting Civilians from Violence,* https://www.ffi.no/no/Publikasjoner/Documents/Protecting-Civilians-from-Violence.pdf, (November 2, 2016). NATO Policy for the Protection of civilians http://www.nato.int/cps/en/natohq/official_texts_133945.htm?selectedLocale=en (July 9, 2016)
[53] ICRC, *Violence and the Use of Force*, https://www.icrc.org/eng/assets/files/other/icrc_002_0943.pdf, (November 2, 2016).
[54] Gerald Stang, *Global Commons: Between Cooperation and Competition*, http://www.iss.europa.eu/uploads/media/Brief__17.pdf, (November 2, 2016).
[55] Technopedia. "Human Augmentation," https://www.techopedia.com/definition/29306/human-augmentation, (November 2, 2016).

Hybrid War - Hostile state actors will using a combination of conventional and unconventional means to avoid being held directly accountable for their actions while retaining the option to employ conventional forces, if directly threatened. One of the major characteristics of hybrid warfare is that it often aims to leverage all elements of power while limiting the conflict below the threshold of conventional war thus complicating the timely and effective use of rigid collective defence mechanisms.[56]

Inform – The ability to establish and maintain the situational awareness and level of knowledge required to allow commanders at all levels to make timely and informed decisions.

Innovation - Critical and creative thinking that converts new ideas into valued outcomes.

Instability – Being in a state of likely change.[57]

Instability Drivers - Conditions, events, or circumstances that increase the tendency for the security environment to be unpredictable, changeable, or erratic.

Instability Situations - Generic descriptions of possible future events of critical significance that could reach the threshold requiring the Alliance's use of military forces.

Interoperability - Ability of Allies to act together coherently, effectively and efficiently to achieve tactical, operational and strategic objectives.

Mission Command – When commanders exercise authority and direction using mission-type orders to enable disciplined initiative within the commander's intent thereby empowering agile and adaptive leaders with freedom to conduct of operations.[58]

Multi-polar – When the fundamental power structure in an international system dominated by several large powers, and is characterized by antagonism between these.[59]

Natural/Man-made Disaster - A sudden large-scale man-made or natural event that could result in serious damage, widespread death, and injury that exceeds response capacity. These events could occur as a culmination of several smaller individual disasters in a way that may have an effect similar to a large-scale disaster.60

Nature of War - The inherent constitution of war, its essence.[61]

Opportunity - A good chance for advancement or progress.

Operational Framework - The basic structure underlying the conduct of military operations in response to actual and potential instability situations in the future.

Pandemic Disease - An outbreak of a disease that occurs over a wide geographic area and affects an exceptionally large proportion of the population exceeding response capacity.[62]

Prepare - Ability to establish, prepare and sustain sufficient and effective presence at the right time, keeping sufficient flexibility to adapt to possible changes in the strategic environment.

---

[56] NATO, International Staff Memo, IMSM-0043-2016, (January 15, 2016).
[57] Merriam-Webster, "Simple Definition of Instability," http://www.merriam-webster.com/dictionary/instability, (November 2, 2016).
[58] AJP-1 (D) Allied Joint Doctrine;
59 Eirik B. Lundestad and Tor G. Jakobsen, "A Unipolar World: Systems and Wars in Three Different Military Eras," http://www.popularsocialscience.com/2013/02/05/a-unipolar-world-systems-and-wars-in-three-different-military-eras/ (November 2, 2016).
[60] Peter Baxter, "Catastrophes – Natural and Manmade Disasters," *Conflict and Catastrophe Medicine*, http://link.springer.com/chapter/10.1007%2F978-1-4471-0215-1_3, (November 2, 2016).
[61] Colin Gray, "War – Continuity in Change, and Change in Continuity," *Parameters*. http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/2010summer/gray.pdf, (November 2, 2016).
[62] Regina Parker, "Prevent Disease to Prevent War," *The Strategy Bridge*, http://www.thestrategybridge.com/the-bridge/2016/10/6/prevent-disease-to-prevent-war, (November 2, 2016).

Project – The ability to conduct strategic (re)deployment and RSOI of both NATO and national headquarters' forces in support of Alliance missions.

Projecting Stability – Proactive activities intended to influence and shape the security environment beyond the limits of Alliance geographical boundaries thereby increasing security and reducing threats.

Protect – The ability to minimize the vulnerability of personnel, facilities, materiel and activities, whilst ensuring the Allies freedom of action and contributing to mission success.

Sustain – The ability to plan and execute the timely logistical support of forces.

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

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

Strategic Military Perspectives - Military advice from the Strategic Commanders describing the broad operational framework for future NATO military forces to address the full range of potential future instability situations.

Strategic Shocks - See "Black Swans"

Tenets - Principles upon which military forces base success on during operations to accomplish the core tasks and address instability in the future security environment.

Terrorist Activities - The use of force and violence against individuals or property at an increased scale, scope or duration in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives. [63]

Unconventional War - Hostile state and non-state actors conducting military activities through or with underground, auxiliary or guerrilla forces to enable a resistance movement or insurgency to coerce, disrupt or overthrow a government or occupying power.[64]

Unipolar – Used to describe the power structure in the international system when one superpower dominates alone.[65]

Virtual Cyber States - Populations within the cyber domain where the collaboration of like-minded individuals could wield influence and power of a physical state.

Weapons of Mass Destruction/ Effect (WMD/E) Use - When hostile state and non-state actors seek access to, and use WMD/Es to cause widespread devastation and loss of life against targets such as political leadership, population concentrations, the global financial system, or locations of symbolic importance. [66]

---

[63] Melissa Clarke, "Globally, Terrorism is on the Rise," *ABC News*, http://www.abc.net.au/news/2015-11-17/global-terrorism-index-increase/6947200 (November 2, 2016).; NATO, *AAP-6 Edition 2015*, MC-472/1 "Military Committee Concept on CT", endorsed by MC and approved by NAC, December 2015)
https://nso.nato.int/nso/sPublic/ap/aap6/AAP-6.pdf, (November 2, 2016), Institute for Economics and Peace, Global Terrorism Index 2015, November 2015, http://economicsandpeace.org/wp-content/uploads/2015/11/2015-Global-Terrorism-Index-Report.pdf; NATO, PO(2015)0045, (November 2, 2016).
[64] NATO, *AAP-6 Edition 2015*, https://nso.nato.int/nso/sPublic/ap/aap6/AAP-6.pdf, (November 2, 2016).
[65] Eirik B. Lundestad and Tor G. Jakobsen, "A Unipolar World: Systems and Wars in Three Different Military Eras," http://www.popularsocialscience.com/2013/02/05/a-unipolar-world-systems-and-wars-in-three-different-military-eras/ (November 2, 2016).
[66] UN, "Weapons of Mass Destruction: Threats and Responses,"
http://www.un.org/sustainabledevelopment/blog/2015/01/weapons-of-mass-destruction-threats-and-responses/, (November 2, 2016); NATO, *AAP-6 Edition 2015*, https://nso.nato.int/nso/sPublic/ap/aap6/AAP-6.pdf, (November 2, 2016).