



FFAO Workshop Read-Ahead Material

Rome, Italy, 28-30 March 2017

1. CORE DOCUMENTS

- [Framework of Future Alliance Operations \(FFAO\) 2015 Report](#)
- [Lucerne Workshop Final Report](#)
- Bydgoszcz Workshop Final Report

These documents are available on the ACT 'Futures Work' website (<http://www.act.nato.int/futures-work>).

2. SUMMARY OF THE BYDGOSZCZ WORKSHOP FINDINGS

- The FFAO workshop (28-30 September 2016) focused on the following problem statement: Based on current trends, what are the challenges and opportunities for NATO in the security environment of 2035 and beyond? To develop a prudent and suitable answer to this question the workshop divided into four syndicates and conducted focused discussion on the characteristics of future armed conflict, future ethical questions, instability situations, and future opportunities. At the end of the workshop, the groups came together to compare and contrast findings in a large-group plenary.
- Discussions at the workshop gained insights into how the participants think the battlefield will likely look like in the future (e.g., increased speed of information, use of Artificial Intelligence to assist commanders in decision making, and activities in the cyber domain impacting the physical domain). Additionally, discussions raised many ethical questions NATO leaders may have to address in the future (e.g., human augmentation, distinguishing between combatants and non-combatants, use of AI and robotics, and cyber). The workshop discussions examined the current instability situations for validity, and the groups developed a refined list that they felt better represented the

possible instability situations in the future. Of note, one of our key take-a-ways is that we should review our model and possibly distinguish between instability drivers and instability situations. Finally, the workshop developed an expanded list of opportunities NATO may have in the future, to include items such as: 1) ability to increase the dispersion on forces, 2) rebalancing of military capabilities away from being only expeditionary or only article 5 oriented, and 3) developing better intelligence by using open source information.

3. FFAO ROME WORKSHOP OVERVIEW

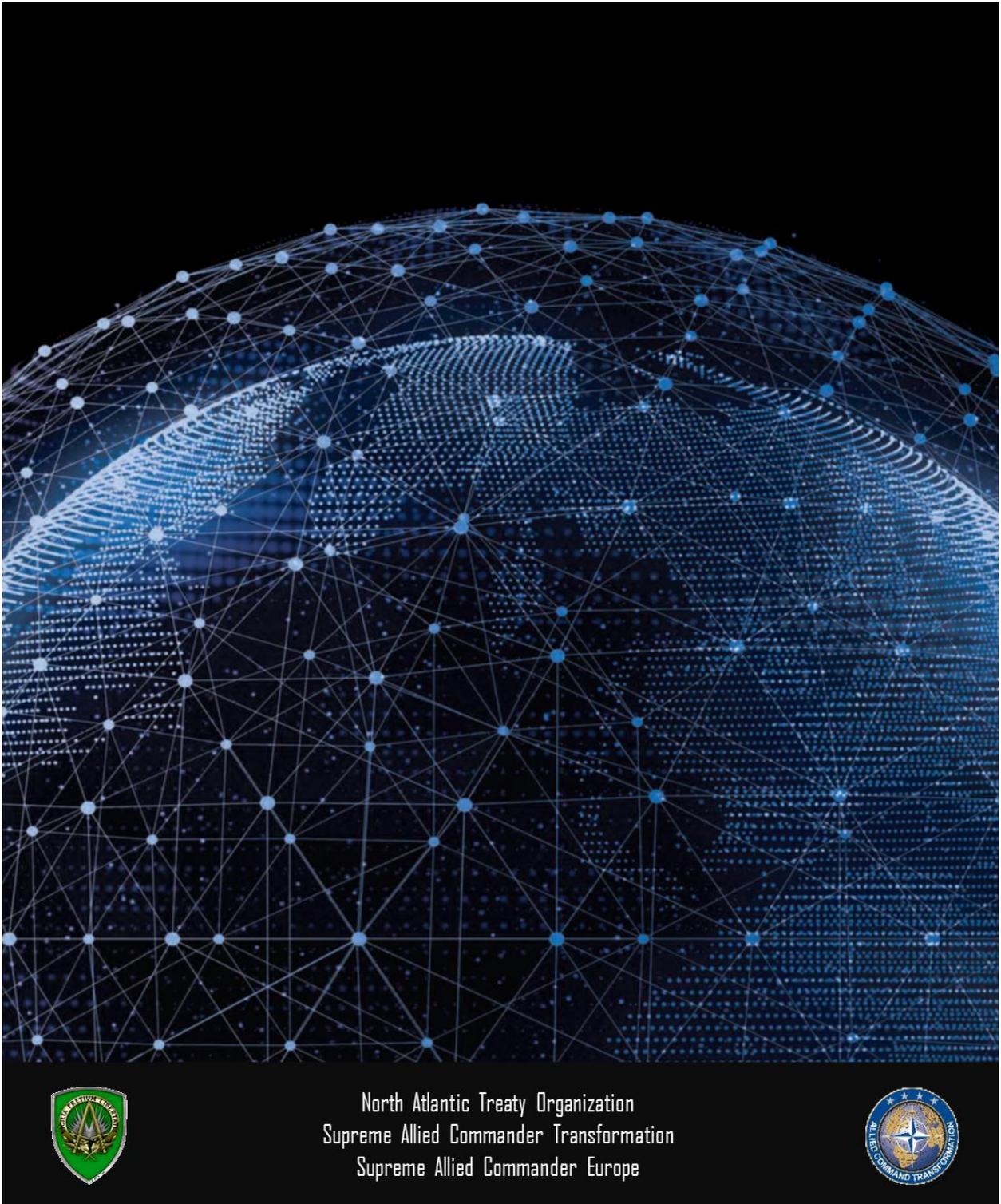
- The FFAO workshop will be a three-day working-level event held at the NATO Defence College in Rome Italy. The first day will begin with a large group plenary for introductory remarks, discussion of workshop concept and objectives, survey results, and applicable lessons learned. Then the workshop participants will be broken down into small syndicates for detailed group work to discuss selected topics concerning to address the core question: Based on the possible INSTABILITY SITUATIONS in the future security environment of 2035 and beyond, what is an FRAMEWORK that will enable the success of NATO military forces at its core tasks? Following the discussions the first day, the workshop participants will be invited to attend a brief icebreaker event.
- The second day of the workshop will begin with a large group plenary session on ACT's Urbanization Project. 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 in the afternoon of day 3.

4. DELIVERABLES

The primary deliverables for this conference are recommended changes to the draft Chapter 2 of the FFAO. Following the conference, Chapter 2 of the FFAO will be finalized and submitted through the official staffing process for adjudication and approval.

Framework for Future Alliance Operations

March 2018



Foreword

PLACE HOLDER





Table of Contents

Executive Summary	4
Introduction	6
Chapter 1	8
The Future Security Environment towards 2035 and Beyond	
Chapter 2	x
Strategic Military Perspectives	
Chapter 3	x
Military Implications	
Conclusion	x
Annexes	
A – Strategic Foresight Analysis (SFA 2017) Trends	x
B – Technology Trends Survey (TTS) Summary	x
C – Urbanization Study Summary	x
D – Glossary of Working Definitions	x

Executive Summary [2 Pages]

1. Today, the Alliance's military forces face a challenge in that they must adapt, evolve and innovate to constantly meet an ambiguous, complex, and rapidly changing security environment. To help inform the discussion 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 of 2035 and beyond.
2. 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 principles 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, and capitalising on innovative technology and ideas to maintain the military edge.

42. NATO will likely face many challenges as it continues to safeguard its enduring interests in the future. When directed, military forces from different countries and services must assemble rapidly, influence/set conditions for success, and act across all domains in order to achieve political goals and uphold the common interests of the Alliance. To achieve this, NATO military forces should grow more federated, aware, resilient, agile, interoperable and credible; apply dynamic operational principles; and be supported with critical elements for success on the future battlefield.
3. [Summary of Chapter 3.]

Introduction

Problem Statement

1. The Alliance's military forces must adapt, evolve, and innovate to constantly meet an ambiguous, complex, and rapidly changing security environment.

Aim

2. To identify characteristics and abilities of a future Alliance pool of forces to meet the potential demands of the future security environment of 2035 and beyond.

Background

3. 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) can 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

Scope

4. 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

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

discussions and white papers; NATO defence planning; capability development; concept development; and doctrine, training, exercises, leadership, and education. 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 general public to stimulate discussion and debate.



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

5. 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.

Key Assumptions

6. This document is intended for multiple audiences and may impact audiences outside of NATO. In addition, NATO's foundational documents will remain unchanged. Also, the SFA and other references used in development of this document are assumed to be 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

7. 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 – NOTE: CHANGES MADE POST STAFFING, SEE TT#161460

The Future Security Environment towards 2035 and Beyond

1. 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 ample opportunities and risks. The increasing interdependency amongst countries has potential to create stability in the long-term. However, the ongoing transition from a unipolar to a multipolar and multi-dimensional world has created instability that is likely to continue or even escalate.²
2. 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.
3. 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 change. This will test the ability of military forces to adapt to the challenges of a rapidly changing global security environment.

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.

³ 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).

Future Challenges

A More Rapidly Changing Security Environment

4. 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 Armed conflict 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 purpose as an instrument of policy.⁵ However, each instance of armed conflict is different than 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
5. 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 within the world might result in cascading instability, blurring 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. Increase in use of innovative ways and means in the realm of weaponization of information activities to influence populations alone or in support of armed conflict.

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. A compression of the traditional levels of war where strategic, operational, and tactical events become difficult to differentiate.
- f. Rapidly emerging technologies in areas such as cyber, autonomy, hypersonic weapons, big data, artificial intelligence, communication, surveillance, electronic warfare.
- g. Increased likelihood of human enhancement through mechanical and biological means to improve military performance.
- h. Over time, the use of automated systems in warfare may increase and eventually may not directly involve humans in the decision cycle.
- i. Smaller numbers of forces may fight over greater distances.
- j. New classes of weapons of mass destruction / effect may emerge.
- k. Increased numbers of sensors and the ubiquitous “internet of things” could influence operational security and increase the impact of social media on the battlefield.
- l. An increase in the likelihood of armed conflict involving global commons, space, densely populated areas and subterranean areas.
- m. The widely accessible and cheaper technologies are increasing the role of individuals, giving separate persons or groups the ability to produce uncontrolled and hard to predict effects.
- n. Increased access to knowledge could enhance and speed up the emergence and mobility of threats.
- o. Increasing overlap between criminal activity and war / armed conflict.⁷

Future Instability

- 6. 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. Therefore, to focus on the specific operational impacts on NATO’s military forces in the future, it is critical to clearly define and

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).

differentiate between instability drivers and instability situations. The trends indicate that the “new normal” operating environment may be dynamic, complex, and characterised by instability that could arise more frequently and be globally interconnected. The nature of security challenges varies from classic state-on-state threats, through challenges to the global commons, to actors with state-like ambitions and transnational threat networks. Instability could present second and third order challenges, internal and external to the Alliance and its partners.

7. 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.
8. 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,

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/>

Biological, Radiological, or Nuclear (CBRN) or weapons of mass destruction based on new technologies.

INSTABILITY SITUATIONS

- WMD/E Use
- Conventional War
- Escalatory Use of Force
- Hybrid War
- Unconventional War
- Terrorist Attack
- Global Commons Disruption
- Critical Infrastructure Attack
- Cyberattack
- Governance Challenges
- Endangerment of Civilian Populations
- Pandemic Disease
- Natural/Man-made Disaster

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.

e. **Unconventional War:** Hostile state and non-state actors may conduct 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.¹⁴ In unconventional

(November 2, 2016); NATO, AAP-6 Edition 2015, <https://nso.nato.int/nso/sPublic/ap/aap6/AAP-6.pdf> (November 2, 2016).

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, AAP-6 Edition 2015, <https://nso.nato.int/nso/sPublic/ap/aap6/AAP-6.pdf> (November 2, 2016).

conflicts the use of propaganda could be used in an attempt to influence populations.

- f. **Terrorist Attack:** Hostile 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.¹⁵
- g. **Global Commons Disruption:** Hostile actors may directly challenge international laws and norms in the global commons through threat or use of force.¹⁶ Increased resource competition and commercialisation of space may lead hostile actors to directly 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.¹⁷
- h. **Critical Infrastructure Attack:** Physical and virtual infrastructure nodes and installations remain essential to the enduring interests of the Alliance. Hostile actors could attack these nodes in an attempt to disrupt vital societal functions and global stability.¹⁸ 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. **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

¹⁵ 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*, <http://economicsandpeace.org/wp-content/uploads/2015/11/2015-Global-Terrorism-Index-Report.pdf> (November 2015); NATO, PO(2015)0045, (November 2, 2016).

¹⁶ Gerald Stang, *Global Commons: Between Cooperation and Competition*, http://www.iss.europa.eu/uploads/media/Brief_17.pdf (November 2, 2016).

¹⁷ 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).

¹⁸ 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).

impact.¹⁹ Hostile actors could use cyberattacks in isolation or in support of conventional, hybrid, or unconventional approaches.

- j. **Governance Challenges:** Some governments may fail to adequately provide administration and basic functions which could threaten internal and external security and destabilise the security 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.
- k. **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, and genocide.²⁰
- l. **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.²¹
- m. **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 disasters in a way that may have an effect similar to a large-scale disaster.²²

Ethical Challenges

- 9. 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.²³ The primary question that NATO must

¹⁹ 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).

²⁰ 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)

²¹ 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).

²² 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).

²³ 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

continually address is: Based on the rapidly changing character of conflict and the potential instability situations, how do forces apply existing principles of the Law of Armed Conflict (e.g., distinction, proportionality, military necessity, prevention of unnecessary suffering, etc.)?²⁴ 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?²⁵
- b. **Autonomous Systems, Artificial Intelligence, 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?²⁶
- c. **Cyber:** 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 intelligence? How do forces find the right balance between information security and the need for transparency?²⁷

(January 24, 2017); The Royal Academy of Engineering, "Autonomous Systems: Social, Legal and Ethical Issues", <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiUrdK82ORAhXE24MKHWxYAUoQFggcMAA&url=http%3A%2F%2Fwww.raeng.org.uk%2Fpublications%2Freports%2Fautonomous-systems-report&usq=AFQjCNGAL49W8TH70oDxnrGjNFQgPiRaA> (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)

²⁴ NATO-ACT, *FFAO Bydgoscs, Poland Conference Report 2016*, <http://www.act.nato.int/futures-ws-5>, (November 2, 2016).

²⁵ Ibid.

²⁶ Ibid; UN, "The Convention on Certain Conventional Weapons,"

[http://www.unog.ch/80256EE600585943/\(httpPages\)/4F0DEF093B4860B4C1257180004B1B30?OpenDocument](http://www.unog.ch/80256EE600585943/(httpPages)/4F0DEF093B4860B4C1257180004B1B30?OpenDocument) (November 2, 2016).

²⁷ Ibid.

d. **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? ²⁸

Future Opportunities

10. In the future, there are many opportunities that NATO forces could seize upon to improve the security environment.²⁹ Innovation and technological changes during this time period will offer military advantages that NATO forces or adversaries could capitalise on. Innovation is not only the adoption of new technologies but could include 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 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.³¹

11. 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

²⁸ Ibid.

²⁹ Ibid.

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).

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

12. 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 which pose a threat to the security of territory and populations. Military forces may also have more opportunities to engage in non-combat operations, deter and prevent conflicts, or help resolve conflicts, all of which could change the future security environment for the better.³⁵

Conclusion

13. 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 principles 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, and capitalising on innovative technology and ideas to maintain the military edge.

³⁴ Ibid.

³⁵ Ibid.

Chapter 2 – NOTE: NON-STAFFED WORKING DRAFT

Strategic Military Perspectives

Introduction

14. Strategic Military Perspectives constitute 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. 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. NATO member states form a unique community of values, committed to the principles of individual liberty, democracy, human rights and the rule of law. The Alliance is firmly committed to the purposes and principles 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.³⁶

15. As discussed in Chapter 1, military forces may need to address a wide variety of instability situations in the future security environment which may challenge these interests and its centre of gravity; the coherence of the Alliance. At the political and strategic level, the Nations that comprise NATO set policy and direct the military instrument of power when needed in the future. This chapter is intended to help the leaders of NATO think clearly about the role military forces could take in safeguarding its enduring interests in the context of the future security environment.

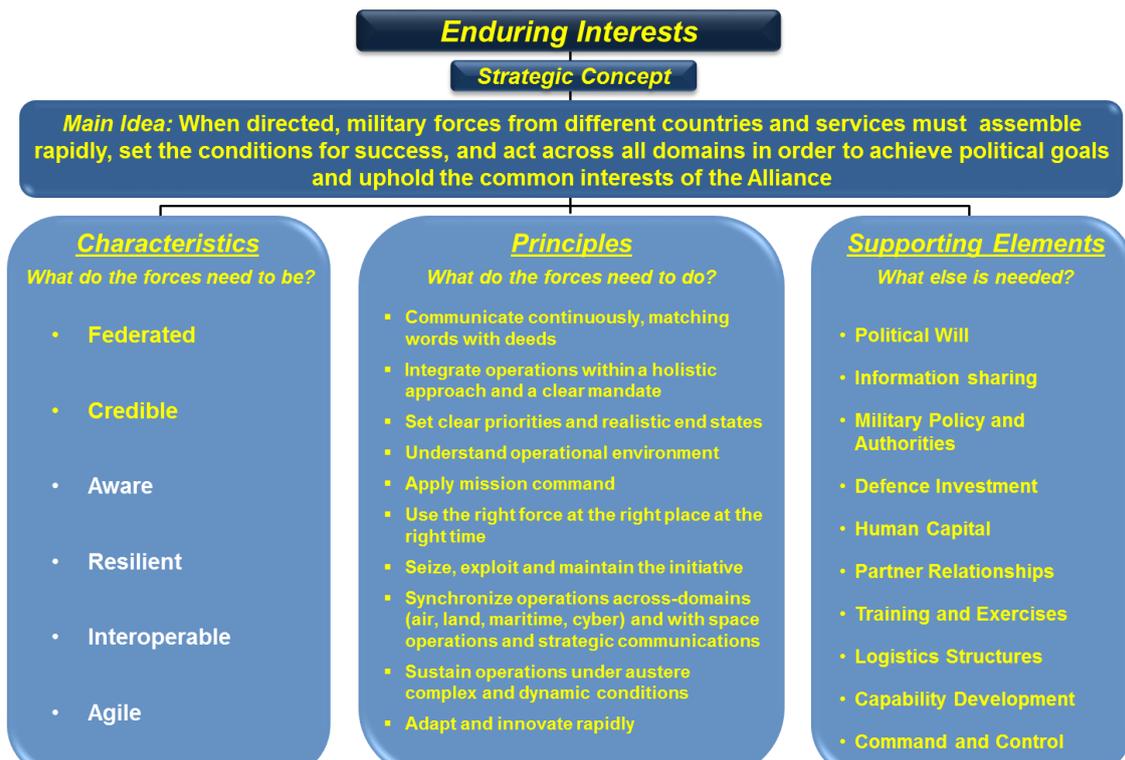
³⁶ http://www.nato.int/cps/en/natolive/official_texts_17120.htm

The Military Problem

16. As the Alliance continues to safeguard its enduring interests and maintain its cohesion, forces will likely face the following military problem: Based on the possible instability situations in the future security environment of 2035 and beyond, what is an operational framework that will enable the success of NATO military forces at its core tasks?

Future Framework

17. When directed, military forces from different countries and services must assemble rapidly, influence/set conditions for success, and act across all domains in order to achieve political goals and uphold the common interests of the Alliance. To achieve this NATO military forces should employ an operational framework consisting of certain characteristics, principles, and supporting elements.



Future Framework

Characteristics

18. Characteristics are features or qualities belonging typically to a person, place, or thing and serving to identify it. To successfully integrate operations across domains in the future, forces will likely require certain characteristics that span all core tasks. Specifically, forces should become more federated, aware, resilient, agile, interoperable and credible.

Federated

19. Federated means increasing of capacities, opportunities, and influence within the security environment by expanding the number and type of partnerships and through continuous partner interaction. Federation presents an opportunity for NATO to act in concert with a variety of state and non-state actors to address future security threats holistically and includes the ability to influence the security environment through continuous interaction via physical and virtual presence. 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 law enforcement, intelligence, and non-governmental organisations.

20. 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 might best be implemented from tactical through strategic levels to build a common view of the situation.

21. Countries always retain the right to act alone, which could in time 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 prearranged 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.

Aware

22. Awareness means providing leaders with a more comprehensive and precise understanding of the situation, available courses of action, and likely risks and threats to enable timely and accurate decision making. By increasing Awareness the Alliance improves cohesion through a shared assessment of current and future strategic level challenges and opportunities, and to allow timely synchronisation and alignment of military planning and organisation with political intent. Institutions and states face a rapidly growing range of security challenges and opportunities, including those presented by trans-national and non-state actors. State-sponsored proxies and other non-state actors using hybrid warfare methods require the Alliance to gain a broad knowledge and understanding of a wide range of criteria that might fuel a potential crisis or conflict. By identifying the first signals of an impending threat, helps the Alliance 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.
23. 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.
24. Awareness leverages new and emerging technologies to collect, process, and analyse a vast amount of data. A shared assessment can be gained by fusing this analysis with traditional intelligence in a 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

25. Resilience is the ability to retain credible 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.
26. In the increasingly complex environment of the future, threats may be less foreseeable. 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 achieving this coordinated effort.
27. Sustainment is another key aspect of Resilience. Forces must possess the capabilities to sustain both themselves and, if necessary, coordinate sustainment for segments of the local population as the introduction of large military forces may tip delicate local resource balances. Pre-aligned coordination and cooperation among civilian and military authorities 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

28. Agility is the ability to respond effectively to dynamic, complex and uncertain operational challenges with appropriate, flexible, and timely actions. 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.

29. 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. This decision-making can be aided by efficient information management, as well as a mission-command type leadership philosophy that allows decentralised, flexible decision-making within the overall commander's intent.
30. 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.
31. 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.
32. Agility places significant importance on the development of leaders with creativity, initiative, and the ability to make timely, effective decisions that support their unit's mission. It reinforces the requirement to organise and operate based on assigned tasks, with scalable troop organisations and command and control structures that are able to aggregate and disaggregate quickly and to adapt easily to the circumstances encountered across all domains and the full spectrum of military operations. 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.

Interoperable

33. In many ways, the Alliance has been building for the ability of forces to work together since its founding in 1949. Interoperability has become even more important, and may continue to grow in importance in the future. Interoperability is the ability for Allies 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 partner countries.

34. Interoperability does not necessarily require common military equipment. What is important is that the equipment can share common facilities, and is able to interact, connect and communicate, 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.

35. In the future, forces may need to achieve a high level of interoperability through joint planning, training and exercises. Alliance members may have to put their interoperability into practice during joint operations in the future. Partner countries may also need to improve interoperability and overcome inequalities in technology procurement and employment.

Credible

36. The characteristic of credibility is defined as 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.³⁷ 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. Simply put, in the future, the entire command structure and force structure – as well as Allies, individually and collectively – need to be prepared and ready to defend each other from any threat from any direction. In the future security environment, the credibility of military forces is a critical factor in maintaining the balance of power both regional and globally.

37. In many ways, credibility can only be judged by understanding the perceptions and the actions of adversaries. How an adversary perceives

³⁷ Warsaw summit

the 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 their abilities through realistic and challenging training exercises. In times of conflict, NATO must have the ability to rapidly deploy forces into non-permissive combat environments and achieve the desired political objectives the Alliance sets forth.

38. It stands to reason that robust military capability is an indispensable element of credibility. Without a wide-range military capability, potential adversaries could judge NATO forces as weak, and may seek to take advantage of the circumstances. In addition to capability, NATO forces must have a sufficient level of readiness to act quickly in times of crisis. Additionally, 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.

Principles

39. Principles are tenets upon which military forces base success on during operations to accomplish the core tasks and address instability in the future security environment. In order to accomplish the core tasks when dealing with the possible instability situations of the future NATO forces should adhere to the following principles:

- a. Communicate continuously, matching words with deeds
- b. Integrate operations within a holistic approach and a clear mandate
- c. Set clear priorities and realistic end states
- d. Understand operational environment
- e. Apply mission command
- f. Use the right force at the right place at the right time
- g. Seize, exploit and maintain the initiative
- h. Synchronize operations across-domains (air, land, maritime, cyber) and with space operations and strategic communications
- i. Sustain operations under austere complex and dynamic conditions
- j. Adapt and innovate rapidly

Supporting Elements

40. Supporting Elements are other activities or things future forces need for success during operations to accomplish the core tasks and address instability in the future security environment. First and foremost, countries must have a shared political will that allows military forces to work together in a complementary manner. As an expression of political will, NATO military forces require the requisite military policies and authorities required to perform operations successfully. Among these authorities, forces need to have the authorities and permissions needed share information at the right level and the right time so that they are successful on the battlefield.
41. There are other enabling functions that will set the conditions for future operational success. It takes time and money to develop and procure combat systems. Therefore, it is critical that adequate resources are allocated to capability development and defense investment years in advance. Perhaps even more critical is that it takes time and effort to develop human capital and execute training and exercises to make the most out of the human capital in the force. Finally, relationships take a tremendous amount of time to develop fully, and will stand to be a core strength of NATO forces looking to the future.

Conclusion

42. NATO will likely face many challenges as it continues to safeguard its enduring interests in the future. When directed, military forces from different countries and services must assemble rapidly, influence/set conditions for success, and act across all domains in order to achieve political goals and uphold the common interests of the Alliance. To achieve this, NATO military forces should grow more federated, aware, resilient, agile, interoperable and credible; apply dynamic operational principles; and be supported with critical elements for success on the future battlefield.

Annex C

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.

Awareness - The ability to provide leaders with a more comprehensive and precise understanding of the situation, available courses of action, and likely risks and threats to enable timely and accurate decision making.

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.³⁸

Characteristic - A feature or quality belonging typically to a person, place, or thing and serving to identify it.³⁹

³⁸ Colin Gray, "War – Continuity in Change, and Change in Continuity," Parameters. <http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/2010summer/gray.pdf>, (November 2, 2016).

³⁹

<https://www.google.com/search?q=characteristics&og=characteristics&ags=chrome..69i57.2671j0j4&sourceid=chrome&ie=UTF-8>

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.⁴⁰

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.⁴¹

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.⁴²

Crisis Management - The full spectrum of crises – before, during and after conflicts.⁴³

Supporting Elements - Activities or things future forces need for success during operations to accomplish the core tasks and address instability in the future security environment.

Federated - Increasing capacities, opportunities, and influence within the security environment by expanding the number and type of partnerships and through continuous partner interaction.

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.

Human Augmentation - used to refer to technologies that enhance human productivity or capability, or that somehow add to the human body.⁴⁴

⁴⁰ NATO, *Strategic Concept*, <http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf>, (November 2, 2016).

⁴¹ Ibid.

⁴² Warsaw summit

⁴³ Ibid.

⁴⁴ Technopedia. "Human Augmentation," <https://www.techopedia.com/definition/29306/human-augmentation>, (November 2, 2016).

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

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

Instability – Being in a state of likely change.⁴⁵

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.

Integrated Cross Domain Operations (IXO)- When military forces from different countries and services operate in a unified and mutually supporting fashion across all domains (air, sea, land, space, cyber) in concert with all elements of power (diplomatic, informational, military, economic, financial, intelligence, and law enforcement) to achieve the desired political outcome.

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.⁴⁶

Multi-polar – When the fundamental power structure in an international system dominated by several large powers, and is characterized by antagonism between these.⁴⁷

Nature of War - The inherent constitution of war, its essence.⁴⁸

⁴⁵ Merriam-Webster, "Simple Definition of Instability", <http://www.merriam-webster.com/dictionary/instability>, (November 2, 2016).

⁴⁶ AJP-1 (D) Allied Joint Doctrine;

⁴⁷ 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).

⁴⁸ Colin Gray, "War – Continuity in Change, and Change in Continuity", Parameters.

<http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/2010summer/gray.pdf> (November 2, 2016).

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.

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

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"

Unipolar – Used to describe the power structure in the international system when one superpower dominates alone.⁴⁹

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

⁴⁹ 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).