Strategic Military Perspectives Workshop

Read-Ahead

11-12 June 2014
Marine Establissement Amsterdam (MEA)
Amsterdam, the Netherlands

Organized by
Allied Command Transformation, Norfolk
Strategic Plans and Policy Directorate

Contents

Agenda

Wednesday, 11 June 2014

0800-0900 Check-in/Registration and Coffee

0900-0945 Plenary Session: Welcome and Introductory Remarks

0945-1015 Coffee Break

1015-1230 Syndicate Session #1

The Syndicates will analyse their assigned Instability Situations by Capability Hierarchy Framework. The Instability Situations will be divided into 3 broad groupings: (1) Urban/Mass Population; (2) Global Commons; and (3) Non-State Actors.

1230-1330 Lunch (Self-paid)

1330-1500 Syndicate Session #2 (Continue Work from Session #1)

1500-1530 Coffee Break

1530 -1700 Syndicate Session #3

The Syndicates will conduct Holistic Analysis of their group of Instability Situations, asking the question "What is expected to be different at the strategic level for the military when faced with these Instability Situations in the future?"

Thursday, 12 June 2014

0830-0945 Syndicate Session #4
(Syndicate discussion of possible Strategic Military Perspectives)

0945-1000 Coffee Break

1000-1115 Syndicate Session #5
(Continue from Session #4/Prepare for Plenary)

1115-1215 Plenary Session: Syndicate Work Debrief & Closing Remarks
The findings of each syndicate will be debriefed in plenary session. The way ahead will be presented.

1230 Lunch (Self-paid)

Workshop Overview

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

- **Objective:**
  - **Conduct a strategic level analysis of the Instability Situations, assessed within the Capability Hierarchy Framework (CHF)**

- **Expected Outcome:**
  - **Derive CHF-structured ideas to inform post-workshop generation of Strategic Military Perspectives (SMP)**

Groups of Instability Situations (Three plus One)

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

Disruptive Impact of Migration
Statement of Context
Mass human migration caused by demographic, environmental, economic or political change or armed conflict will exceed the ability of governments to protect and provide services for their resident populations. This uncontrolled migration will increase the potential for inter-ethnic, cultural, racial and religious tensions.
Main Contributing Trends
(4) Changing Demographics, (5) Urbanisation, (6) Human Networks/Transparency, (7) Fractured Identities, (14) Environmental/Climate Change, (15) Natural Disasters
Who:
Nations with limited resources or infrastructure that have weak immigration control could become target nations for migrant source nations. Other nations could expel their populations to cause civil unrest in a target nation. Extremist, criminal, ethnic organisations interested in creating instability will establish their networks with large, displaced, urban, populations.
Why:
Rapidly changing environments (economic, political, or physical) will cause massive migration. People will move to avoid epidemic, poverty, inequality, political oppression, climate change or natural disaster. Government authorities are under resourced to respond adequately to large migrant populations. Groups will use population displacement to gain power through ethnic cleansing.
How (Ways and Means):
Actors will cause mass demonstrations to disrupt life support within urban areas. The increased communication and human networking capabilities available through the internet and social media will accelerate disputes within migrant populations. Migrants will use a range of transportation means, (air, rail, road, and sea), to move to urban areas. Open borders, global transportation network and ease of movement enable rapid migration between countries. Political groups, state actors or criminal networks use migration as a means to achieve organisational goals.
Where:
People are moving from rural to urban areas. Megacities within poor countries will be less able to manage the mass of migrants. Regions at high risk for earthquakes, hurricanes, and other natural disasters, underdeveloped countries with autocratic regimes and lightly defended borders especially near coastal areas, as well as regions with politically oppressed populations will be the migrant source areas.
What is new in 2030?
Control over the flow of mass migration will become a widespread security issue especially within urban areas. More areas will be at tipping points where thresholds leading to crises will be more easily exceeded. More populations will be at risk caused by greatly increased urban population growth; accelerating climate change and political unrest. The speed and rate of movement and size of migrant groups will increase thus degrading ability to control migration. Multiple migration flows will occur simultaneously. Migrants provide opportunity for host nations to address declining populations by increasing human capital and supporting population growth. Disruptive migration also has the ability to increase the internal strife between government and immigrants as well as between residents from different subnational groups.

Large-Scale Disaster
Statement of Context
Large-scale disasters, such as deadly pandemics (natural or manmade), famine or natural disasters result in governments seeking external support in the provision of health, security, and welfare of governed populations. Entities like nations, criminal organisations or extremist groups exploit the chaos to achieve goals.
Main Contributing Trends
(5) Urbanisation, (6) Human Networks, (14) Environmental/Climate Change, (15) Natural Disasters
Who:
The government and people who live within an area impacted by a disaster will be the most involved. However, a disaster will attract a range of opportunistic groups including state and non-state actors, extremists, and criminal organisations. Also there will be a large number of other actors who will respond or be impacted by the disaster including state military and disaster relief agencies international organisations (IO), non-governmental organisations (NGO), private sector or commercial entities, and security organisations.
Why:
Although disasters negatively affect the people in impacted regions, such crises also create opportunities for others. Since vulnerability to a disaster is increased by heavy urbanisation, limited resource availability, and weak governments, any disruption of transportation, energy supply or communications may challenge civil services and degrade the ability to respond. This lack of control allows state or non-state actors to use disaster as an opportunity to destabilise a government. Also as a consequence of globalisation populations tend to concentrate and people can move rapidly between urban population centres thus increasing the potential for epidemic or pandemic. Climate change will increase the frequency and severity of weather-related natural disasters.
How (Ways and Means):
Large-scale disaster (natural or manmade) will significantly increase the flow of people creating mass movement of populations. National capabilities in underdeveloped areas will be unable to cope with large-scale disasters and some regions will experience transnational impacts that could cascade across borders and lead to widespread humanitarian catastrophe. Some actors will take advantage of such situations to gain or consolidate influence over established governments, or to take control of vital infrastructure. Such a regional or global disaster provides a profit opportunity for business or criminal organisation by providing relief at a premium cost to impacted people. Opportunistic actors will seek to control resource distribution and may engage in hoarding or extreme market inflation of food, water, medical supplies, housing and energy. Competition for and authority over resource allocation during the chaos of a disaster will challenge security providers.
Where:
Large-scale disasters, either natural or manmade, can occur anywhere but are especially challenging to governmental control in locations with high densities of population and in littoral areas. Disasters in such regions can rapidly become a global challenge. Also, the continued and effective operation and populations of any one of the world's financial or commercial centres are especially vulnerable to large-scale disaster.
What is new in 2030?
The frequency and severity of large-scale disasters will increase due to climate change and urbanisation. The threshold is reduced for the collapse of a state or region. Increased globalisation, urbanisation and interconnectedness make the spread of disease easier and more devastating. Faster information flows will spread fear and panic at an accelerated rate. Multinational corporations and criminal organisations play a bigger role disaster relief. Megacities in weaker states raise the probability of a collapse. Private security organisations will play an increased role in providing security.

Megacity Turmoil
Statement of Context
Confrontation between multiple actors with varying levels of external support and competing interests create or aggravate chaotic situations to cause turmoil within megacities.
Main Contributing Trends
(4) Changing Demographics, (5) Urbanisation, (6) Human Networks/Transparency, (7) Fractured Identities, (9) Increased Access to Technology, (12) Increased Resource Scarcity, (15) Natural Disasters
Who:
Local and/or national authorities, political parties; tribal and/or ethnic groups; criminal organisations, extremist/terrorist organisations; super-empowered individuals; resource starved neighbours; new politically competitive groups (e.g. during the Arab Spring established soccer fan clubs became empowered actors of revolution) will all compete for political power within large urban areas.
Why:
Highly urbanised populations are not resourced to be self-sustaining and will therefore consume more food, water, and energy than they produce, which further increases competition for limited resources in the urban area. Urban actors who lack political power will seek to replace governments that fail to provide security or respond sufficiently to economic distress or social unrest and that cannot prevent pervasive criminal activities or provide basic city services. Such actors will have large incentives to gain political power because of their requirement to obtain a greater share of scarce resources and to ensure security. Also, confined spaces within cities create tension and fracture identities.
How (Ways and Means):
Megacities amplify tensions between people and cause a fragility that lowers the security threshold (the point where governments cannot protect most of the people). Urban actors will seek to use unidentifiable crowds to take control over scarce resources. They will blend into large populations to challenge the ability of military forces to operate and will cause a human disaster to increase chaos. They will seek to disrupt services and influence populations by use of physical attacks and the spread anti-establishment narratives that are designed to provoke people to act against the government and security forces. For example, street-gangs or organised crime syndicates with military capabilities can produce no-go areas, distribute weapons, and provide misinformation to persuade local inhabitants to support their goals.
Where:
Urban actors will operate within densely populated areas or megacities and in places with insufficient infrastructure and services to provide for the population. They will live and work in areas with limited vehicle access and in the complex 3-dimensional terrain of urban areas with underground spaces, like subways and sewers, and within tall buildings and the dense entanglements of residential slums, abandon buildings, factories, and power plants. They will target resource exporting countries in regions of high-density traffic and data flow with potential global communication nodes and strategic choke points, and cities near coastal locations.
What is new in 2030?
New alliances are formed to challenge existing powers and control capacities of established authorities are unable to govern. Non-state actors will have greater influence due to the spread of technology. Large populations of unemployed youth connect via networks to form groups that alter resource provider/consumer relationships. All Main Contributing Trends are amplified. Urbanisation will increase substantially and result in resource scarcity, reduced resilience, and will expose people to more vulnerability (e.g. disease, famine, economic, and social disorder).

Access and Use of Global Commons Challenged

Statement of Context

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

Main Contributing Trends

(3) Polycentric World, (9) Increased Access to Technology, (11) Globalisation of Financial Resources, (12) Increased Resource Scarcity, (13) Decreasing Defence Expenditures, (14) Environmental/Climate Change

Who:

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

Why:

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

How (Ways and Means):

Actors may disrupt lines of communications and distribution networks to deny natural resources to states. They will challenge maritime freedom of navigation and commerce (e.g. pirates, undersea robots and sea mines) extending their reach beyond the littorals to blue water. They will seek to increase their technical capabilities to disrupt trade. They will interrupt the air freedom of movement via widely available air defence and missile systems, unmanned vehicles, and computer technology that provide global reach. They will work to control the cyber domain to interdict satellite and voice communications, undermine financial electronic systems and degrade intelligence collection systems. It will be more expensive in the future to prevent or counter an adversary's use of low cost technology, such as the use of improvised explosive devices.

Where:

Actors will seek greater access to common use areas with a particular focus on new areas of exploration, resource development and trade. Examples of these new areas include the Arctic, outer space and cyberspace.

What is new in 2030?

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

High-Impact Cyber Threat

Statement of Context

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

Main Contributing Trends

(7) Fractured Identities, (8) Technology Accelerates Change, (9) Increased Access to Technology, (10) Centrality of Computer Networks, (11) Globalisation of Financial Resources

Who:

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

Why:

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

How (Ways and Means):

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

Where:

State and non-state actors will seek to control network infrastructure including computer centres and servers, hardware and software, electronic and fibre optic transmission lines, internet providers, and anything located in the physical world that is critical to network security. These powers will focus on a range of locations and systems to conduct operations from healthcare, transportation, communication, financial, energy, military or civilian services. With the rise of the “internet of things”, these operations will move to include almost all tangible and physical objects. Also, actors will seek to control virtual worlds and will conduct operations entirely within a computer based virtual battle-space.

What is new in 2030?

Essentially all things will be vulnerable due to near total interconnectedness and the blurring of physical and virtual worlds. The power of computing will be exponentially greater. The use of artificial intelligence and robotics will be pervasive throughout societies. The scale, speed, and impact of a cyber attack combined with the use of new technologies such as additive manufacturing will have global reach and influence across any and all borders. The ability to remain unknown while targeting specific systems combined with the minimal cost and low barrier of entry to obtaining a cyber-capability enhances the impact of cyber-attacks and provides little or no warning, i.e. a highly accurate stealth attack capability will be available to almost everyone. Cyber defence will lag further behind offense technology widening the gap between attack and protect capabilities.

Space Capability Disruption
Statement of Context
State or non-state actors compete for control over the space domain, e.g. freedom of operation in and through space. A broad range of multiple actors could take advantage of Alliance dependence on space enabled technologies which will increase vulnerability to NATO.
Main Contributing Trends
(1) Shift of Global Power, (3) Polycentric World, (8) Technology Accelerates Change, (9) Increased Access to Technology, (10) Centrality of Computer Networks, (13) Decreasing Defence Expenditures
Who:
State and non-state organisations with space capabilities and technologies may compete directly. There is also an advantage for those actors who are less dependent on space to attack space capabilities of those more dependent on space.
Why:
Less technology-dependent actors will use a vulnerability of space dependency to gain an asymmetric advantage, e.g. economic, and/or military advantage. These actors will seek to gain political power by attacking or disrupting space dependent powers and will compete for limited space resources (e.g. orbital and launch locations).
How (Ways and Means):
Actors will hijack or employ piracy of space infrastructure to achieve virtual or physical disruption or destruction of military, financial, navigation and communication capabilities. These actors will deny access to space, destroy or deny use of satellites, execute offensive space to space, earth to space, and space to earth operations. They will seek to gain either permanent or temporary control over space assets including communication, intelligence and navigation.
Where:
Actors will compete in space, within cyberspace, and on terrestrial based installations of geostrategic significance, e.g. launch sites and communication centres.
What is new in 2030?
Diminished redundancy because of greater dependence on space based systems creates new vulnerabilities, e.g. widespread dependence on Global Positioning System (GPS) and communication. Decreases in costs; proliferation of space technology; and increases in the number of potential actors in space, including private or commercial actors, increases competition and vulnerability to those who depend upon space capabilities and technology. There will be new actors in space including emerging powers. These emerging powers will have such an increased interest in the space domain to make the space increasingly more contested in 2030. There will be greater pressure to locate weapons in space. There will be a range of actors in space who are not directly controlled by any government.

Conflict in Euro-Atlantic Region

Statement of Context

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

Main Contributing Trends

(1) Shift of Global Power, (3) Polycentric World, (4) Changing Demographics, (6) Human Networks/Transparency, (7) Fractured Identities, (13) Decreasing Defence Expenditures

Who:

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

Why:

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

How (Ways and Means):

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

Where:

Euro-Atlantic Region; particularly NATO's periphery.

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

Non-State Actors Rival States

Statement of Context

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

Main Contributing Trends

(2) Shifting Political Structures, (3) Polycentric World, (4) Changing Demographics, (6) Human Networks/ Transparency, (7) Fractured Identities, (8) Technology Accelerates Change, (9) Increased Access Technology

Who:

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

Why:

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

How (Ways and Means):

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

Where:

This will occur along the border of NATO. These organisations will form by drawing globally members with similar agendas.

What is new in 2030?

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

Weapons of Mass Destruction / Effect (WMD/E) Use or Threat
Statement of Context
More actors have access to WMD/E leading to increased possibility of their use. Specifically, chemical, biological, and radiological weapons will be universally available to almost anyone with enough financial resources. Moreover, the impact of these weapons will increase significantly within the large urban populations of 2030.
Main Contributing Trends
(5) Urbanisation, (7) Fractured Identities, (8) Technology Accelerates Change, (9) Increased Access to Technology; 10) Centrality of Computer Networks
Who:
States and state-sponsored groups; emergent powers, non-state actors including super-empowered individuals, separatist groups and liberation movements or single issue political groups e.g. environmental politics.
Why:
In a multipolar world, actors use WMD/E to achieve a strategic shock that alters the power balance. These actors will also use WMD/E for deterrence, to influence negotiations or to blackmail an adversary. Use of WMD/E is a way for actors to achieve goals when other means like political, military, or financial are not available.
How (Ways and Means):
Having gained the capability to use WMD/E through widespread proliferation, actors can then threaten or actually conduct an attack. Actors will convert the opportunity of availability and access to these weapons and the increasing diversity in types of Weapons of Mass Destruction / Effect (e.g. atomic, chemical, biological, and cyber) as the means to empower weak actors.
Where:
WMD/E attacks will target overcrowded urban areas; critical infrastructure, water and food supplies, as well as communication nodes. These attacks may impact or threaten populations within regions of significant political tension. However as a tool for changing the balance of power, the attackers are more likely to target regions of established low political tension to create widespread chaos that will result in new governments.
What is new in 2030?
Due to globalisation and technological proliferation, actors will have far greater access to WMD/E technology and the ability to rapidly transmit the weapon components anywhere. The high speed of movement of any contagion, especially within urban areas, will greatly increase the appeal of megacities as a target for biological attack. The increased access to WMD/E technology within the commercial sector greatly improves the ability of radical and extremist groups to use WMD/E. Computer networks and the near total interconnectedness of all things will increase the ability of actors to execute a WMD/E attack via networks.

State to State Conflict
Statement of Context
Regional instability resulting from conflicts between states over territory, resources or historical tensions (e.g. border, ethnic, cultural, or religious disputes) will have global consequences due to globalisation, shifting political structures, and the expanding size and mobility of populations.
Main Contributing Trends
(1) Shift of Global Power, (2) Shifting Political Structures, (8) Technology Accelerates Change, (11) Globalisation of Financial Resources, (12) Increased Resource Scarcity, (13) Decreasing Defence Expenditures
Who:
States will compete globally resulting in armed action. This will involve a range of actors including private contractors, militias, religious or ethnic minorities, multinational corporations, and insurgent groups, as well as intergovernmental organisations, regional frameworks and alliances, like NATO, EU, and African Union.
Why:
States will resort to armed conflict because of fear, honour and/or interests. States will seek to increase national power and prestige by gaining resources, expanding territory, controlling populations, influencing supply lines, gaining or increasing economic power, bolstering national pride, rebalancing power and influence, forming new alliances, developing buffer zones, integrating territories or ethnic minorities, spreading ideologies, and reacting to crises in their geographic vicinity.
How (Ways and Means):
States will use all conventional means including the full range of military capabilities and operations, including all political, economic, and diplomatic means. States will also employ non-conventional means to deter or compel other states including offensive cyber capabilities, irregular militias and special forces and unconventional capabilities, like Weapons of Mass Destruction or Effect. States will demonstrate power with kinetic and non-kinetic means and will seek new international conventions and laws and will build new alliances and political blocks to enforce them. States will attempt to influence their narrative via new technology i.e. through social media and extending pervasive internet connectivity. States will provide economic and military support of minorities and implement embargos.
Where:
States will compete globally in all dimensions and domains, including space and cyberspace; particularly in densely populated, littoral and other regions rich in resources.
What is new in 2030?
States will possess wide-spread access to the most advanced technology, such as space-based weapon systems; artificial intelligence (AI), robotic systems, enhanced human capabilities, additive manufacturing, advanced electronic warfare, and WMD/E. Population increasing will exceed the ability of states to provide basic needs. New resources will be available due to new technologies and climate change. Urbanisation will drive the need for more resources. Global transparency will allow rapid dissemination of ideas (political, economic, religious, cultural, and social), highlighting the disparity between developing and developed regions. Multipolar competition will replace unipolar hegemony and bipolar competition.

Strategic Military Perspectives

SACT delivered the following ideas in his speech for the Military Committee in Chiefs of Staff Session on 21 May 2014:

"Last time we met, I stressed that Framework of Future Alliance Operations was from my point of view one of our most important strands of work in the enduring transformation of NATO. More than ever we have to focus on adapting our military strategy to "redefine" the employment of military forces in order to face the wide variety of situations, risks and threats in short to keep the relevance of our forces in the foreseeable future.

Taking into account the outcome of the Strategic Foresight Analysis which identified emerging trends in the future security environment, we have identified generic potential what we call instability situations which will help us to shape strategic military perspectives and their military implications.

I must stress at this point, we have already clear confirmation on **3 major trends** that will influence future planning and capability development which are relevant in the scope of the current crisis even if we develop, namely **improved situational awareness**, and operational intelligence, and more **adaptable shaping** ready forces. Lastly, but not least, the maintaining of **robust collective resilience**, but obviously we must carry on digging deeper to get full Strategic Military Perspectives and Military implication.

I see FFAO as an indispensable tool to provide the MC with a vehicle to refine long term military capability requirements, as well as doctrine, training and exercises. FFAO is a key to inform next NDPP cycle.

FFAO is a collective effort which has already enjoyed the benefit of many nations' involvement plus 9 COEs and partners. Concerning the latter, we must consider how they will be involved in the next more sensitive works. Obviously in developing strategic military perspectives we will seek full MC involvement and furthermore I propose to make FFAO content a permanent topic for the MCCS."

Strategic Military Perspectives

Examples

1. **Strategic Awareness**

Strategic Awareness is a deliberate and continuous focus on a shared and agreed assessment of future strategic level challenges and opportunities, to enable the synchronization and alignment of military planning with political intent. Strategic Awareness supports a more coherent understanding of the greater interconnectedness, economic and political interdependency and their change over time which may impact the Alliance, its individual members and partners at the global level. This understanding will enable the Alliance to anticipate and address the increased uncertainty and unpredictability and to exploit opportunities.

Strategic Awareness is the ability to deal with two main aspects: "actors" and "issues" that are likely to cause challenges to states and traditional institutions in the future. New emerging non-state and transnational actors, and individuals through rapidly expanding human networks, may create threats. Strategic Awareness is linked to understanding the motivation, aim and role of these actors in the overall future context, as well as the level at which they are likely to challenge the states and traditional institutions. Issues, such as environment and climate change, natural disasters and demographics will also cause challenges for the Alliance. Both actors and issues may present security challenges at the local, regional and global level.

2. Adaptive Shaping

Adaptive Shaping is the ability to anticipate and counter a diversified range of potential threats, depending on the scope, scale and attribution. This may require a strategic approach, in conjunction with other intergovernmental decision-making bodies, and a combination of soft and hard power solutions to

deal with multi-layer hybrid and dynamic trans-national groups in an expanded engagement space. Adaptive Shaping will encompass a broadened deterrence posture, which could increase NATO's ability to deter similarly adaptive adversaries who may be operating in less attributable domains such as cyber or space. The ability to adapt shaping actions to a variety of identified threats is critical in a future characterized by a decreased time to respond to security challenges and opportunities in current and new domains.

Analysis of SFA trend combinations indicates the changing character of emerging defence and security challenges. Specifically, the trends of technology accelerating change, population growth in urban areas, and human networks expanding at an exponential rate combine to increase the need for a broader deterrent posture that can rapidly adapt in type and pace. Furthermore, adaptive shaping provides the Alliance the ability to identify opportunities within the challenges and act quickly to gain an advantage. Adaptive Shaping and deterrence depends upon a rapid decision making process and a shared awareness gained through an established process of rapid continuous exchange of relevant information between the all members of the defence and security community. That is why adaptive Shaping focuses so closely on gaining and maintaining trust within the wider defence and security community. Moreover, these trend combinations indicate potential changes in the character of future crises and challenge this community with finding new ways of managing crises.

NATO's 2010 Strategic Concept presented the idea of security through crisis management by stating the "*best way to manage conflicts is to prevent them from happening. NATO will continually monitor and analyse the international environment to anticipate crises and, where appropriate, take active steps to prevent them from becoming larger conflicts*." Adaptive Shaping expands this idea and builds upon this view of crisis management by prevention. Shaping in this way would prevent conflict by focusing resources more sharply on the military capability to anticipate crises. Adaptive Shaping then retains the structure, capacity, and ability to adapt military action in a timely manner to

prevent future crises. Developing and maintaining the ability to anticipate and counter threats by broadening the Alliance's deterrence posture includes an expanded and shared awareness of the evolving character of threats. As threats change, the Alliance's ability to deter would anticipate the risks and rapidly work to counter the emerging challenge. Thus eliminating or moderating risks before they become uncontrollable. The increased speed of deterrence required to counter such threats depends upon achieving a more comprehensive capacity to prevent conflict. The Alliance could build trust through reciprocity, cooperation, and collaboration to achieve complementary action in countering the variety of identified threats. This could, for example, involve enabling a joint military and civilian coordination center to monitor the growth of populations, human networks and technology to achieve greater sharing of knowledge and allow better collaborative planning of mitigating actions to counter threats.

3. Shared Resilience

Shared Resilience is to maintain sufficient reserve capacity across the Alliance member states to provide a shared ability to withstand strategic shocks and the ability to adapt to the Future Security Environment (FSE). Shared Resilience should also include structures and systems, with the capability for rapid recovery, and the constant ability to analyse and process data throughout crises despite potential interruption. One foundation of Shared Resilience is a comprehensive, rapid and adaptive decision making process. Another foundation is a certain degree of trust between the involved actors. Enhanced mutual transparency and understanding will increase the level of trust and will enable an improved coordinated response to any threat or opportunity.

Countering strategic shocks depends greatly on the nature and level of Alliance reserves. The nature of the FSE combines several threats that could lead to a systemic failure that overwhelms NATO capacities. National resilience is adequate for securing state borders but the Alliance contains excess capacity and local and regional expertise in order to counter conventional threats and deter unconventional threats. By vastly expanding the number of state and non-state actors interacting with NATO, the Alliance could significantly

increase its reserve capacity which will eventually improve its ability to manage crises, with relatively similar resources. These interactions could include establishing routine communication channels to facilitate coordination and collaboration with the purpose of increasing interoperability without requiring interdependence. In addition to military aspects of capacity, the Alliance could benefit from the unique skills and abilities of organizations and individuals.

Gaining and maintaining a comprehensive and adaptive decision making process is the most important factor in order to generate the required rapid and coordinated response required. This includes coordinating with non-governmental and other governmental organizations, such as the European Union or Interpol, to support Alliance military decision making processes that need to be dynamic and networked.

Capability Hierarchy Framework Definitions

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

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

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

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

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

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

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

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